Schleswig-Holsteinischer Landtag
Umdruck 16/2169

ULD • Postfach 71 16 • 24171 Kiel

Vorsitzenden
des Innen- u. Rechtsausschusses
des Schleswig-Holsteinischen Landtags
Herrn Werner Kalinka
Postfach 7121
24171 Kiel

Holstenstraße 98
24103 Kiel
Tel.: 0431 988-1200
Fax: 0431 988-1223

Ansprechpartner/in:
Herr Bergemann
Durchwahl: 988-1216

Aktenzeichen:
LD5-73.03/99.091

Kiel, 27. Juni 2007

Gesetzesentwurf der Bundesregierung für ein Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, BR-Drucksache 275/07
45. Sitzung des Innen- und Rechtsausschusses vom 18. April 2007, Punkt 4 der Tagesordnung

Sehr geehrter Herr Vorsitzender,
sehr geehrte Damen und Herren Abgeordnete,

der Innen- und Rechtsausschuss hat das Unabhängige Landeszentrum für Datenschutz gebeten, zu dem ersten Referentenentwurf des Bundesjustizministeriums zur Gesamtreform der strafprozessualen Eingriffsbefugnisse Stellung zu nehmen. Dieser Bitte ist das ULD mit Schreiben vom 12. März 2007 (Umdruck 16/1857) nachgekommen. Der erneuten Bitte des Innen- und Rechtsausschusses, den nunmehr vorliegenden Gesetzesentwurf der Bundesregierung (siehe oben) zu bewerten, kommen wir ebenfalls gerne nach. Ergänzend gehen wir auf einige der aktuellen Änderungsvorschläge des Bundesrates (Beschluss vom 8. Juni 2007) ein (Anlage 1). Unsere aktuelle Stellungnahme erläutert ausführlich die Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. Juni 2007 (Anlage 2), der eine Entschließung vom 8./9. März 2007 voranging (Anlage 3).

Mit freundlichen Grüßen

Dr. Thilo Weichert

Anlagen:
Stellungnahme des ULD vom selben Tage
Entschließungen der DSB-Konferenz vom 8. Juni 2007 und vom 8./9. März 2007

Anlage 1

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Stellungnahme

Gesetzesentwurf der Bundesregierung für ein Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, BR-Drucksache

Inhalt

ULD • Postfach 71 16 • 24171 Kiel

Holstenstraße 98
24103 Kiel
Tel.: 0431 988-1200
Fax: 0431 988-1223

Ansprechpartner/in:
Herr Bergemann
Durchwahl: 988-1216

Aktenzeichen:
LD5-73.03/99.091

Kiel, 27. Juni 2007

Gesetzesentwurf der Bundesregierung für ein Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, BR-Drucksache 275/07
45. Sitzung des Innen- und Rechtsausschusses vom 18. April 2007, Punkt 4 der Tagesordnung

Das mit dem Entwurf von der Bundesregierung verfolgte Ziel, ein in sich schlüssiges Gesamtsystem strafprozessualer heimlicher Ermittlungsmethoden zu schaffen sowie die umfassende aktuelle Rechtsprechung des Bundesverfassungsgerichts umzusetzen, begrüßen wir ausdrücklich. Das Ziel einer Verbesserung des Grundrechtsschutzes im strafrechtlichen Ermittlungsverfahren erreicht der Entwurf jedoch nur unzureichend.

Die Einführung der Vorratsdatenspeicherung durch Umsetzung der EG-Richtlinie (Richtlinie 2006/24/EG) ist verfassungsrechtlich nicht tragbar. Die Überarbeitung des ersten Referentenentwurfs führte zu einer weiteren Ausdehnung der Datenschutzbefugnisse, die über die durch die Richtlinie gezogenen Grenzen hinausgeht.

A. Reform der verdeckten Ermittlungsmethoden in der Strafprozessordnung (Artikel 1)

Der vorliegende Entwurf muss sich an der umfangreichen Verfassungsrechtsprechung der letzen Jahre messen lassen. Notwendige Kernpunkte einer Reform sind:

- Überarbeitung der Eingriffsvoraussetzungen verdeckter Ermittlungsmaßnahmen, orientiert am Grundsatz der Verhältnismäßigkeit sowie der Normenklarheit und -bestimmtheit, auch im Hinblick darauf, die Erfassung unverdächtiger Personen zu vermeiden
- Herstellung eines umfassenden Schutzes des Kernbereichs privater Lebensgestaltung

- Schutz aller Informationen, die Zeugnisverweigerungsberechtigten im Vertrauen auf ihre besondere Stellung überlassen wurden
- Effektive Verfahrenssicherungen, etwa Richtervorbehalte, die jedoch eine rechtsstaatlich saubere Ausgestaltung der Eingriffsvoraussetzungen und der Eingriffsbegrenzungen nicht ersetzen können, sondern diese ergänzen
- Sicherstellung der Benachrichtigung aller Betroffenen über verdeckt durchgeführte Maßnahmen (Art. 19 Absatz 4 GG)

In einer jüngeren Entscheidung formuliert das Bundesverfassungsgericht als gedanklichen Ausgangspunkt einer Reform der verdeckten Ermittlungsmaßnahmen:

> *„Das Bundesministerium der Justiz hat mitgeteilt, seit längerem an einer Gesamtregelung der strafprozessualen heimlichen Ermittlungsmaßnahmen zu arbeiten, die die Vorschriften zur Telekommunikationsüberwachung (…) umfassen. Bei der Umsetzung dieser Vorschläge wird der Gesetzgeber die technischen Entwicklungen wegen des schnellen und für den Grundrechtsschutz riskanten informationstechnischen Wandels aufmerksam beobachten und gegebenenfalls durch Rechtssetzung korrigierend eingreifen müssen (vgl. BVerfGE 112, 304 [320 f.] = NJW 2005, 1338). Dabei wird zu prüfen sein, ob verfahrensrechtliche Vorkehrungen - wie etwa Benachrichtigungspflichten oder Rechtsschutzmöglichkeiten - zu erweitern sind, um den Grundrechtsschutz effektiv zu gewährleisten. 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.“ (BVerfG NJW 2007, 351, 356)*

Eine Überarbeitung der Vorschriften kann in sinnvoller Weise nur auf Grundlage einer umfassenden wissenschaftlichen Evaluation erfolgen, die durch eine unabhängige Stelle durchgeführt wurde. Evaluationen liegen bislang nur für die Telekommunikationsüberwachung und für den Großen Lauschangriff vor. Erforderlich ist wenigstens eine in Zukunft regelmäßig vorzunehmende Evaluation der verdeckten Ermittlungsmaßnahmen. Aus dem Entwurf ergibt sich nicht unmittelbar, ob und in welcher Form eine solche durchgeführt werden soll bzw. muss.

Die bisherigen Defizite der strafprozessualen Regelungen werden durch die Neuregelung nicht beseitigt. Teilweise führen die geplanten Vorschriften sogar zu einer Erweiterung der Eingriffsbefugnisse, wie etwa ein Blick auf den Anlasstatenkatalog der Telekommunikationsüberwachung zeigt.

1. Zu § 53b StPO-E – Schutz der Zeugnisverweigerungsberechtigten

Das Ziel, einen einheitlichen Schutz der Informationen sicherzustellen, die Zeugnisverweigerungsberechtigten im Vertrauen auf ihre Verschwiegenheit anvertraut wurden, ist grundsätzlich sehr zu begrüßen. Dies gilt insbesondere, soweit neue Schutzregeln auch bei verdeckten Ermittlungsmaßnahmen eingreifen. Die Schutzansprüche der Zeugnisverweigerungsberechtigten drohen jedoch in der vorliegenden Entwurfsfassung durch weit angelegte Abwägungsklauseln aufgeweicht zu werden.

a) Differenzierung der Zeugnisverweigerungsberechtigten

Die im Entwurf vorgenommene Differenzierung nach verschiedenen „Klassen“ von Zeugnisverweigerungsberechtigten ist nicht nachvollziehbar und untergräbt einen wirksamen Grundrechtsschutz.

Der Entwurf unterscheidet zwischen Geistlichen, Strafverteidigern sowie Abgeordneten auf der einen Seite (§ 53b Abs. 1 StPO-E) und Rechtsanwälten, Steuerberatern, Ärzten und ähnlichen Personen sowie Journalisten auf der anderen Seite (§ 53b Abs. 2 StPO-E). Nur bei der ersten Gruppe sind die verdeckten Ermittlungsmaßnahmen unzulässig. Bei der zweiten Gruppe sind die Zeugnisverweigerungsrechte bei der heimlichen Überwachung lediglich „im Rahmen der Prüfung der Verhältnismäßigkeit und der Würdigung des öffentlichen Interesses an den von dieser Person wahrgenommenen Aufgaben und des Interesses an der Geheimhaltung der dieser Person anvertrauten oder bekannt gewordenen Tatsachen besonders zu berücksichtigen“. Diese wortreiche Abwägungsklausel lässt jeden *objektiv messbaren Maßstab* vermissen. Aus welchem Grund wird ein Arzt oder Rechtsanwalt weniger geschützt als ein Strafverteidiger oder Geistlicher? Die Sachentscheidung wird damit faktisch der Exekutive überlassen, eine Entscheidung frei von subjektiver Willkür ist – auch bei bestem Willen der handelnden Beamten – kaum möglich.

b) Schutz der Kommunikation mit Zeugnisverweigerungsberechtigten

Durch die neue Formulierung nach der Überarbeitung des ersten Referentenentwurfs sollen Informationen bei Zeugnisverweigerungsberechtigten nur noch dann dem Schutz der Regelung unterliegen, wenn sich die Maßnahme *„gegen“* eine zeugnisverweigerungsberechtigte Person richtet. Nicht mehr ausreichend soll es sein, wenn der Zeugnisverweigerungsberechtigte durch eine Maßnahme *„betroffen“* ist. Lediglich dann, wenn sich konkret ergibt, dass Erkenntnisse erlangt worden sind, die einem Zeugnisverweigerungsrecht unterliegen, soll ein relativer Schutz eingreifen.

Diese neue Regelung ist, worauf bereits der Bayerische Landesbeauftragte für Datenschutz in seiner Stellungnahme vom 22. Mai 2007 zutreffend hingewiesen hat, unzureichend. Denn durch die neue Formulierung bleibt eine Maßnahme, die sich gegen andere Personen – etwa einen Beschuldigten oder einen Dritten – richtet, grundsätzlich zulässig, und zwar sogar dann, wenn nicht ausgeschlossen werden kann oder gar zu erwarten ist, dass auch die Kommunikation mit Zeugnisverweigerungsberechtigten und die dabei ausgetauschten Inhalte betroffen sein werden.

Beispiel:

> *Der Beschuldigte, dessen Telefonanschluss überwacht wird und der seinen Verteidiger anruft, wäre durch die aktuelle Entwurfsfassung nicht durchgehend geschützt. Denn diese Überwachung richtet sich nicht „gegen“ den Verteidiger. Nach dem Wortlaut des Entwurfs könnte das Gespräch mit dem Strafverteidiger zunächst abgehört werden. Erst wenn sich im Rahmen der Überwachung ergibt, dass das Gespräch Erkenntnisse betrifft, über die der Verteidiger das Zeugnis im Einzelfall verweigern kann, würde ein insoweit begrenzter – relativer – Schutz eingreifen. Dies widerspricht den verfassungsrechtlichen Vorgaben, die eine*

vollständig geschützte Kommunikation zwischen Verteidiger und Mandant gewährleisten. Der Referentenentwurf des BMJ vom 27. November 2006 hätte insoweit zu einem besseren Schutz dieser Kommunikation geführt, da der Strafverteidiger im Beispiel durch die Telekommunikationsüberwachung „betroffen" gewesen wäre.

Gespräche mit Strafverteidigern oder Seelsorgern betreffen in der Regel Inhalte aus dem Kernbereich privater Lebensgestaltung (BVerfG NJW 2004, 999, 1004). Insoweit müsste die Regelung ein absolutes Erhebungsverbot festlegen, auch soweit sich die Maßnahme nicht gegen den Strafverteidiger oder Seelsorger richtet. Danach müsste eine Überwachung unterbrochen werden, sobald ersichtlich ist, dass der Beschuldigte etwa den Anschluss seines Verteidigers anwählt. Zwar mag diese Vorgehensweise in den verwendeten technischen Anlagen noch nicht implementiert sein, technisch wäre sie aber realisierbar, verfassungsrechtlich ist sie gefordert.

c) Beteiligung des Zeugnisverweigerungsberechtigten

Die Durchbrechung des Schutzes bei einer Beteiligung des Zeugnisverweigerungsberechtigten, einer Strafvereitelung oder einer Anschlusstat ist insofern problematisch, als diese ein Unterlaufen der Schutzregelungen wahrscheinlicher macht. Dies gilt insbesondere für Fälle, in denen gegen Journalisten wegen Beteiligung an einer Geheimnisverletzung vorgegangen wird. Hier besteht die Gefahr, dass als Ziel der Maßnahme auch die Beschlagnahme der redaktionellen Unterlagen ermöglicht wird (vgl. BVerfG JNW 2007, 1117 f Cicero). Daher wurden verschiedene Gesetzesinitiativen zum Schutze der Pressefreiheit eingebracht, die bislang aber noch keine Berücksichtigung gefunden haben (vgl. BT-Drs. 16/956; BT-Drs. 16/576 sowie BR-Drs. 650/06.). Immerhin sieht der Entwurf eine Durchbrechung nur dann vor, wenn ein formelles Verfahren eingeleitet wurde. Dieses ist bereits möglich, wenn ein einfacher Anfangsverdacht vorliegt, immerhin aber mit einer formellen Prüfung verbunden. Problematisch ist jedoch auch diese Schwelle, da keine ausdrückliche Bezugnahme auf Tatsachen – wie etwa bei § 100a StPO – gefordert ist.

d) Entscheidung über die Verwertbarkeit

Nach der noch im Referentenentwurf in § 53b Absatz 1 Satz 4 StPO-E vorgesehenen Regelung sollte bei Zweifeln über die Verwertbarkeit eine gerichtliche Entscheidung eingeholt werden. Diese Regelung wurde im nunmehr vorliegenden Entwurf gestrichen, was nicht nachzuvollziehen ist.

e) Vorschläge des Bundesrates

Die Änderungswünsche des Bundesrates (BR-Drucksache 275/07 Beschluss v. 8. Juni 2007) drohen den Versuch, einen wirksamen Schutz der Zeugnisverweigerungsrechte sicherzustellen, weiter zu verwässern. Dies gilt insbesondere für die geänderte Fassung des § 53b Absatz 4 Satz 1 und § 97 Nr. 3 Buchstabe a Doppelbuchstabe bb StPO-E. Diese will die Durchbrechung des Schutzes schon dann erlauben, wenn noch kein Strafverfahren gegen den Zeugnisverweigerungsberechtigten eingeleitet wurde; ein bloßer Verdacht soll genügen. Dies würde in der Praxis zu einer kaum überschaubaren

Aushöhlung des Schutzes der Zeugnisverweigerungsrechte führen, da sogar eine formelle Prüfung bei Einleitung des Verfahrens fehlen würde.

