

**Stellungnahme der Humanistischen Union**  
zum Regierungsentwurf eines  
„Gesetz zur Neuregelung der Telekommunikationsüberwachung  
und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung  
der Richtlinie 2006/24/EG“ (BT-Drucksache 16/5846)

Berlin, 12. September 2007

*Dr. Fredrik Roggan*

*unter Mitarbeit von*