2. Zu §§ 99, 100 StPO

Der Entwurf beschäftigt sich im Rahmen des § 100 StPO-E mit einigen Anpassungen. Eine – angesichts der angestrebten Gesamtreform – naheliegende Frage blendet der Entwurf aus: Für die Beschlagnahme von Postsendungen ist bislang ein strafprozessualer Anfangsverdacht i.S.d. § 152 Abs. 2 StPO ausreichend. Als Grundrecht ist das Postgeheimnis in gleicher Weise durch Art. 10 GG geschützt wie das Fernmeldegeheimnis. Daher ist nicht nachvollziehbar, aus welchem Grund die bisherige Regelung in ihrem Schutzstandard noch nicht an die Anforderungen zur Telekommunikationsüberwachung angeglichen ist. Im Rahmen des vorliegenden Gesetzgebungsverfahrens besteht die Gelegenheit, dies nachzuholen.

3. Zu § 100a StPO-E

Die Telekommunikationsüberwachung ist Kernstück der mit dem Entwurf verfolgten Neuregelung der verdeckten Ermittlungsmaßnahmen. Die Rechtsprechung des Bundesverfassungsgerichts der letzten Jahre macht eine Überarbeitung unumgänglich. Die Erweiterung der Eingriffsmöglichkeiten mit dem Mittel der Telekommunikationsüberwachung durch eine Ausdehnung des Anlasstatenkatalogs lässt allerdings zweifelhaft erscheinen, ob der Grundrechtsschutz an erster Stelle stand, ebenso die mangelhafte Umsetzung des vom Bundesverfassungsgericht eingeforderten Schutzes des Kernbereichs privater Lebensgestaltung.

a) Eingriffsschwelle (Absätze 1 – 3)

Das vom Entwurf angestrebte Ziel, die Telekommunikationsüberwachung nur bei mindestens „schweren Straftaten“ zuzulassen, ist im Grundsatz zu begrüßen. Allerdings lässt der mit dem Entwurf wesentlich erweiterte Anlasstatenkatalog diesen Ansatz in weiten Teilen unvollendet.

Die gestiegenen Anwendungszahlen der Telekommunikationsüberwachung in den letzten Jahrzehnten zeigen, dass eine grundlegende Überarbeitung der Eingriffsschwelle dieser Maßnahme notwendig ist. Die Besorgnis erregende Entwicklung der Telekommunikationsüberwachung ergibt sich etwa aus der umfassenden Studie des Max-Planck-Instituts für ausländisches und internationales Strafrecht (vgl. hierzu Albrecht/Dorsch/Krüpe, Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen - Abschlussbericht, Freiburg 2003, S. 27 ff. - im Folgenden: MPI-Studie). Diese gestiegenen Fallzahlen sind nicht zuletzt auf den bisherigen Straftatenkatalog des § 100a Strafprozessordnung (StPO) zurückzuführen, der inzwischen eine kaum überschaubare Weite aufweist.

Statt auf diese Entwicklung einschränkend zu reagieren, wurde der Katalog der Straftaten, deren Anfangsverdacht die Durchführung einer Telekommunikationsüberwachung rechtfertigt, mit dem vorliegenden Entwurf nochmals erweitert (§ 100a Absatz 2 StPO-E). Aus dem Straftatenkatalog

wurden lediglich solche Delikte herausgestrichen, die in der Praxis ohnehin gar nicht oder kaum vorkommen, so etwa die Fahnenflucht (vgl. § 100a Satz 1 Nr. 1d StPO).

Zugleich sind die Erweiterungen beträchtlich; sie hier alle im Einzelnen zu bewerten, würde den Rahmen der Stellungnahme sprengen. Beispielhaft sind aber die neu aufgenommenen bestimmten Urkunds- oder Betrugsdelikte oder bestimmte Delikte aus der Abgabenordnung zu nennen, deren strafrechtliche Regelung mit dem Entwurf gleichzeitig überarbeitet wird. In der Entwurfsbegründung wird an verschiedenen Stellen zur Begründung auf ein „erhebliches praktisches Bedürfnis“ abgestellt, so etwa bei der Begründung der Aufnahme von Delikten nach der Abgabenordnung oder aus dem Bereich der Wirtschaftskriminalität. Ein solches „praktisches Bedürfnis“ dürfte bei der Kriminalitätsbekämpfung – unabhängig vom Schweregrad der Kriminalität – generell bestehen. Auch wenn das „praktische Bedürfnis“ mit dem Begriff der Geeignetheit gleichzusetzen sein sollte: Praktische Bedürfnisse ersetzen nicht eine umfassende Abwägung mit den erheblichen Grundrechtseingriffen zu Lasten der durch die Überwachungsmaßnahme betroffenen Personen. Es geht bei der gesetzgeberischen Abwägung darum, die Grenzen strafverfolgender Ermittlungstätigkeit rechtsstaatlich festzulegen – Grenzen, die auch in den Fällen gelten, in denen die Maßnahme als nützlich erscheint. Besteht kein praktisches Bedürfnis, kommt ohnehin niemand auf die Idee, eine Maßnahme einzusetzen. Diese Abwägung fehlt in den einzelnen Begründungen der Katalogerweiterungen und ist lediglich in der Einleitung der Begründung zu Absatz 2 kurz erwähnt.

Bei der Anwendung des Kataloges ist zu beachten, dass bereits ein Verdacht genügt, der Tatvorwurf gegen den Beschuldigten also noch nicht erhärtet sein muss. Die Entwurfsbegründung weist selbst darauf hin, dass es in der Strafverfolgungspraxis gerade im Bereich der Wirtschafts- und Transaktionskriminalität schwierig sei, in „abgeschottete Strukturen“ einzudringen. Strukturermittlungen bergen stets die Eigenart in sich, dass gegen eine Vielzahl von Personen ermittelt wird. Hierdurch steigt das Risiko, dass viele unbeteiligte Personen in die Überwachung einbezogen wird. Dies gilt um so mehr, als sich nach wie vor die Maßnahme gegen Personen richten darf, deren Anschluss der Beschuldigte voraussichtlich nutzt oder die voraussichtlich Nachrichten an diesen weiterleiten.

Angesichts des Umfangs des Katalogs ist das Gesetz nicht mehr weit von dem Punkt entfernt, an dem es – sprachlich – einfacher wird, die Delikte zu benennen, die nicht mit dem Mittel der Telekommunikationsüberwachung überwacht werden können. Dass hierbei die Grundrechte auf der Strecke bleiben, ist offensichtlich. Hatte die Telekommunikationsüberwachung bei ihrer Einführung noch Ausnahmecharakter, so ist sie inzwischen zu einem „Massenverfahren“ geworden.

Zu begrüßen ist die gesetzliche Klarstellung, dass die Anlasstat auch im Einzelfall schwer wiegen muss (§ 100 Abs. 1 Nr. 2 StPO-E).

Die verwendete Subsidiaritätsklausel (§ 100 Abs. 1 Nr. 3 StPO-E) zeigt im Vergleich zu den anderen geplanten bzw. zu überarbeiteten Vorschriften, dass der Gesetzesentwurf das sich selbst gesetzte Ziel einer Harmonisierung und Präzisierung der verdeckten Ermittlungsmaßnahmen nicht

erreicht. Subsidiaritätsklauseln dienen der Entscheidung, ob andere, weniger in die Grundrechte eingreifende Ermittlungsmethoden vorrangig anzuwenden sind. Diese sind im Entwurf jedoch für die einzelnen Ermittlungsmaßnahmen höchst unterschiedlich geregelt; teilweise gilt keinerlei Subsidiaritätsklausel, sondern es wird lediglich die sachliche Erforderlichkeit einer Ermittlungsmethode verlangt. Subsidiaritätsbestimmungen, wie „wesentlich erschwert“ oder „unverhältnismäßig erschwert“, stellen in der Praxis keine hinreichend bestimmte Begrenzung für den Einsatz verdeckter Ermittlungsmaßnahmen dar.

b) Schutz des Kernbereichs privater Lebensgestaltung (Absatz 4)

Verdeckte Ermittlungsmaßnahmen dürfen niemals in den **Kernbereich privater Lebensgestaltung** eingreifen. Dies hat das Bundesverfassungsgericht in seinen Entscheidungen vom 03.03.2004 (NJW 2004, 999, Großer Lauschangriff) und vom 27.07.2005 (BVerfG NJW 2005, 2603, präventive Telekommunikationsüberwachung) klargestellt.

Das Bundesverfassungsgericht hat in seiner Entscheidung vom 27. Juli 2005 auch für den Bereich der Telekommunikationsüberwachung Erhebungsverbote gefordert (siehe hierzu z. B. die Beiträge in Schaar, Folgerungen aus dem Urteil des Bundesverfassungsgerichts zur akustischen Wohnraumüberwachung, Staatliche Eingriffsbefugnisse auf dem Prüfstand? sowie in Roggan, Lauschen im Rechtsstaat, Zu den Konsequenzen des Urteils des Bundesverfassungsgerichts zum großen Lauschangriff – Gedächtnisschrift für Hans Lisken, 2004; Graulich, NVwZ 2005, 273; Kötter, DÖV 2005, 225 (233); Kutscha NVwZ 2005, 1231 f.; Gusy, JuS 2004, 461; anders soweit ersichtlich nur: Haas 2004, 3082 ff., Löffelmann NJW 2005, 2033, 2035; Märkert, Kriminalist 2004, 443, 447). Dies gilt für den Fall, dass im konkreten Fall tatsächliche Anhaltspunkte für die Annahme sprechen, dass die Überwachung Inhalte erfasst, die den Kernbereich betreffen.

Der Entwurf fügt eine Regelung zum Kernbereichsschutz ein, die allerdings nur als rudimentär bezeichnet werden kann und die den Karlsruher Vorgaben nicht gerecht wird.

(1) Vollständigkeit des Kernbereichsschutzes

Die überwachten Gespräche sind „in der Regel durch eine Gemengelage unterschiedlicher Inhalte geprägt“ (BVerfG 2004, 999, 1006). Ein Erhebungsverbot besteht nach Ansicht des Bundesverfassungsgerichts bereits dann, wenn nur ein Teil des Gesprächs diesen Bereich betreffen wird (BVerfG a.a.O.; Denninger ZRP 2004, 103; Leutheusser-Schnarrenberger ZRP 2005, 1, 2 m.w.N.; Bergemann in Roggan, Lauschen im Rechtsstaat, S. 77).

Daher ist es verfassungsrechtlich nicht hinnehmbar, wenn der Entwurf den Kernbereichsschutz erst dann gewährt, wenn das Gespräch ***allein*** (!) den Kernbereich privater Lebensgestaltung betrifft, wie dies nach § 100a Abs. 4 Satz 1 StPO-E nunmehr geregelt sein soll.

(2) Gestufter Kernbereichsschutz

Zum Schutz des Kernbereichs hat das Bundesverfassungsgericht ein gestuftes Vorgehen vorgezeichnet. Die Ermittlungsbehörden haben bereits vor Durchführung der Maßnahme auf der ersten Stufe eine Prognoseentscheidung zu treffen, ob zu erwarten ist, dass kernbereichsrelevante Gesprächsinhalte erfasst werden (Erhebungsverbot erster Stufe). Denn das Bundesverfassungsgericht hat formuliert: „Bestehen im konkreten Fall tatsächliche Anhaltspunkte für die Annahme, dass eine Telekommunikationsüberwachung Inhalte erfasst, die zu diesem Kernbereich zählen, ist sie nicht zu rechtfertigen und muss unterbleiben“ (BVerfG NJW 2005, 2603, 2612).

> *Beispiel: Lebt ein Beschuldigter mit seiner Lebensgefährtin, die selbst nicht tatverdächtig ist, in einer – aufgrund der aktuellen Anforderungen des Arbeitsmarktes zunehmend verbreiteten – „Fernbeziehung“, so ist dies ein Anhaltspunkt dafür, dass diese Personen voraussichtlich kernbereichsrelevante Gesprächsinhalte haben werden. In diesem Fall sind die zwischen den Anschlüssen dieser Personen geführten Gespräche von der Überwachung auszunehmen, da Anhaltspunkte die Annahme rechtfertigen, dass der Kernbereich betroffen wird.*

Der Schutz wäre allerdings unvollständig, wenn während der Durchführung der Maßnahme die Situation nicht beobachtet würde, um ggf. reagieren zu können und Eingriffe in den Kernbereich abzustellen. Erscheint angesichts der Prognoseentscheidung die Überwachungsmaßnahme möglich, ist daher auf der *zweiten Stufe* das Abhören und die Aufzeichnung der Gespräche ständig zu kontrollieren („Live-Überwachung“). Entsprechend formuliert das Gericht für die Telekommunikationsüberwachung: „Hinzu müssen Vorkehrungen kommen, die sichern, dass die Kommunikationsinhalte des höchstpersönlichen Bereichs nicht gespeichert […] werden dürfen, sondern unverzüglich gelöscht werden, wenn es ausnahmsweise zu ihrer Erhebung gekommen ist“ (BVerfG NJW 2005, 2603, 2612).

Unabhängig von der Frage der „Live-Überwachung“ sollte zumindest ein Abbruchgebot formuliert werden. Es muss im Gesetz klargestellt sein, dass nach Beginn der Maßnahme und nach Erlass des richterlichen Überwachungsbeschlusses ein Abbruch erfolgen muss, sobald die Kernbereichsrelevanz der Gesprächsinhalte aufgrund tatsächlicher Anhaltspunkte anzunehmen ist.

Gegen die Einführung solcher Erhebungsverbote kann nicht eingewandt werden, die gegenwärtige Überwachungstechnik sei hierauf noch nicht eingerichtet. Denn zum einen ist die Einführung entsprechender Schutzmechanismen ist technisch realisierbar. An anderer Stelle fordert der Entwurf selbst ein, im Bereich der Vorratsdatenspeicherung (dazu unten II) noch nicht vorhandene Speicherungstechnik im großen Umfang zu beschaffen.

Das Bundesverfassungsgericht hat in seiner Entscheidung vom 3. März 2004 einfache Verwertungsverbote als nicht ausreichend erachtet, sondern diesen eine Fernwirkung zuerkannt (NJW 2004, 999, 1007 - Abs.-Nr. 184). Die Regelung in § 100a Abs. 4 Satz 2 StPO-E enthält hierauf keinen Hinweis. Wir regen insoweit an, sie um eine klarstellende Formulierung zu ergänzen.

(3) Alternativformulierung zum Kernbereichsschutz

Aus vorstehenden Gründen regen wir an, § 100a Abs. 4 StPO-E wie folgt zu fassen:

> *„(4) Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch eine Maßnahme Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, ist die Maßnahme unzulässig. Die Datenerhebung ist sofort abzubrechen, sofern unerwartet erkennbar wird, dass solche Erkenntnisse erlangt werden. Während der Datenerhebung ist dies ständig zu kontrollieren. Sofern unerwartet Erkenntnisse erlangt werden, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, sind diese unverzüglich zu löschen. Sie dürfen nicht verwertet werden, auch nicht als Ansätze für weitere Ermittlungen. Die Tatsache ihrer Erlangung und Löschung ist aktenkundig zu machen."*

Darüber hinaus regen wir an, Kriterien oder Regelbeispiele zu benennen, in welchen Fällen im Rahmen einer Prognoseentscheidung anzunehmen ist, dass der Kernbereich privater Lebensgestaltung betroffen ist (s.o.).

c) Vorschläge des Bundesrates

Die Vorschläge des Bundesrates sind inakzeptabel. Sie wollen auch nicht schwerwiegende Straftaten – teilweise noch nicht einmal Straftaten von erheblicher Bedeutung – in den Katalog aufnehmen, so etwa § 20 Abs. 1 Nr. 1 – 4 VereinsG. Diese Straftat ist mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bedroht, also auf unterster Stufe des strafrechtlichen Wertstufensystems. Abgesehen von ihrer Unverhältnismäßigkeit stellen solche Vorschläge die vom Regierungsentwurf zumindest teilweise angestrebte grundsätzlich sinnvolle Systematik, die die Telekommunikations-überwachung nur bei schweren Straftaten erlauben will, endgültig auf den Kopf.

Die Anmerkungen des Bundesrates zu § 100a Absatz 4 StPO-E sind verfassungsrechtlich schlicht nicht haltbar. Technisch sind die Anforderungen des Bundesverfassungsgerichts realisierbar. Wenn den Ermittlungsbehörden Technik fehlt, die die Vorgaben des höchsten Gerichts umsetzen, dann muss sie beschafft werden. Im Rahmen der Vorratsdatenspeicherung äußert der Bundesrat verwunderlicherweise keine Bedenken, dass die Anschaffung neuer Technik für die Provider oder für Behörden zu teuer wäre.

Sofern neue Technik zu beschaffen ist, kommt allenfalls eine Abfederung der Anforderungen durch eine Umsetzungsfrist in Betracht.

4. Zu § 100b StPO-E

Im Rahmen des § 100b StPO-E wäre insbesondere eine ausdrückliche Begründungspflicht für richterliche Beschlüsse und eine weitere Verbesserung der Berichtspflichten wünschenswert.

a) Richtervorbehalt (Absatz 1)

Die Feststellung, dass 22,5 % der richterlichen Beschlüsse zur Durchführung einer Telekommunikationsüberwachung nur eine „formelhafte Begründung“ enthalten und in 15 % der Fälle lediglich die „Gesetzesformel zur Begründung wiedergegeben“ wird, hingegen bloß 23,5 % der Beschlüsse als substantiell begründet gewertet werden (MPI-Studie S. S. 231; hierzu kritisch Bizer, KrimJ 2003, 280), hat in der Vergangenheit beunruhigt. So konstatiert die weitere Untersuchung von Backes und Gusy eine Erosion des Richtervorbehaltes und den „weitgehenden Verzicht der Richter selbst, die ihnen vom Gesetz aufgegebene eigenständige und grundrechtsorientierte Prüfung der staatsanwaltschaftlichen Anträge auf Telefonüberwachung vorzunehmen“ (Backes/Gusy u. a., StV 2003, 249, 252). Daher ist nicht verständlich, dass der Entwurf – außer in den Fällen der akustischen Wohnraumüberwachung, § 100d StPO-E – auf eine gesetzlich normierte Pflicht zur einzelfallbezogenen Begründung verzichten will.

b) Formale Anforderungen an richterlichen Beschluss (Absatz 2)

Nach dem neu gefassten § 100b Absatz 2 Satz 2 Nr. 1 StPO-E sind in der Anordnung künftig der Name und die Anschrift des Betroffenen nur noch „soweit möglich“ anzugeben. Diese Formulierung betrifft zwar auf den ersten Blick „nur“ die formalen Anforderungen an richterliche Beschlüsse, hat in Wirklichkeit aber eine Aufweichung in materieller Hinsicht zur Folge. Denn sie würde Maßnahmen auch gegen „Unbekannt“ erlauben und die Prüfung der Anordnungsvoraussetzungen beeinträchtigen.

c) Statistische Erhebung (Absatz 6)

Die im § 100b Abs. 5 f. StPO-E vorgesehene erweiterte statistische Erhebung über Maßnahmen der Telekommunikationsüberwachung ist grundsätzlich zu begrüßen, da sie für eine Evaluierung der Vorschriften notwendig ist. Allerdings ist die im ersten Referentenentwurf bereits erweiterungsbedürftige Vorschrift bei der Überarbeitung weiter eingeschränkt worden. War nach dem ersten Entwurf beispielsweise noch die Angabe erforderlich, ob das Verfahren Ergebnisse erbracht hat, die für das Verfahren relevant waren, so ist dieses Detail nunmehr gestrichen. Eine Berichterstattung und „Evaluierung“, die den Erfolg der Maßnahmen gänzlich unberücksichtigt lässt, kann nicht mehr als ein Feigenblatt sein.

Im Rahmen der Neuregelung böte sich an dieser Stelle die Festlegung einer Evaluierungspflicht einschließlich der einzuhaltenden Bedingungen an. Eine Evaluierung sollte regelmäßig durch eine unabhängige Stelle durchgeführt werden, nicht hingegen durch die Strafverfolgungsbehörden selbst. Zudem ist der Gesetzgeber selbst zur ständigen Beobachtung der Auswirkungen der beschlossenen Regelungen aufgefordert.

d) Vorschläge des Bundesrates

Die Aussage des Bundesrates in Nummer 6 zu § 100b Absatz 1 Satz 4 und 5 StPO-E, dass durch eine Verkürzung der Kontrollfrist eine inhaltliche Verbesserung des Grundrechtsschutzes nicht zu

erwarten sei, ist weder begründet noch belegt. Der Vergleich mit den Regelungen des Zollfahndungsdienstgesetzes berücksichtigt nicht die inhaltlichen Unterschiede zwischen den Aufgaben der Strafverfolgung und den weitergehenden Aufgaben des Zollkriminalamtes (ZKA).

Die Empfehlung des Bundesrates, § 100b Absatz 1 Satz 6 StPO-E zu streichen, ist abzulehnen. Dies würde den ohnehin bestehenden Kontroll- und Begründungsdefiziten (vgl. oben a) nicht gerecht.

Angesichts der Äußerungen zur Gerätekennung (IMEI, § 100b Absatz 2 Satz 2 Nr. 2 StPO-E) muss darauf hingewiesen werden, dass die IMEI auf Grund ihrer leichten Fälschbarkeit keine eindeutige Gerätekennung ist.

Die Pflicht der Staatsanwaltschaft, dem anordnenden Gericht über den Verlauf und die Ergebnisse der Überwachungsmaßnahme zu berichten (§ 100b Absatz 4 Satz 2 StPO-E), ist zur Realisierung einer effektiven Kontrolle der Maßnahme durch das Gericht sinnvoll und sollte beibehalten werden. Die Argumentation, das Gesetz sehe keine Erfolgsaussicht der Maßnahme als Voraussetzung vor, weshalb diese durch das anordnende Gericht auch nicht zu berücksichtigen sei, ist falsch. Eine Einbeziehung der Erfolgsausichten in die richterliche Prüfung ist unabdingbar, da eine Maßnahme ohne Erfolgsaussichten ein nicht geeigneter und damit unverhältnismäßiger Grundrechtseingriff wäre. Auch bei einer rein praktischen Betrachtung wird man wohl kaum ein polizeiliches oder staatsanwaltschaftliches Interesse an einer solchen Maßnahme annehmen dürfen. Die Einwendungen des Bundesrates gegen die im Regierungsentwurf vorgesehene sinnvolle Regelung verfangen daher nicht.

Die weiteren vom Bundesrat gewünschten Einschränkungen der Berichtspflichten sind ebenfalls abzulehnen, da sie einen Überblick über das wahre Ausmaß der Überwachung unnötig erschweren würden.

Bzgl. der vorgeschlagenen Verwendung der durch die Telekommunikationsüberwachung erlangten Erkenntnisse auch im Besteuerungsverfahren (Vorschlag Nr. 25 zu § 393 Abs. 3 neu AO-E) bestehen erhebliche Bedenken, ob dies noch verhältnismäßig sein kann.

5. Zu § 100f – Lauschangriff außerhalb von Wohnungen

Die Maßnahme ermächtigt dazu, das außerhalb von Wohnungen nichtöffentlich gesprochene Wort abzuhören und aufzuzeichnen. Die Verhältnismäßigkeit der Vorschrift steht insbesondere wegen der relativ weitgehenden Einbeziehung nicht beschuldigter Personen in Frage. Es fehlt eine Regelung zum Schutz des Kernbereichs privater Lebensgestaltung.

a) Eingriffsschwelle und Adressaten

Um als Nichtverdächtiger zum Ziel verdeckter Ermittlungsmaßnahmen zu werden, reicht nach Absatz 2 die auf Tatsachen gestützte Annahme der Strafverfolgungsbehörden aus, mit dem Beschuldigten in Verbindung zu stehen. Freunde und Bekannte des Verdächtigen können schon dann ins Visier der Richtmikrofone, Wanzen und Abhöreinrichtungen geraten, wenn die Polizei sich

aus deren Gesprächen einen Aufschluss über den Aufenthaltsort des Verdächtigen erhofft. Eine wesentlich präzisere Fassung bzw. gesetzliche Abgrenzung des Kreises der Kontakt- und Begleitpersonen wäre ebenso zu wünschen gewesen wie eine deutliche Anhebung der Eingriffsschwellen. Es ist fraglich, ob die bloße Ermittlung des Aufenthaltsorts eines Verdächtigen auch das heimliche Abhören von vertraulichen Gesprächen Nichtverdächtiger rechtfertigen kann.

b) Schutz des Kernbereichs privater Lebensgestaltung

Die Entscheidungen des Bundesverfassungsgerichts zur akustischen Wohnraumüberwachung und zur präventiven Telekommunikationsüberwachung (siehe oben 3.b) dürfen nicht als begrenzte Entscheidungen zum in Art. 13 Grundgesetz garantierten Grundrecht auf Unverletzlichkeit der Wohnung bzw. zum in Art. 10 Grundgesetz garantierten Fernmeldegeheimnis gesehen werden. Das Bundesverfassungsgericht hat die Frage des Kernbereichsschutzes vielmehr an dem für sämtliche heimliche Ermittlungsmaßnahmen zentralen Maßstab des Grundgesetzes, nämlich an der Menschenwürdegarantie – und dem damit verbundenen allgemeinen Persönlichkeitsrecht – gemessen.

Der durch Art. 1 Abs. 1 GG absolut geschützte Achtungsanspruch verbietet nicht sämtliche heimlichen Beobachtungen, es ist jedoch stets ein unantastbarer Kernbereich privater Lebensgestaltung zu wahren (BVerfG Urteil vom 03.03.2004, Abs. 118). Würde der Staat in diesen Kernbereich eindringen, verletzte dies die jedem Menschen unantastbar gewährte Freiheit zur Entfaltung in den ihn betreffenden höchstpersönlichen Angelegenheiten. Dieser Kernbereich ist *nicht relativierbar*. Das heißt: Auch überwiegende Interessen der Allgemeinheit können einen Eingriff nicht rechtfertigen.

Dabei steht der *Inhalt der Kommunikation bzw. der Interaktion* im Vordergrund, nicht der Ort der Kommunikation und auch nicht das Mittel der Kommunikation. Ein intimes Gespräch zwischen engsten Vertrauten – etwa Ehe- oder Lebenspartnern – berührt nicht nur in einer Wohnung den Kernbereich der persönlich-vertraulichen Kommunikation, sondern z. B. auch während einer gemeinsamen Autofahrt oder in einem Telefongespräch.

Auswirkungen ergeben sich daher nicht nur für die akustische Wohnraumüberwachung – den Großen Lauschangriff i.S.d. § 100c StPO, sondern daneben auch für weitere verdeckte Maßnahmen, bei denen ein Eingriff in den Kernbereich der privaten Lebensgestaltung bzw. der persönlich-vertraulichen Kommunikation möglich ist, insbesondere die hier in Rede stehende Maßnahme des Abhörens und Aufzeichnens des nicht öffentlich gesprochenen Wortes außerhalb von Wohnungen.

Dass im Ergebnis lediglich zur akustischen Wohnraumüberwachung und zur Telekommunikationsüberwachung Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung eingeführt werden, ist angesichts der klaren Ausführungen des Bundesverfassungsgerichts zur Betroffenheit der Menschenwürde bzw. zum Schutz der persönlich-vertraulichen Kommunikation unverständlich. Aus unserer Sicht ist es erforderlich, für verdeckte Maßnahmen einen *„vor die Klammer gezogenen“* Kernbereichsschutz zu regeln, so wie der Entwurf den Schutz der Zeugnisverweigerungsberechtigten – und dies wird ausdrücklich begrüßt – ebenfalls

in einer allgemeinen Regelung verankert; für den Bereich der akustischen Wohnraumüberwachung (§ 100c StPO) kann die zu schaffende Vorschrift durch eine spezielle Regelung ergänzt werden.

6. Zu §§ 100g - Verkehrsdatenabfrage

Mit der Einführung der Vorratsdatenspeicherung in Artikel 2 des Regierungsentwurfs ist noch nicht vollständig geregelt, in welchen Fällen Strafverfolgungsbehörden auf die bei den Telekommunikationsdiensteanbietern gespeicherten Daten zugreifen können. Dieser Frage widmet sich § 100g StPO-E. Aufgrund dieses Zusammenhangs kann die Verhältnismäßigkeit dieser Norm nicht ohne einen gleichzeitigen Blick auf die Vorratsdatenspeicherung beurteilt werden. Die starken Zweifel an der verfassungsrechtlichen Zulässigkeit der mit der Vorratsdatenspeicherung eingeführten Mindestspeicherfristen (dazu unten II.) wirken sich auf die in § 100 g StPO-E geregelte Verkehrsdatenspeicherung aus. Neben der Verletzung dieser verfassungsrechtlichen Grenzen überschreitet die Ausgestaltung des § 100g StPO-E den rechtlichen Rahmen dadurch, dass die durch die Richtlinie festgelegten Vorgaben beachtet werden. Das Ziel einer möglichst grundrechtsschonenden Umsetzung der EU-Richtlinie wird verfehlt.

a) Eingriffsschwelle

Die Richtlinie sieht vor, dass die aufgrund dieser Speicherungsverpflichtung vorgehaltenen Daten nur zur „Ermittlung, Feststellung und Verfolgung von *schweren Straftaten*“ eingesetzt werden dürfen. Diese Eingrenzung beachtet der Entwurf nicht.

Die Eingriffsschwelle der „schweren Straftat“ verwendet der Entwurf lediglich im Rahmen der Telekommunikationsüberwachung nach § 100a StPO-E (siehe oben 3.a.), nicht jedoch für den strafprozessualen Zugriff auf die gespeicherten Vorratsdaten, also die Verkehrsdatenabfrage nach § 100g StPO-E. Diese geplante Vorschrift setzt in Absatz 1 Nr. 1 lediglich den auf Tatsachen gestützten Verdacht einer *„Straftat von erheblicher Bedeutung“* voraus. Zutreffend grenzt die Entwurfsbegründung zu § 100a StPO-E in Anlehnung an die bisherige Rechtsprechung den Begriff der „schweren Straftat“ vom Begriff der „Straftat von erheblicher Bedeutung“ und dem der „besonders schweren Straftat“ ab. Der Begriff der „schweren Straftat“ nimmt zwischen diesen – so die Begründung ausdrücklich – eine Zwischenstellung ein (BR-Drs. 275/07, S. 86 f.). Abweichend hiervon versucht die Begründung zu § 100g StPO-E den durch die Richtlinie verwendeten Begriff der „schweren Straftat“ mit dem Begriff der „Straftat von erheblicher Bedeutung“ gleichzusetzen (S. 118 f.). Dies führt dazu, dass derselbe Begriff unterschiedlich ausgelegt und verstanden wird bzw. werden kann. Durch diese Inkonsistenz bleibt nicht nur die Rechtsklarheit auf der Strecke, sondern auch die möglichst grundrechtsfreundliche Umsetzung der Richtlinie. Der Grundsatz der Verhältnismäßigkeit zwingt dazu, die Eingriffsschwelle höher anzusetzen. Dies gilt auch für die Auslegung des Begriffs der „schweren Straftat“ im europäischen Kontext, da auch hier die Verhältnismäßigkeit Geltung beansprucht. Zu beachten ist unter anderem, dass durch die Vorrats-datenspeicherung für im Ergebnis unschuldige Bürgerinnen und Bürger die Wahrscheinlichkeit steigt, Gegenstand eines strafrechtlichen Ermittlungsverfahrens zu werden. Zur Durchführung der Strafverfolgungsmaßnahmen genügen tatsachengestützte Verdachtsmomente; bei informationellen

Eingriffen in Telekommunikationsvorgänge sind regelmäßig auch unbeteiligte Dritte betroffen. Zudem darf der Beweiswert etwa einer IP-Adresse nicht überschätzt werden: Bereits durch einen fehlerhaften Zeitstempel eines Servers bei einem Inhalteanbieter können leicht falsche Verdachtsmomente entstehen. Damit hält sich § 100g Absatz 1 Nr. 1 StPO-E nicht im Rahmen der Richtlinienvorgabe; die verfassungsrechtlich allenfalls denkbare grundrechtsschonendste Umsetzung der Richtlinie wird nicht erreicht.

Noch eklatanter verstößt die Regelung in § 100a Absatz 1 Nr. 2 StPO-E gegen Verfassungsrecht, die beim Verdacht einer „mittels Telekommunikation" begangenen Straftat die Verkehrsdatenabfrage ermöglichen will (Absatz 1 Nr. 2). Der Gesetzentwurf fordert nicht, dass diese Delikte schwere Straftaten bzw. Straftaten von erheblicher Bedeutung sein müssen und entfernt sich damit vollends von den Vorgaben der Richtlinie und von den Anforderungen des Verhältnismäßigkeitsgrundsatzes.

b) Dynamische IP-Adressen

Einen noch weitergehenden Schritt macht der Gesetzesentwurf im Hinblick auf die Herausgabe *dynamischer IP-Adressen,* die in Zukunft praktisch voraussetzungslos möglich sein wird. Die Entwurfsbegründung stuft dynamische IP-Adressen pauschal als sog. Bestandsdatum ein (BR-Drs. 275/07, S. 53 f.) Damit werden diese datenschutzrechtlich in die Nähe von einfachen Telefonbucheinträgen gerückt. Eine Abfrage bedarf dann nicht mehr der Voraussetzungen des § 100g StPO-E, sondern ist nach § 113 TKG möglich und kann z.B. zur Aufklärung von Ordnungswidrigkeiten eingesetzt werden. Dies wird der Sensibilität dieser Datenart nicht gerecht. Dass die IP-Adresse dem Schutz des Telekommunikationsgeheimnisses in gleicher Weise unterliegt wie andere Verkehrsdaten, hat u. a. der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zuletzt in seiner Stellungnahme Regierungsentwurf eines „Gesetzes zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums" (BT-Drs. 16/5048) zutreffend dargelegt (S. 2 f). Die Aussagen des Bundesbeauftragten in dieser Stellungnahme machen wir uns zu eigen.

Die IP-Adresse wird in der Praxis von vielen Internetanbietern – entgegen der Gesetzeslage – „mitgeloggt". Erhalten die Behörden Zugriff auf Logdateien, so lassen sich umfassende Interessenprofile des Betroffenen abbilden. So lässt sich etwa bei einem Besuch einer Online-Zeitung genau nachvollziehen, für welche Zeitungsartikel er sich interessiert hat. Verknüpft man die Log-Dateien verschiedener Anbieter, lässt sich mit Hilfe der Vorratsdatenspeicherung ein umfassendes Persönlichkeitsbild erstellen. Hierauf soll nach der Gesetzesbegründung – abgesehen vom einfachen Tatverdacht, der sehr leicht gegeben sein kann – ohne jede Eingriffsschwelle zugegriffen werden können. Ein Richtervorbehalt besteht in diesem Falle ebenfalls nicht.

b) Zielwahlsuche, Funkzellenabfrage und Auskunft in Echtzeit

Deutlich abgesenkt werden durch die neue Fassung des § 100g StPO-E die Voraussetzungen für die so genannte *Zielwahlsuche*, die eine Vielzahl unbeteiligter Personen erfasst. Auch die so genannte *Funkzellenabfrage* wird nur rudimentär mit wenigen Worten im Rahmen der allgemeinen Verkehrsdatenerhebung erwähnt. Hierbei handelt es sich um einen tief greifenden

Grundrechtseingriff, der in erster Linie unverdächtige Bürgerinnen und Bürger betrifft, die durch ihr Verhalten keinen Anlass für strafrechtliche Ermittlungseingriffe gegeben haben (s. hierzu 28. Tätigkeitsbericht des ULD 2006, Ziff. 4.3.2). Die weitgehende Regelung ohne Begrenzung auf schwere Straftaten ist unverhältnismäßig. Nicht nachzuvollziehen ist, weshalb das Gesetz auf eine Regelung des Umgangs mit den erlangten Daten vollständig verzichtet. Zu begrüßen ist aber, dass zumindest die Begründung des Entwurfs auf die in Schleswig-Holstein gesammelten Erfahrungen zurückgreift und klarstellt, dass sich die Maßnahme nur gegen die oder den Beschuldigten oder dessen Nachrichtenmittler richten darf. Eine „Generierung von Zeugen“ ist und bleibt unzulässig.

Beispiel für eine kleine Veränderung mit großer Wirkung ist der Verzicht auf das Tatbestandsmerkmal *„im Falle einer Verbindung“*. Dies führt dazu, dass in Zukunft die Erhebung von Standortdaten bei Mobiltelefonen in Echtzeit für zulässig erklärt wird. Damit können die Strafverfolgungsbehörden in Zukunft Bewegungsbilder einer Person in Echtzeit erstellen. Dies zeigt die besondere Eingriffsintensität der Vorschrift zur Verkehrsdatenabfrage. War diese im ersten Referentenentwurf noch auf Straftaten i.S.d. § 100a Abs. 2 StPO-E begrenzt, soll sie nach dem aktuellen Entwurf der Bundesregierung ausdrücklich schon bei Straftaten von erheblicher Bedeutung i.S.d. § 100g Abs. 1 Nr. 1 StPO möglich sein.

c) Vorschläge des Bundesrates

Die nochmalige Erweiterung der Funkzellenabfrage ist schon aus den oben angesprochenen Gründen abzulehnen. Die Vorschläge des Bundesrates würden die Defizite der Regelung nochmals erweitern. Die vorgeschlagenen Einschränkungen der Berichtspflichten sind angesichts der Belastungen für die Grundrechtsträger nicht hinnehmbar. Die Intensität der Belastungen wird durch die geplante Vorratsdatenspeicherung erheblich gesteigert. Dagegen – wie der Bundesrat – einseitig die „Belastung“ für die Praxis in den Mittelpunkt zu stellen, wird dieser Grundrechtsbeeinträchtigung nicht gerecht. Insgesamt scheint dem Bundesrat eine rechtstatsächliche Untersuchung der Arbeit nur von untergeordneter Bedeutung zu sein. Dabei ist diese nicht nur zur Herstellung eines effektiven Grundrechtsschutzes notwendig, sondern auch zur Verbesserung einer effektiven Arbeit der Ermittlungsbehörden.

Das Votum des Bundesrates gegen eine Veröffentlichungspflicht der statistischen Daten im Internet ist verwunderlich – dient doch die Veröffentlichung dazu, eine im demokratischen Gemeinwesen notwendige öffentliche Diskussion über Gesetzesfolgen zu unterstützen und zu ermöglichen.

7. Zu § 100h – Bildaufnahmen und Einsatz technischer Mittel

Bezüglich Eingriffsschwellen und Kernbereichsschutz gilt das zu § 100 f StPO-E Gesagte sinngemäß.

8. Zu § 100i StPO-E – IMSI-Catcher

Der vorliegende Entwurf erweitert die Möglichkeiten des Einsatzes des sog. IMSI-Catchers. Der Einsatz dieses Gerätes war bislang nur bei Katalogtaten vorgesehen, die auch eine

Telekommunikationsüberwachung rechtfertigen. Darüber hinaus sollte die Maßnahme nach der ersten Entwurfsfassung lediglich dazu dienen, eine Maßnahme nach § 100a StPO vorzubereiten oder eine Festnahme zu ermöglichen. Nunmehr soll die Maßnahme auch bei Straftaten von im Einzelfall erheblicher Bedeutung möglich sein, soweit sie „für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich ist."

Diese Erweiterung ist abzulehnen; ihre Notwendigkeit ist nicht dargetan. Zudem ist ihre Verhältnismäßigkeit zweifelhaft. Das Bundesverfassungsgericht hat zwar in seiner Entscheidung vom 22. August 2006 (2 BvR 1345/03 = NJW 2007, 351) die bisherige Regelung nicht aufgehoben, es hat jedoch in diesem Zusammenhang vor einer Erweiterung der heimlichen Ermittlungsmaßnahmen gewarnt (S. 356 a.E.). Vor diesem Hintergrund sollte die mit dem Regierungsentwurf verfolgte Erweiterung nochmals überdacht werden. Sofern am Einsatz des IMSI-Catchers festgehalten werden soll, wäre die im ersten Referentenentwurf enthaltene Fassung des § 100i StPO-E zu bevorzugen.

9. Zu § 101 – Benachrichtigungspflichten und Rechtsschutz

Die Beschäftigung des Entwurfs mit einer Vereinheitlichung der Benachrichtigungspflichten für alle verdeckten Ermittlungsmaßnahmen ist im Grundsatz zu begrüßen, allerdings bedarf die konkrete Umsetzung im Interesse eines wirksamen Schutzes der informationellen Selbstbestimmung der Betroffenen erheblicher Nachbesserungen.

Für den Bereich der verdeckten Ermittlungsmaßnahmen in Strafverfahren hat das Bundesverfassungsgericht die grundsätzliche Notwendigkeit einer Information der Betroffenen hervorgehoben, so insbesondere in den Fällen einer Telekommunikationsüberwachung (u. a. BVerfG 100, 313, 361) oder einer akustischen Wohnraumüberwachung (BVerfG Urteil vom 03.03.2004, Abs. Nr. 290 ff).

> *„Art. 10 GG vermittelt den Grundrechtsträgern ferner Anspruch auf Kenntnis von Maßnahmen der Fernmeldeüberwachung, die sie betroffen haben. Das ist ein Erfordernis effektiven Grundrechtsschutzes. Denn ohne eine solche Kenntnis können die Betroffenen weder die Unrechtmäßigkeit der Erfassung und Kenntnisnahme ihrer Fernmeldekontakte, noch etwaige Rechte auf Löschung oder Berichtigung geltend machen. Dieser Anspruch verengt sich nicht sogleich auf den gerichtlichen Rechtsschutz aus Art. 19 Abs. 4 GG. Zunächst handelt es sich vielmehr um ein spezifisches Datenschutzrecht, das gegenüber der informations- und datenverarbeitenden staatlichen Stelle geltend gemacht werden kann." (BVerfGE 100, 313, 361)*

Damit ist der zu überarbeitende § 101 StPO Ausfluss der Verpflichtung, den Grundrechtsträgern zum Schutz ihres Grundrechts umfassende Benachrichtigung und Auskunft zu gewährleisten. Ebenfalls dient § 101 StPO der Möglichkeit für die Betroffenen, eine gerichtliche Überprüfung von Maßnahmen einzufordern.

Allerdings ist die Benachrichtigung der Betroffenen in der Praxis – auch soweit § 101 bereits jetzt rechtliche Verpflichtungen regelt – leider keine Selbstverständlichkeit. Rechtstatsächliche Untersuchungen belegen, dass die Frage der Benachrichtigung in der Praxis oftmals stiefmütterlich behandelt wird. So weist etwa die MPI-Studie nach, dass die Praxis der Benachrichtigung von erheblichen Defiziten gekennzeichnet ist (S. 276 ff). Die Studie stellt insbesondere fest, dass eine ausdrückliche Beschäftigung mit der Frage der Benachrichtigung den Verfahrensakten nur für ein Drittel der überwachten Anschlüsse zu entnehmen war. Lediglich in etwa 15% aller Anschlüsse ist eine Benachrichtigung der Anschlussinhaber erfolgt, in knapp 12% der Fälle lag eine sonstige Kenntniserlangung im weiteren Verlauf des Ermittlungsverfahrens vor, insbesondere durch Akteneinsichtnahme. Ausdrücklich nicht benachrichtigt wurde, bezogen auf private Festnetz- und Mobilanschlüsse, jeweils in 44% der Fälle. Besonders erschreckend sind diese Zahlen, wenn man bedenkt, dass lediglich in 38% der Fälle Anschlussinhaber und Anschlussnutzer bei einer Telekommunikationsüberwachung auch Beschuldigte des Verfahrens waren (S. 289). Damit besteht ein Defizit der Benachrichtigung gerade im Hinblick auf solche Personen, die als Unverdächtige betroffen sind und die im weiteren Verlauf des Verfahrens keine Kenntnis von der Maßnahme erhalten werden, etwa durch Akteneinsicht. Insgesamt kommt die Studie zu dem Ergebnis, dass die Benachrichtigungen somit nicht in dem Umfang und unter den Erwägungen erfolgen, die das Gesetz in § 101 StPO verlangt. (Zur grundsätzlichen Problematik auch der nachträglichen Beauskunftung siehe zudem 29. TB ULD, 4.2.2)

Diese Praxisdefizite zu beseitigen, ist eine Aufgabe der hier besprochenen Überarbeitung der Strafprozessordnung.

a) Absätze 4 - 7

Die geplante Neuregelung der **Benachrichtigungspflichten** in § 101 Abs. 4-7 StPO-E wird nur wenig dazu beitragen diese Praxisdefizite zu beseitigen. Die Vorschrift spricht bei den zu benachrichtigenden Personen in Nr. 4b von „sonstigen überwachten Personen“ und in Nr. 5 ff von „erheblich mit betroffenen Personen“. Diese Begriffe sind unklar, ebenso wie die zu weit gefassten Formulierungen, nach denen von einer Benachrichtigung abgesehen werden kann. Zu benachrichtigen sind von Verfassung wegen sämtliche Personen, die in irgendeiner Weise durch die Überwachungsmaßnahme betroffen worden sind, in deren Grundrechte also eingegriffen worden ist. Die Benachrichtigungspflicht ist die Grundlage für die Möglichkeit der Betroffenen, die Rechtmäßigkeit der Maßnahme durch ein Gericht überprüfen lassen. Wer nicht weiß, ob eine Maßnahme gegen ihn durchgeführt wurde, hat keinerlei Möglichkeit, sich vor Gericht gegen eine ungerechtfertigte Datenverarbeitung zur Wehr zu setzen und etwa Berichtigung, Löschung oder Sperrung zu verlangen. Die Garantie, dass jeder die Gerichte anrufen kann, wenn er sich durch die öffentliche Gewalt in seinen Rechten verletzt fühlt, würde ohne Auskunft und Benachrichtigung ins Leere führen. Benachrichtigung und Auskunft sind also direkter Ausfluss der Rechtsweggarantie in Artikel 19 Abs. 4 des Grundgesetzes, die nur in äußerst eng begrenzten Ausnahmefällen Einschränkungen zulässt (s. o.).

Die Formulierung, nach der die Benachrichtigung unterbleibt, wenn eine Person „nur unerheblich betroffen wurde und anzunehmen ist, dass sie kein Interesse an einer Benachrichtigung hat“, ist zu verschwommen. Sie wird zu einem Leerlaufen der Benachrichtigung führen und die oben angesprochenen erheblichen Praxisdefizite verstärken.

Abzulehnen ist darüber hinaus, dass beim Einsatz verdeckter Ermittler die Verschiebung der Benachrichtigung auch dann zulässig sein soll, wenn sonst der weitere Einsatz des Ermittlers gefährdet werden kann (Absatz 5). Das Bundesverfassungsgericht hat beim Lauschangriff eine solche Einschränkung für verfassungswidrig erklärt. Nicht nachvollziehbar ist weiterhin, aus welchem Grund mit einer Benachrichtigung bis zu 12 Monate gewartet werden kann, ehe ein Gericht eingeschaltet werden muss. Eine länger als sechs Monate andauernde Frist ist nicht gerechtfertigt. Verfassungsrechtlich äußerst bedenklich ist schließlich das Ende der Benachrichtigungspflicht nach fünf Jahren, wie § 101 Abs. 7 StPO-E dies vorsieht. Es ist in aller Deutlichkeit hervorzuheben: Die *Strafverfolgungsbehörden dürfen nicht zu Geheimdiensten gemacht werden*, indem ihnen eine dauerhafte Heimlichkeit ihrer Maßnahmen zugebilligt wird. Jede Bürgerin und jeder Bürger hat nach Abschluss der Maßnahmen – spätestens nach Abschluss der Ermittlungen – einen Anspruch auf vollständige Transparenz. Einschränkungen sind nur zum Schutz höchstrangiger Rechtsgüter zulässig, etwa bei Gefahr für Leib, Leben oder Freiheit einer Person.

b) Absatz 9

Sehr zu begrüßen ist, dass die Möglichkeit des **Rechtsschutzes** gegen verdeckte Ermittlungsmaßnahmen nunmehr ausdrücklich geregelt werden soll (§ 101 Abs. 9 StPO-E). Die *Frist von 14 Tagen* für den Antrag auf Überprüfung der Rechtmäßigkeit der Maßnahme erscheint allerdings als *zu kurz*. Die Benachrichtigung dürfte für die Betroffenen in der Regel äußerst überraschend kommen. Anders als im laufenden gerichtlichen Verfahren hatten die Betroffenen daher in der Regel zunächst keine Gelegenheit, sich anwaltlich beraten zu lassen oder einen Verteidiger zu suchen. Viele Betroffene, denen oft jede juristische Vorbildung fehlt, dürften mit einer solch kurzen Frist überfordert sein.

B. Artikel 2 – Vorratsdatenspeicherung

Die Vorratsdatenspeicherung verstößt formell und materiell gegen Europäisches Recht und ist als unverhältnismäßiger Eingriff in die Grundrechte aller (!) Bürgerinnen und Bürger nicht mit dem Grundgesetz vereinbar.

Darüber hinaus soll die Richtlinie 2006/24/EG vom 15. März 2006 der Harmonisierung der Pflichten für Diensteanbieter bzw. Netzbetreiber im Zusammenhang mit der Vorratsspeicherung dienen (Erwägungsgrund 21). Aus diesem Grunde darf der Regelungsgehalt der Richtlinie nicht überschritten werden. Bereits dieses „Minimalziel“ ist nicht erreicht, da die Regelungen über die Anforderungen der Richtlinie hinausgehen.

1. Zu § 113a – „Kernregelung“ der Vorratsdatenspeicherung

„Kernregelung“ der geplanten Vorratsdatenspeicherung – so die Entwurfsbegründung – ist § 113a TKG-E, der Voraussetzungen und Umfang der Speicherungspflichten bestimmt. Die damit verfolgte Einführung einer verdachtsunabhängigen Vorratsdatenspeicherung verstößt gegen Verfassungsrecht. Darüber hinaus ist die Richtlinie erheblichen europarechtlichen Bedenken ausgesetzt.

a) Europarechtliche Wirksamkeit der Richtlinie

Die EG-Richtlinie zur Vorratsdatenspeicherung selbst ist erheblichen europarechtlichen Bedenken ausgesetzt, weil sie auf einer falschen Rechtsgrundlage erlassen worden ist. Die Richtlinie stützt sich auf Art. 95 EGV mit der Begründung, sie diene der Angleichung von Rechts- und Verwaltungsvorschriften zur Verbesserung des Binnenmarktes. Art. 95 EGV ist jedoch keine ausreichende Rechtsgrundlage für eine Maßnahme, die als Rahmenbeschluss der justiziellen Zusammenarbeit in der sog. „dritten Säule“ hätten beschlossen werden müssen. Dieser Meinung war ursprünglich auch die Kommission, weil die Vorratsdatenspeicherung ausschließlich für Zwecke der Strafverfolgung erfolgen sollte (siehe Art. 1 Abs. 1). Die Kommission änderte ihre Meinung, als die erforderliche Einstimmigkeit im Rat für einen solchen Rahmenbeschluss nicht erreicht werden konnte (siehe auch Gutachten des Wiss. Dienstes des Dt. Bundestages, a.a.O., S. 8). Nach der jüngsten Entscheidung des EuGH vom 30. Mai 2006 sind die europarechtlichen Zweifel erheblich gestiegen, denn das Gericht hat die ebenfalls auf Art. 95 basierende Regelung der Weitergabe von Flugdaten in die USA, die gleichfalls aus justiziellen Gründen erfolgt, wegen der falschen Wahl der Rechtsgrundlage für nichtig erklärt (NJW 2006, 88). Der Deutsche Bundestag teilt die Bedenken, dass Art. 95 die falsche Rechtsgrundlage für die Verpflichtung zur Vorratsspeicherung ist (BT-Drs. 16/545, S. 3).

Schon vor diesem Hintergrund sollte zunächst auf eine Umsetzung verzichtet und der Ausgang des bereits anhängigen gerichtlichen Verfahrens abgewartet werden.

b) Verfassungsverstoß

Die durch diese Vorschrift eingefügte Verpflichtung zur Vorratsdatenspeicherung verstößt gegen das national durch Art. 10 GG sowie europarechtlich durch Art. 8 EMRK geschützte Fernmeldegeheimnis und gegen das Verbot der Speicherung „nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken“ (BVerfGE 65, 1, 47). Dieses Verbot der Vorratsdatenspeicherung hat das Bundesverfassungsgericht für den Bereich der Telekommunikation (BVerfGE 100, 313, 360) und jüngst in der Entscheidung zur Einschränkung der Rasterfahndung bestätigt (BVerfG NJW 2006, 1939). Die Zwecke der Vorratsdatenspeicherung sind unbestimmt, weil die Verkehrs- und Standortdaten aller Teilnehmer und Netze öffentlicher elektronischer Kommunikationsdienste pauschal und ohne jeden konkreten Anhaltspunkt für eine konkrete Straftat der betroffenen Personen gespeichert werden.

Die Einbeziehung aller Kommunikationsteilnehmer qualifiziert die Vorratsdatenspeicherung als eine Maßnahme mit einer außerordentlich hohen Eingriffsintensität (vgl. BVerfG, Beschluss vom 4.

April 2006). Das Bundesverfassungsgericht hat bei Maßnahmen mit einer hohen Streubreite auf die gesamtgesellschaftliche Bedeutung des Schutzes der Vertraulichkeit der Telekommunikation verwiesen. Es gefährdet die Unbefangenheit der Nutzung der Telekommunikation und in der Folge die Qualität der Kommunikation einer Gesellschaft, wenn die Maßnahmen dazu beitragen, dass die Risiken des Missbrauches und ein Gefühl des Überwachtwerdens entstehen (BVerfGE 107, 299, 328). Für die Vorratsdatenspeicherung gilt dies erst recht, weil es sich um einen Grundrechtseingriff mit maximaler Streubreite handelt, durch den alle Teilnehmer und Nutzer der elektronischen Kommunikation erfasst werden.

Die Vorratsdatenspeicherung ist unverhältnismäßig und damit verfassungswidrig, weil sie die Speicherung von Verkehrs- und Standortdaten aller Kommunikationsteilnehmer ohne jeden Verdacht anordnet. Nach dem Grundsatz der Verhältnismäßigkeit dürfen intensive Grundrechtseingriffe erst von bestimmten Verdachts- oder Gefahrenstufen an vorgesehen werden (vgl. BVerfGE 100, 313, 383 f.; 109, 279, 350 ff.). Grundrechtseingreifende Maßnahmen „ins Blaue hinein“ sind unzulässig (vgl. BVerfGE 112, 284, 297, Beschluss vom 4. April 2006). Verfassungswidrig sind Maßnahmen, bei denen die Betroffenen keinerlei Nähe zu der abzuwehrenden Gefahr aufweisen (Beschluss vom 4. April 2006). Dies ist bei der Vorratsdatenspeicherung der Fall, weil sie ausnahmslos alle Teilnehmer öffentlicher elektronischer Kommunikationsdienste ohne jede begrenzende Anforderungen an die Wahrscheinlichkeit eines Gefahreneintritts erfasst.

Die Vorratsdatenspeicherung ist verfassungswidrig, weil sie nicht erforderlich ist. Ein milderes und geeignetes Mittel wäre die gesetzliche Regelung eines so genannten Quick Freeze. Mit einer solchen Regelung können die Strafverfolgungsbehörden ermächtigt werden, in einem konkreten Verdachtsfall die zeitlich begrenzte Speicherung bestimmter Kommunikationsbeziehungen anzuordnen. Auf diese Weise wird die Speicherung auf konkrete Anlässe verfassungskonform beschränkt, ohne eine wirksame Strafverfolgung zu behindern. Vorschläge in diese Richtung sind von den Datenschutzbeauftragten des Bundes und der Länder bereits mehrfach unterbreitet worden. Der Gesetzgeber hat mit § 16b Wertpapierhandelsgesetz eine solche Regelung u. a. zur Bekämpfung des Insiderhandels an Börsen bereits erlassen.

Die Vorratsdatenspeicherung ist unverhältnismäßig, weil der Aufwand in keinem Verhältnis zu ihrem Ertrag steht. Erfasst werden von der Vorratsdatenspeicherung alle Teilnehmer und Nutzer der elektronischen Kommunikation, ohne einen konkreten Anlass geboten zu haben. Es handelt sich für einen Zeitraum von 6 Monaten um mehrere Milliarden Datensätze. Nach Feststellungen des Bundesverfassungsgerichts waren es 2002 alleine bei der Deutschen Telekom und nur bezogen auf die Sprachtelefonie täglich 216 Mio. Datensätze (BVerfGE 107, 299, 327). Hinzu kommen die Datensätze der anderen Telefonanbieter sowie die Verkehrsdaten der Internetanbieter. Nach Feststellungen des Industrieverbandes BITKOM würde die Erfassung der Verkehrsdaten eines größeren Internetproviders eine Datenmenge von 20- bis 40.000 Terabytes pro Jahr umfassen. Eine Menge von 40.000 Terabytes entspricht ungefähr rund 40 km gefüllter Aktenordner. Zudem verdoppelt sich laut BITKOM der Internetverkehr in Deutschland alle 14 Monate (Bitkom, Stellungnahme vom 14. 9. 2004, S. 6). Nach einer unveröffentlichten Untersuchung des

Bundeskriminalamtes wurden für den Zeitraum vom 1. April bis zum 30. September 2005 insgesamt jedoch nur 381 Fälle gemeldet, in denen eine längere Speicherdauer den Ermittler nach eigenen Angaben geholfen hätte. Nur 2 Fälle betrafen Straftaten aus dem Bereich der organisierten oder terroristischen Kriminalität nach § 129a, § 129b StPO (BKA, Mindestspeicherungsfristen für Telekommunikationsverkehrsdaten, 15.11.2005).

Die Vorratsdatenspeicherung begegnet auch wegen der Dauer der Speicherung von 6 Monaten erheblichen verfassungsrechtlichen Vorbehalten. Nach schwedischen und britischen Erkenntnissen beziehen sich die Datenabfragen der Sicherheitsbehörden zu 80 bis 85% auf einen Zeitraum der letzten drei Monate, nicht aber auf längere Zeiträume (Gutachten des Wiss. Dienstes des Deutschen Bundestages vom 3. August 2006, S. 13). Diese Aussage stützt sich auf eine von dem Industrieverband BITKOM in Auftrag gegebene Studie, wonach in den Staaten, die bereits eine Vorratsdatenspeicherung erlassen haben, von den Sicherheitsbehörden Daten in der Regel nur aus Zeiträumen angefragt werden, die bis zu 3 Monate zurückliegen. Eine Vorratsdatenspeicherung über einen Zeitraum von 6 Monaten ist demnach nicht erforderlich. Diese Erkenntnis zeigt zugleich, dass die der Vorratsdatenspeicherung zugrunde liegenden rechtstatsächlichen Annahmen offensichtlich noch einer unabhängigen Überprüfung und Bewertung bedürfen.

Die Vorratsdatenspeicherung begegnet verfassungsrechtlichen Bedenken, weil die massenhafte Speicherung von Verkehrs- und Standortdaten das Risiko eines Datenmissbrauches deutlich erhöht. Der Grundsatz der Erforderlichkeit, der auch Grundlage des Gebotes der Datensparsamkeit und -vermeidung ist, beschränkt die Datenspeicherung auf das nach Art, Umfang und Dauer für die Abwicklung der betrieblichen Zwecke notwendige Maß. Durch die Verpflichtung zur Löschung der Verkehrs- und Standortdaten werden gleichzeitig Gesetzesverstöße präventiv verhindert. Die Verpflichtung zur Vorratsdatenspeicherung bewirkt demgegenüber eine deutliche Risikoerhöhung, weil nun Verkehrs- und Standortdaten über längere Zeiträume entgegen den gesetzlichen Regelungen bspw. für die Auswertung für Kundenprofile zur Verfügung stehen. Der aktuelle italienische Telefonskandal – dort konnte durch interne Sicherheitsmaßnahmen nicht wirksam verhindert werden, dass ehemalige Mitarbeiter über längere Zeiträume zahlreiche Telefongespräche gezielt abhören konnten – belegt die erhebliche Verletzlichkeit der Telekommunikation gegen interne, aber auch externe Angriffe und damit die Risiken eines unzureichenden Datenschutzmanagements. Besorgnis erregend ist, dass die Angriffe nicht durch interne Sicherheitsmaßnahmen, sondern erst durch Hinweise eines Tatbeteiligten aufgedeckt werden konnten. Der Entwurf gibt nicht zu erkennen, durch welche zusätzlichen Maßnahmen er zum Schutz der auf Vorrat gespeicherten Daten ein wirksames präventives Datenschutzmanagement gewährleisten will. Die Regelung in § 113b Absatz 10 TKG-E bietet jedenfalls keine nennenswerte Verbesserung im Sinne eines solchen Konzeptes.

c) Einzelregelungen

Nach dem im Referentenentwurf eingefügten Absatz 6 sollen laut Entwurfsbegründung (S. 167) offenbar Betreiber von **Anonymisierungsdiensten** von der Speicherungsverpflichtung umfasst sein.

Die Unverhältnismäßigkeit des zu speichernden Datenkatalogs wurde bereits oben (b.) dargelegt. Besonders ins Auge fällt die Regelung in Absatz 6, die ein faktisches Verbot der Anonymisierungsdienste schaffen soll.

Anonymisierungsdienste sind ein wichtiges Mittel des Selbstschutzes der Bürgerinnen und Bürger, ihre informationelle Selbstbestimmung bei der Nutzung von Telemediendiensten zu wahren. Die gesetzlich geforderte grundsätzlich anonyme Nutzung von Websites könnte zwar heutzutage von Providern dadurch recht einfach unterstützt werden, dass auf dem Webserver IP-Adressen und andere Daten gar nicht erst protokolliert oder nach wenigen Stunden gelöscht werden. Auch eine Pseudonymisierung der (Log-)Daten wäre mit einfachen technischen Mitteln möglich. Dies wird jedoch nach Erfahrung des ULD häufig nicht praktiziert (siehe auch zur Suchmaschine „google“ u.a.; http://www.heise.de/newsticker/meldung/91570). Stattdessen wird die Standardfunktionalität der Webserver zur längerfristigen Protokollierung der Zugriffe beibehalten. Einige kommerzielle Anbieter von sog. „Hosting“ sehen das Abschalten der Protokollierung selbst dann nicht vor, wenn es der Kunde wünscht. Darüber hinaus werden die Daten häufig zu weiteren Zwecken wie Werbung ausgewertet. Es wird somit derzeit nach der Erfahrung des ULD massenhaft gegen § 13 Abs. 6 bzw. § 15 Abs. 1 TMG verstoßen. Daneben schützt etwa der Anonymisierungsdienst AN.ON vor dem Ausforschen des Surfverhaltens durch Dritte – einschließlich der Provider des Internet-Zugangs oder der Betreiber der einzelnen Komponenten des Anonymisierungsdienstes selbst. Dies schützt das Recht der Bürger auf informationelle Selbstbestimmung ebenso wie die Firmenkommunikation vor Wirtschaftsspionage, z.B. durch fremde Geheimdienste. Die Bürgerinnen und Bürger sind auf die durch Anonymisierungsdienste gegebenen Möglichkeiten angewiesen, um ihr „Recht auf Anonymität“ selbst durchzusetzen.

Nach der Richtlinie über die Vorratsdatenspeicherung müssen Telekommunikationsanbieter künftig solche Verbindungs- und Standortdaten vorhalten, die bei der Abwicklung von Diensten wie Telefonie, SMS, E-Mail, Voice over IP oder Internetzugang anfallen. Nach Art. 1 Abs. 2 der Richtlinie gilt diese Pflicht „für Verkehrs- und Standortdaten […] sowie für alle in Zusammenhang stehenden Daten, die zur Feststellung des Teilnehmers oder registrierten Benutzers erforderlich sind“. Art. 5 der Richtlinie erwähnt Datenkategorien, die (nur) folgende Bereiche betreffen: „Telefonnetz und Mobilfunknetz“ sowie „Internetzugang, Internet-E-Mail und Internet-Telefonie“. Ob damit auch Anonymisierungsdienste erfasst werden, ist zweifelhaft. Sie unter „Internetzugang“ zu subsumieren, ist zu weitgehend. Gegebenenfalls könnten Anonymisierungsdienste in der Pflicht sein, wenn über sie E-Mail oder Internet-Telefonie betrieben wird. Dies ist jedoch etwa beim AN.ON-Dienst nicht der Fall. Insofern geht eine Regelung, die Anonymisierungsdienste erfassen würde, bereits über die Vorgaben der Richtlinie hinaus.

Dem recht unbestimmt formulierten Wortlaut und der Systematik des § 113 Absatz 6 TKG-E ist außerdem nicht zu entnehmen, dass Anonymisierungsdienste unter diese Vorschrift fallen sollen.

Dies gilt schon deshalb, weil Anonymisierungsdienste – anders als die Entwurfsbegründung annimmt – regelmäßig keine Telekommunikationsdienste sind. Beispielsweise handelt es sich beim AN.ON-Dienst um ein Telemedium (bis 28.02.2007 nach altem Recht Teledienst). Telemedien sind

nach § 1 Abs. 1 Satz 1 TMG „alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 des Telekommunikationsgesetzes, die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, telekommunikationsgestützte Dienste nach § 3 Nr. 25 des Telekommunikationsgesetzes […] sind“. Telekommunikationsdienste sind hingegen nach § 3 Nr. 24 Telekommunikationsgesetz (TKG) „in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen“. Beispiele hierfür sind neben der Telefonie die Vermittlung des Zugangs zum Internet, wie auch Email-Dienste. „Telekommunikationsgestützte Dienste“ sind nach § 3 Nr. 25 TKG „Dienste, die keinen räumlichen und zeitlich trennbaren Leistungsfluss auslösen, sondern bei denen die Inhaltsleistung noch während der Telekommunikationsverbindung erfüllt wird“. Beispiele hierfür sind insbesondere Mehrwertdienste, die über Nummerngassen wie 0900 oder 0800 erbracht werden. Grob kann man sagen, dass Telekommunikationsdienste der technischen Übermittlung von Daten (z.B. IP-Paketen) dienen. Telemedien beziehen sich auf die Inhaltsebene (z.B. Webseiten).

Dem AN.ON-Dienst liegt zwar eine Übertragung von Signalen zugrunde. *Die Verschlüsselung der Inhalte und die Tarnung der IP-Adresse erfolgt jedoch auf der Inhaltsebene.* Die zu übertragenden Daten werden entsprechend den Einstellungen des Nutzers bzw. der Konfiguration der verwendeten Mixrechner neu verarbeitet und unter Einsatz von Telekommunikationsdiensten weiter versendet. Dies ist vergleichbar mit einem automatischen Übersetzungsdienst, bei dem Inhalte von Webseiten über einen zwischengeschalteten Dienst geleitet werden, der den Inhalt so verändert, dass die Worte in eine andere Sprache übersetzt werden. Bei AN.ON werden die Daten in eine verschlüsselte Form „übersetzt“ und zur Gewährung des Rechts auf Anonymität über mehrere sog. Mixrechner geleitet. Somit handelt es sich bei AN.ON um ein Telemedium, das auf Telekommunikationsdiensten aufsetzt.

Damit kann AN.ON als Verarbeitung von Telekommunikations*inhalten* nicht unter die Vorratsdatenspeicherung fallen, da die Richtlinie eine Speicherung von Inhaltsdaten ausdrücklich nicht zulässt. Zudem können Inhalte der Telekommunikation schon nach gegenwärtigem Recht nicht nach §§ 100g/h StPO herausgegeben werden, sondern nur nach § 100a StPO (siehe dazu unten).

Unklar ist, in welcher Form die Regelung die unterschiedlichen Arten von Anonymisierungsdiensten jeweils erfasst. Es gibt eben gerade keinen zentralen Anbieter, den man verpflichten könnte. Vielmehr ist jeder Mixbetreiber einer Kaskade selbständig und kann nur Teilinformationen zur Rückverfolgung von IP-Adressen liefern. Durch das verteilte Logging könnte keiner der Betreiber mit den gesammelten Log-Daten Missbrauch betreiben, da sie für ihn alleine keine relevanten Informationen enthalten. Erst wenn alle Betreiber einer Kaskade ihre Logs verbinden würden (etwa bei einer Anfrage der Strafverfolgungsbehörden und eventuell nach einem richterlichen Beschluss), wäre eine Aufdeckung der wahren IP-Adressen möglich. Die Pflicht zur Wahrung der Anonymität wird weiterhin für Telemedien-Anbieter gelten. Zu lösen bliebe bei einer Vorratsdatenspeicherung das Problem festzustellen, wer aus der Masse der Nutzer einer Kaskade auf die angefragte Zieladresse zugegriffen hat. Zieladressen dürfen laut Richtlinie – aus guten Gründen – nicht gespeichert werden, da dies eine Inhaltsüberwachung wäre (vgl. im Einzelnen zu den rechtlichen

Grundlagen des Anonymisierungsdienstes AN.ON: https://www.daten-schutzzentrum.de/projekte/anon/20070316-rechtliche-grundlagen.htm.).

Auch wenn auf Anonymisierungsdienste diese – „eigentlich nicht passende" – Regelung des § 113a Absatz 6 TKG-E angewendet würde, wird mit der Regelung einer effektiven Strafverfolgung ein Bärendienst erwiesen. Die Regelung würde nur diejenigen Dienste treffen, die im räumlichen Bereich der Bundesrepublik Deutschland rechtmäßig betrieben werden. Der AN.ON-Dienst sieht bereits zum gegenwärtigen Zeitpunkt eine „Strafverfolgungsfunktion" vor, auch wenn die Praxis diese Möglichkeit bislang kaum nutzt. So ist etwa der Diensteanbieter AN.ON heute technisch in der Lage, die Strafverfolgung bei Vorliegen einer richterlich angeordneten Überwachung zu unterstützen. Diese bezieht sich jeweils auf einen konkreten Tatverdacht und konkret verdächtige kriminelle Inhalte, verzichtet aber auf eine Pauschalverdächtigung aller unbescholtenen Nutzerinnen und Nutzer. In Zukunft würden – sofern die Vorratsdatenspeicherung hier greift – Nutzer voraussichtlich verstärkt auf Anonymisierungsdienste zugreifen, die im außereuropäischen Ausland oder in sog. „Schurkenstaaten" betrieben werden oder auf solche Dienste, die dezentral laufen und vom Anwendungsbereich der Vorschrift nicht erfasst werden. In diesen Fällen wird die geplante Regelung keine Erfolge bringen, sondern – im Gegenteil – Ermittlungserfolge vereiteln, da eine Überwachung nach § 100 a StPO-E erschwert sein wird.

Bevor durch die aktuelle Gesetzgebung also in das Recht der Bürgerinnen und Bürger, sich unbeobachtet im Internet zu bewegen, durch ein faktisches Verbot der Anonymisierungsdienste eingegriffen wird, sollten die bereits vorhandenen Möglichkeiten ausgeschöpft werden. Ein faktisches Verbot von Anonymisierungsdiensten kann bereits aus der Richtlinie nicht abgeleitet werden, im Gegenteil: Die Verarbeitung von Inhaltsdaten soll gerade unangetastet bleiben.

2. Zu § 113b TKG-E – Verwendung der Vorratsdaten

Die Vorschrift regelt die Voraussetzungen, unter denen die Diensteanbieter zur Herausgabe der Vorratsdaten verpflichtet werden sollen. Sie korrespondiert mit teilweise erst noch zu schaffenden Vorschriften für die Sicherheitsbehörden, die diesen einen Zugriff auf die Vorratsdaten ermöglichen sollen. Neben dem zu weitgehenden Zugriff auf die Vorratsdaten zur Strafverfolgung ist der Zugriff zur Gefahrenabwehr und zur Aufgabenerfüllung der Nachrichtendienste vorgesehen. Damit entfernt sich der Entwurf endgültig von den Vorgaben der Richtlinie und vertieft die Unverhältnismäßigkeit der Gesamtregelung. Besonders die geplante Zugriffsmöglichkeit der Nachrichtendienste wäre ein eklatanter Verfassungsverstoß.

a) Zugriff zur Strafverfolgung (Satz 1 Nr. 1)

Die Vorratsdatenspeicherung wird nicht dadurch verfassungsmäßig, dass die Speicherung der Verkehrs- und Standortdaten durch die Dienstanbieter und die Herausgabe der Daten erst im Einzelfall durch eine richterliche Anordnung erfolgt. Ein solches zweistufiges Verfahren ändert zum einen nichts an der Eingriffsqualität der Verpflichtung zur Vorratsdatenspeicherung, die ausnahmslos alle Kommunikationsteilnehmer ohne einen konkreten Anlass erfasst. Zum anderen

will die Regierungskoalition die Rechtsgrundlagen, auf die sich eine Auskunft auf Verkehrs- und Standortdaten im Ermittlungsverfahren stützen würde (§§ 100g, h StPO), tatbestandlich nicht einschränken (hierzu ausführlich siehe oben A.6).

Daher sei an dieser Stelle nochmals auf die verfassungsrechtliche Notwendigkeit einer Einschränkung der §§ 100g, h StPO hingewiesen. Von der bisherigen und der geplanten Regelung sind – entgegen der EG-Richtlinie zur Vorratsdatenspeicherung – auch Delikte unterhalb der Schwelle schwerer Straftaten erfasst, soweit nur der Verdacht besteht, dass sie mit Hilfe von Telekommunikation begangen worden sind. Eine Einschränkung ist auch deswegen geboten, weil in der Rechtswirklichkeit über §§ 100g, h StPO nicht nur die Kommunikationsdaten von Beschuldigten, sondern zudem von gänzlich Unbeteiligten und Unverdächtigen wie potentiellen Zeugen beauskunftet werden (z.B. Funkzellenabfrage). Da mit der Vorratsdatenspeicherung die elektronischen Kommunikationsakte aller Teilnehmer über einen Zeitraum von 6 Monaten erfasst werden, bedarf die Regelung über die Beauskunftung aus den Verkehrs- und Standortdaten erheblicher tatbestandlicher Einschränkungen.

b) Zugriff zur Gefahrenabwehr (Satz 1 Nr. 2)

Die Vorratsdatenspeicherung bezieht sich nur auf Telekommunikationsvorgänge, die in der Vergangenheit stattgefunden haben. Daher kann sie im Bereich der Gefahrenabwehr ohnehin nur eine untergeordnete Rolle spielen (vgl. Leutheusser-Schnarrenberger ZRP 2007, 9, 11). Bei der Verwendungsregelung in § 113b Satz 1 Nr. 2 TKG-E stellt sich die Frage der Erforderlichkeit also in besonderer Weise.

Zudem ist der Begriff „erhebliche Gefahr“ nicht für eine verhältnismäßige Eingrenzung der Zugriffsbefugnisse geeignet. Unter einer erheblichen Gefahr wird – hierauf weist u. a. der Bayerische Landesbeauftragte in seiner Stellungnahme hin – jegliche Gefahr für ein bedeutsames Rechtsgut verstanden. Hierzu zählen die Rechtsgüter Leben, Gesundheit, Freiheit, Eigentum, Vermögenswerte, Rechte von bedeutendem Wert und eine Gefahr für den Bestand des Staates und seiner Einrichtungen. Damit wird der Anwendungsbereich auf eine Vielzahl – auch minderschwerer – Fälle ausgedehnt.

c) Zugriff durch Nachrichtendienste (Satz 1 Nr. 3)

Die geplante Regelung in Nr. 3 – die einen Zugriff „zur Erfüllung der gesetzlichen Aufgaben“ der Nachrichtendienstbehörden erlauben will – missachtet die Vorgabe der Richtlinie, wonach die Vorratsdatenspeicherung nur „zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten“ eingesetzt werden darf. Eine sprachliche Anpassung der Vorschriften an diesen Zweck ist in Bezug auf die Nachrichtendienste nicht denkbar. Strafverfolgung kann und darf aufgrund des verfassungsrechtlichen Trennungsgebotes nicht Aufgabe der Nachrichtendienste sein.

Die Zugriffsmöglichkeit der Nachrichtendienste auf die Vorratsdaten verstärkt die Unverhältnismäßigkeit der Vorratsdatenspeicherung. Mit ihrer Hilfe ist es möglich, umfassende Kommunikations- und Persönlichkeitsprofile zu erstellen und Beziehungsgeflechte zu ermitteln.

Wollten die Nachrichtendienste entgegen ihrem gesetzlichen Auftrag politische Interessen und Verhaltensweisen einzelner Bürgerinnen und Bürger und ihr politisches oder gesellschaftliches Zusammenwirken ergründen, wäre die Vorratsdatenspeicherung hierfür ein „geeignetes“ Mittel. Das Risikopotential für die freie politische und persönliche Entfaltung engagierter Menschen ist enorm.

Selbstverständlich liegt es fern, den Nachrichtendiensten einen Missbrauch ihrer Befugnisse zu unterstellen, auch wenn zur Zeit einzelne Ereignisse deswegen einer Überprüfung – etwa in den Bundestags-Ausschüssen – unterzogen werden müssen. Der Bericht des durch das Parlamentarische Kontrollgremium des Deutschen Bundestages beauftragten Sachverständigen Dr. Schäfer zur Observation von Journalisten durch den BND hat festgestellt, dass die untersuchten Maßnahmen „ganz überwiegend rechtswidrig“ waren (Gutachten vom 26. Mai 2006, für die Veröffentlichung bestimmte Fassung, S. 173, http://www2.bundestag.de/bnd_bericht.pdf).

Die bisherigen Formulierungen der einschlägigen Nachrichtendienstgesetze sind in Verbindung mit der hier besprochenen Gesetzesvorlage nicht geeignet, eine extensive Überwachung weiter Bevölkerungskreise durch Nachrichtendienste auszuschließen. Bei Betrachtung der einschlägigen Vorschriften ist nicht nur festzustellen, dass die Eingriffsschwellen niedrig liegen, sondern auch, dass zunehmend unverdächtige und gänzlich unbescholtene Menschen als sog. „Kontaktpersonen“ oder „Befürworter“ in das Fadenkreuz geheimdienstlicher Tätigkeit geraten. *Das bestehende Nachrichtendienstrecht lässt de lege lata die Beobachtung gesetzestreuer Bürgerinnen und Bürger zu, sie wird nicht erst durch illegales Handeln ausgelöst.*

Die Nachrichtendienste werden mit Hilfe des geplanten § 113b Satz 1 Nr. 3 TKG-E Verkehrs- und Standortdaten der Betroffenen auch ohne einen konkreten Straftatenverdacht bzw. ohne eine konkrete Gefahrenlage erhalten – möglicherweise unter den Voraussetzungen des § 3 Abs. 1 des Artikel 10-Gesetzes (vgl. § 8 Abs. 8 f. BVerfSchG, § 8 Abs. 3 a BND-Gesetz, § 10 Abs. 3 MAD-Gesetz; diesen Vorschriften fehlt bislang die nötige Bezugnahme auf § 113b Satz 1 Nr. 3 TKG-E). Darüber hinaus ist zu erwarten, dass die erlangten Daten Nachrichtendiensten anderer Staaten zur Verfügung gestellt werden. Durch die Vorratsdatenspeicherung wird die Proliferation derartiger Daten zunehmen.

Eine solche Vorrats-Überwachung weiter Kreise der Bevölkerung für nachrichtendienstliche Zwecke nicht hingenommen werden, die Verfassungswidrigkeit einer solchen Maßnahme wäre offensichtlich.

d) Prüfungsrecht

Nach der Gesetzesbegründung soll den Diensteanbietern keine Prüfungsmöglichkeit zustehen, ob die anfordernde Behörde im Einzelfall zum Zugriff berechtigt ist. Gerade bei heimlichen Ermittlungsmaßnahmen ist die Beibehaltung einer solchen Prüfungsmöglichkeit als zusätzliche Sicherungsmaßnahme notwendig. Es kann nicht sein, dass ein Diensteanbieter zur Herausgabe von Daten verpflichtet sein soll, wenn etwa die offenkundig notwendige richterliche Anordnung fehlt. Zwar nimmt die Entwurfsbegründung auf die notwendige Legitimation etwa durch einen

richterlichen Beschluss Bezug, sie sagt jedoch nichts über die Folgen, wenn diese nicht vorliegt, sondern durch eine einfache Anordnung der anfordernden Stelle „ersetzt“ wird.

3) Vorschläge des Bundesrates

Die Verpflichtung zur Vorratsdatenspeicherung bewirkt eine deutliche Risikoerhöhung, weil dann Verkehrs- und Standortdaten über längere Zeiträume entgegen den gesetzlichen Regelungen bspw. für die Auswertung für Kundenprofile zur Verfügung stehen. Bereits nach den Vorgaben des Regierungsentwurfs ist zweifelhaft, ob zum Schutz gegen eine missbräuchliche Verwendung der Daten ein hinreichendes präventives datenschutzrechtliches Regelungskonzept vorliegt. Die Vorschläge des Bundesrates zu einer weiteren Abschwächung des Schutzes der Vorratsdaten gegen eine missbräuchliche Verwendung (Vorschlag Nr. 19) sind daher unverständlich.

Die Vorschläge des Bundesrates für eine Auskunftspflicht gegenüber privaten Dritten zur Durchsetzung privater Rechte stehen in diametralem Widerspruch zu den verfassungs- und europarechtlichen Vorgaben. Die Richtlinie gibt klar vor, dass die Daten nur „zum Zwecke der Ermittlung, Feststellung und Verfolgung von schwersten Straftaten“ genutzt werden können. Hierauf eine zivilrechtliche Auskunft stützen zu wollen, ist nicht möglich. Zu den Plänen der Bundesregierung, einen zivilrechtlichen Auskunftsanspruch über Verkehrsdaten einzuführen, verweise ich auf die Stellungnahme des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vom 16. Juni 2007, die dieser im Rahmen des Anhörungsverfahrens im Deutschen Bundestag abgegeben hat. Auch unter dem genannten Aspekt einer missbräuchlichen Verwendung der durch das Telekommunikationsgeheimnis geschützten Daten (sic!) ist der Zugriff durch private Stellen nicht hinnehmbar.

Eine „klarstellende“ Regelung, wonach die Herausgabe der Verkehrsdaten aufgrund §§ 161, 163 StPO i.V.m. § 113 TKG möglich sein solle, ist aus den oben dargestellten Gründen strikt abzulehnen. Eine solche Regelung wäre unverhältnismäßig und ein Verstoß gegen Art. 10 GG.

Ebenso nicht haltbar ist die vom Bundesrat vorgeschlagene Streichung der Worte „unter Bezugnahme auf § 113a“ in § 113b Satz 1 Halbsatz 1 TKG-E. Dies würde dazu führen, dass sämtliche Regelungen über den Zugriff auf Verkehrsdaten mit einem Schlag – ohne weitere gesetzgeberische Prüfung der Verhältnismäßigkeit – die im Rahmen der Vorratsdatenspeicherung gespeicherten Daten betreffen würden. Damit wären etwa sämtliche für Nachrichtendienste geltenden Regelungen anwendbar. Die Unverhältnismäßigkeit der Gesamtregelung wird hierdurch nochmals unterstrichen, die durch die Richtlinie angemahnte Begrenzung auf „schwere Straftaten“ damit endgültig Makulatur.

C. Zusammenfassung

Wir appellieren an den Gesetzgeber, von der **Vorratsdatenspeicherung** Abstand zu nehmen. Vor einer Umsetzung der Richtlinie sollte dringendst das bereits beim Europäischen Gerichtshof anhängige Verfahren abgewartet werden. Möglicherweise wird sie bereits dort für unwirksam erklärt.

- Die Vorratsdatenspeicherung ist unverhältnismäßig und damit verfassungswidrig. Sie verstößt gegen das national durch Art. 10 GG sowie europarechtlich durch Art. 8 EMRK geschützte Fernmeldegeheimnis und gegen das **Verbot der Speicherung „nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken“** (BVerfGE 65, 1, 47). Die Zwecke der Vorratsdatenspeicherung sind unbestimmt, weil die Verkehrs- und Standortdaten aller Teilnehmer und Netze öffentlicher elektronischer Kommunikationsdienste pauschal und ohne jeden konkreten Anhaltspunkt für eine konkrete Straftat der betroffenen Personen gespeichert werden.

- Die **Einbeziehung aller Kommunikationsteilnehmer** qualifiziert die Vorratsdatenspeicherung als eine Maßnahme mit einer außerordentlich hohen Eingriffsintensität. Sie gefährdet die Unbefangenheit der Nutzung der Telekommunikation und in der Folge die **Qualität der Kommunikation einer Gesellschaft**, weil die Maßnahmen dazu beitragen, dass die Risiken des Missbrauches und ein Gefühl des Überwachtwerdens entstehen.

- Die Vorratsdatenspeicherung ist unverhältnismäßig und damit verfassungswidrig, weil sie die Speicherung von Verkehrs- und Standortdaten aller Kommunikationsteilnehmer **ohne jeden Verdacht** anordnet. Nach dem Grundsatz der Verhältnismäßigkeit dürfen intensive Grundrechtseingriffe erst von bestimmten Verdachts- oder Gefahrenstufen an vorgesehen werden. Grundrechtseingreifende Maßnahmen „ins Blaue hinein“ sind unzulässig.

- Die **Zugriffsmöglichkeit der Nachrichtendienste** steigert die Unverhältnismäßigkeit auf ein unerträgliches Maß. Das bestehende Nachrichtendienstrecht lässt die Beobachtung gesetzestreuer Bürgerinnen und Bürger zu. Diese müssen nicht erst illegal handeln. Die bisherigen Formulierungen der einschlägigen Nachrichtendienstgesetze sind nicht geeignet, eine extensive Überwachung weiter Bevölkerungskreise durch Nachrichtendienste auszuschließen.

- Angesichts der Missbrauchsmöglichkeiten warnen wir dringend vor der Verankerung eines **zivilrechtlichen Auskunftsanspruches** auf die Vorratsdaten. Private Dritte könnten ein Interesse daran haben, die Kommunikationsprofile außerhalb ihrer Zweckbestimmung einzusetzen. Man bedenke, dass Adresshändler für weit belanglosere Daten teilweise erhebliche Summen zahlen. Dem kommerziellen Gebrauch darf der Gesetzgeber nicht Vorschub leisten – es geht um das Telekommunikationsgeheimnis.

Das Ziel, im Bereich der **Strafprozessordnung** eine „harmonische Gesamtregelung“ der verdeckten Ermittlungsmaßnahmen zu schaffen, ist grundsätzlich zu begrüßen. Vor Überarbeitung der Strafprozessordnung wäre eine umfassende Evaluation zu wünschen gewesen. Eine solche ist bislang

nur für Wohnraumüberwachung und Telekommunikationsüberwachung durchgeführt worden. Im Hinblick auf das verfolgte Ziel sind insbesondere folgende Punkte problematisch:

- Die Regelungen des Gesetzesentwurfs senken **Eingriffsschwellen**, nicht nur bei der Telekommunikationsüberwachung. Es wird voraussichtlich zu einer erheblichen Ausweitung von Eingriffen in das Telekommunikationsgeheimnis und in das Recht auf informationelle Selbstbestimmung kommen. Der Entwurf räumt tatsächlichen oder vermeintlichen Sicherheitsinteressen den Vorrang ein. Besonders heikel ist die zu umfangreiche Einbeziehung von Kontakt- und Begleitpersonen.

  Zweifel an der Verfassungsmäßigkeit gelten insbesondere für den Zugriff auf die im Rahmen der Vorratsdatenspeicherung erfassten *Verkehrsdaten* (§ 100g StPO-E). Der Entwurf geht über die Grenzen der Verhältnismäßigkeit und die Grenzen der Richtlinie deutlich hinaus, indem er die Herausgabe der Daten schon in Fällen der Bagatellkriminalität zulässt. Jede „mittels eines Telekommunikationsendgerätes“ begangene Straftat soll ausreichen – darunter fällt schon die telefonische Beleidigung. Im Bereich der Internetdaten wird praktisch auf jede Eingriffsschwelle verzichtet.

  Der Anlasstatenkatalog zur *Telekommunikationsüberwachung* wird ohne hinreichende Begründung erweitert. Nur solche Straftaten werden aus dem Katalog gestrichen, die ohnehin keine praktische Bedeutung haben.

- Der Schutz des **Kernbereichs privater Lebensgestaltung** wird durch die geplante Regelung (§ 100a Absatz 4 StPO-E) ausgehöhlt. Wenn nur Inhalte geschützt sind, die „allein“ den Kernbereich betreffen, wird nichts geschützt. Denn ein solcher Fall wird in der Praxis kaum vorkommen. Die Vorgaben aus Karlsruhe blieben unbeachtet. Der Schutz muss über den Bereich der Telekommunikationsüberwachung hinausgehen. Auch andere Maßnahmen können den Kernbereich berühren, so etwa das vertrauliche Gespräch außerhalb von Wohnungen (§ 100f StPO-E). Notwendig ist eine „vor die Klammer gezogene“ Regelung.

- Die Schutzansprüche der **Zeugnisverweigerungsberechtigten** drohen durch weiche Abwägungsklauseln verwässert zu werden. Die Differenzierung nach verschiedenen Klassen von Zeugnisverweigerungsberechtigten ist nicht nachvollziehbar und untergräbt einen wirksamen Grundrechtsschutz. Dass ein Schutz nach neuerer Planung erst eingreifen soll, wenn sich die Maßnahme „gegen“ den Zeugnisverweigerungsberechtigten richtet, verringert den Schutz zusätzlich.

- Den **Verfahrenssicherungen** fehlt eine Begründungspflicht für richterliche Beschlüsse. Auf die in wissenschaftlichen Studien festgestellten aufsehenerregenden Praxisdefizite sollte reagiert werden.

- Die **Benachrichtigungsregel** in § 101 StPO-E enthält Schlupflöcher, die eine Benachrichtigung im Einzelfall umgehen oder ausschließen. Die Benachrichtigung ist Ausfluss der Rechtsweggarantie in Art. 19 Absatz 4 GG und hat darüber hinausgehende Bedeutung. Sie kann verfassungsrechtlich nur in eng begrenzten Fällen unterbleiben. Die bestehenden Defizite in der Praxis würden verstärkt.

08. Juni 2007

Telekommunikationsüberwachung und heimliche Ermittlungsmaßnahmen dürfen Grundrechte nicht aushebeln

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wendet sich mit Nachdruck gegen die von Bundesregierung und Bundesratsgremien geplante Einführung der Vorratsspeicherung von Telekommunikationsverkehrsdaten und die Verschärfungen verdeckter Ermittlungsmaßnahmen, vor allem durch Telekommunikationsüberwachung:

Die Datenschutzbeauftragten haben am 8./9. März 2007 auf ihrer Konferenz in Erfurt einen ersten Gesetzentwurf als verfassungswidrig beanstandet. Insbesondere haben sie vor heimlichen Online-Durchsuchungen und der Vorratsdatenspeicherung gewarnt. Damit würde tief in die Privatsphäre eingegriffen und das Kommunikationsverhalten der gesamten Bevölkerung – ob via Telefon oder Internet – pauschal und anlasslos erfasst.

Die einhellige Kritik der Datenschutzbeauftragten und ihre Aufforderung, stattdessen verhältnismäßige Eingriffsregelungen zu schaffen, wurden von der Bundesregierung nicht beachtet. In ihrem Gesetzentwurf vom 27. April 2007 wird demgegenüber der Schutz der Zeugnisverweigerungsberechtigten verringert, Benachrichtigungspflichten gegenüber betroffenen Personen werden aufgeweicht, Voraussetzungen für die Erhebung von Standortdaten in Echtzeit und für den Einsatz des IMSI-Catchers erheblich ausgeweitet und die Verwendungszwecke für die auf Vorrat gespeicherten Daten über die europarechtlichen Vorgaben hinaus auch auf leichte Straftaten, auf Zwecke der Gefahrenabwehr und sogar der Nachrichtendienste erstreckt.

Die nun im Bundesratsverfahren erhobenen zusätzlichen Forderungen zeugen von mangelndem Respekt vor den Freiheitsrechten der Bürgerinnen und Bürger. Dies zeigen folgende Beispiele: Die ohnehin überzogene Speicherdauer aller Verkehrsdaten wird von 6 auf 12 Monate verlängert. Die Überwachungsintensität erhöht sich durch eine Verschärfung der Prüfpflichten der Telekommunikationsunternehmen – bis zum Erfordernis des Ablichtens und Aufbewahrens von Identitätsnachweisen aller Personen, die Prepaid-Produkte nutzen wollen. Die Sicherheitsbehörden erhalten Auskunft über Personen, die bestimmte dynamische IP-Adressen nutzen. Ausschüsse des Bundesrates wollen die Nutzung dieser Daten sogar zur zivilrechtlichen Durchsetzung der Rechte an geistigem Eigentum gestatten und bewegen sich damit weit jenseits des durch die EG-Richtlinie zur Vorratsspeicherung abgesteckten Rahmens, die Nutzung auf die Verfolgung schwerer Straftaten zu beschränken. Weiterhin ist eine Ausdehnung der Auswertung von Funkzellendaten von Mobiltelefonen mit dem Ziel der Ermittlung des Aufenthaltes von möglichen Zeuginnen und Zeugen geplant. Daten, die Beweiserhebungs- oder -verwertungsverboten unterliegen, sollen nicht unmittelbar gelöscht, sondern nur gesperrt werden.

Ganz nebenbei will der Innenausschuss des Bundesrats eine Rechtsgrundlage für die heimliche Online-Durchsuchung von Internet-Computern schaffen. Allein die Zulassung dieser Maßnahme würde rechtsstaatlichen Grundsätzen eklatant widersprechen und das Vertrauen in die Sicherheit der Informationstechnik massiv beschädigen.

Das Bundesverfassungsgericht hat in letzter Zeit eine Reihe von Sicherheitsgesetzen mit heimlichen Erhebungsmaßnahmen aufgehoben. Auch europäische Gerichte haben Sicherheitsmaßnahmen für rechtswidrig erklärt. Eine Entscheidung des Europäischen Gerichtshofs über die Verpflichtung zur Vorratsdatenspeicherung von Telekommunikationsverbindungsdaten sollte abgewartet werden, ebenso wie die Entscheidung des Bundesverfassungsgerichtes zur nordrhein-westfälischen Regelung, die dem Verfassungsschutz die Online-Durchsuchung erlaubt.

Die Forderungen im Gesetzgebungsverfahren zeugen von einem überzogenen Sicherheitsdenken. Sie führen dazu, dass die Freiheitsrechte der Bevölkerung untergraben werden. Sicherheit in der Informationsgesellschaft ist nicht mit überbordenden Überwachungsregelungen zu erreichen, sondern nur durch maßvolle Eingriffsbefugnisse mit effektiven grundrechtssichernden Verfahrensregelungen und durch deren besonnene Anwendung. Die betroffenen Grundrechte verkörpern einen zu hohen Wert, als dass sie kurzfristigen Sicherheitsüberlegungen geopfert werden dürfen.

Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 08. - 09. März 2007 in Erfurt

Vorratsdatenspeicherung, Zwangsidentifikation im Internet, Telekommunikationsüberwachung und sonstige verdeckte Ermittlungsmaßnahmen

Die gesetzlichen Regelungen der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sollen nach der Ankündigung der Bundesregierung unter Berücksichtigung der Rechtsprechung des Bundesverfassungsgerichts einer umfassenden Neuregelung unterzogen werden. Die Bundesregierung will in diesem Zusammenhang auch die europäische Richtlinie zur Vorratsspeicherung von Telekommunikationsverkehrsdaten umsetzen. Das Bundesministerium der Justiz hat zwischenzeitlich einen Referentenentwurf vorgelegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder betont erneut, dass die Vorratsdatenspeicherung deutschem Verfassungsrecht widersprechen würde. Nach der Rechtsprechung des Bundesverfassungsgerichts ist die Speicherung von Daten auf Vorrat zu nicht hinreichend bestimmbaren Zwecken verfassungswidrig. Zudem würde die für eine freiheitliche Gesellschaft konstitutive unbefangene Kommunikation erheblich beeinträchtigt. Die Konferenz fordert die Bundesregierung auf, die Umsetzung der Europäischen Richtlinie zur Vorratsdatenspeicherung zumindest solange zurückzustellen, bis der bereits angerufene Europäische Gerichtshof über deren Rechtmäßigkeit entschieden hat.

Die geplante Ausweitung der Vorratsdatenspeicherung geht weit über die europarechtliche Umsetzungsverpflichtung hinaus und wäre ein zusätzlicher unverhältnismäßiger Eingriff in die Kommunikationsfreiheit der Bürgerinnen und Bürger. So sollen die Daten auch zur Verfolgung von Straftaten von erheblicher Bedeutung sowie mittels Telekommunikation begangener Straftaten genutzt werden. Zudem soll die Möglichkeit zur anonymen E-Mail-Kommunikation abgeschafft und die Nutzenden öffentlich zugänglicher E-Mail-Dienste sollen zur Angabe ihres Namens und ihrer Adresse verpflichtet werden. Diese Angaben sollen außerdem einer Vielzahl von Behörden zum Online-Abruf zur Verfügung gestellt werden, darunter der Polizei, den Staatsanwaltschaften, den Nachrichtendiensten, dem Zoll und der Bundesanstalt für Finanzdienstleistungsaufsicht. Auch dies begegnet erheblichen datenschutzrechtlichen Bedenken.

Zwar stärken einige der vorgesehenen Änderungen der Strafprozessordnung die rechtsstaatlichen und grundrechtlichen Sicherungen bei verdeckten strafprozessualen Ermittlungsmaßnahmen. Es besteht jedoch noch erheblicher Verbesserungsbedarf, insbesondere im Hinblick auf den Schutz des Kernbereichs privater Lebensgestaltung, den Schutz von Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern und die Voraussetzungen der Telekommunikationsüberwachung:

- Mit einer erneuten Ausweitung des Straftatenkatalogs für die Telekommunikationsüberwachung würde die Tendenz zunehmender Überwachungsmaßnahmen in verstärktem Maße fortgesetzt. Der Katalog sollte deshalb mit dem Ziel einer deutlichen Reduzierung kritisch überprüft werden. Es sollten nur Straftaten aufgenommen werden, deren Aufklärung in besonderem Maße auf die Telekommunikationsüberwachung angewiesen ist, die mit einer bestimmten gesetzlichen Mindeststrafe (z. B. ein Jahr) bedroht sind und die auch im Einzelfall schwer wiegen.

- Die vorgesehene Kernbereichsregelung ist ungenügend. Sie nimmt in Kauf, dass regelmäßig auch kernbereichsrelevante Informationen erfasst werden. Für solche Informationen muss stattdessen grundsätzlich ein Erhebungsverbot gelten. Erkenntnisse aus dem Kernbereich der privaten Lebensgestaltung, die dennoch erlangt werden, müssen zudem einem absoluten Verwertungsverbot unterliegen, nicht nur für Strafverfahren.

- Der Schutz des Kernbereichs privater Lebensgestaltung ist nicht nur in den Bereichen der Wohnraum- und Telekommunikationsüberwachung zu gewährleisten. Auch für alle anderen verdeckten Ermittlungsmaßnahmen ist eine Regelung zum Schutz des Kernbereichs zu treffen.

- Für die Kommunikation mit Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern sollte ein absolutes Erhebungs- und Verwertungsverbot geschaffen werden, das dem jeweiligen Zeugnisverweigerungsrecht entspricht. Dieses sollte unterschiedslos für alle Berufsgeheimnisträgerinnen und Berufsgeheimnisträger und deren Berufshelferinnen und Berufshelfer gelten. Die im Entwurf enthaltene Differenzierung zwischen bestimmten Gruppen von Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern ist sachlich nicht gerechtfertigt.

- Für Angehörige i.S.v. § 52 StPO sollte ein Erhebungs- und Verwertungsverbot für die Fälle vorgesehen werden, in denen das öffentliche Interesse an der Strafverfolgung nicht überwiegt. Die besonderen verwandtschaftlichen Vertrauensverhältnisse dürfen nicht ungeschützt bleiben.

- Für teilnehmende Personen von Kernbereichsgesprächen, die weder Berufsgeheimnisträgerinnen und Berufsgeheimnisträger noch Angehörige i.S.v. § 52 StPO sind, sollte insoweit ein Aussageverweigerungsrecht aufgenommen werden. Andernfalls bleibt der Kernbereich teilweise ungeschützt.

- Für die sog. Funkzellenabfrage, die alle Telefonverbindungen im Bereich einer oder mehrerer Funkzellen erfasst, sollten klare und detaillierte Regelungen mit engeren Voraussetzungen normiert werden. Diese sollten vorsehen, dass im Rahmen einer besonderen Verhältnismäßigkeitsprüfung die Anzahl der durch die Maßnahmen betroffenen unbeteiligten Dritten berücksichtigt und die Maßnahme auf den räumlich und zeitlich unbedingt erforderlichen Umfang begrenzt wird. Die Unzulässigkeit der Maßnahme zur Ermittlung von Tatzeuginnen und Tatzeugen sollte ins Gesetz aufgenommen werden.

- Die aufgrund einer Anordnung der Staatsanwaltschaft bei Gefahr in Verzug erlangten Daten dürfen nicht verwertet werden, wenn die Anordnung nicht richterlich bestätigt wird. Dieses Verwertungsverbot darf nicht - wie im Entwurf vorgesehen - auf Beweiszwecke begrenzt werden.

- Art und Umfang der Begründungspflicht für den richterlichen Beschluss der Anordnung der Telekommunikationsüberwachung sollte wie bei der Wohnraumüberwachung im Gesetz festgeschrieben werden. Im Sinne einer harmonischen Gesamtregelung sollten darüber hinaus qualifizierte Begründungspflichten für sämtliche verdeckte Ermittlungsmaßnahmen geschaffen werden.

- Zur Gewährleistung eines effektiven Rechtsschutzes ist sicherzustellen, dass sämtliche Personen, die von heimlichen Ermittlungsmaßnahmen betroffen sind, nachträglich von der Maßnahme benachrichtigt werden, soweit diese bekannt sind oder ihre Identifizierung ohne unverhältnismäßige weitere Ermittlungen möglich ist und nicht überwiegende schutzwürdige Belange anderer Betroffener entgegenstehen. Darüber hinaus sollte bei Massendatenerhebungen über eine ergänzende Benachrichtigung durch eine öffentliche Bekanntmachung der Maßnahme nachgedacht werden.

- Die für die Telekommunikationsüberwachung vorgesehenen Berichts- und Statistikpflichten sollten um Angaben zur Dauer der Überwachung, zur Anzahl der Gespräche und zur Benachrichtigung Betroffener ergänzt werden.

- Die im Entwurf enthaltenen erweiterten Eingriffsgrundlagen sollten befristet und einer unabhängigen, gründlichen und wissenschaftlich unterstützten Evaluation unterzogen werden.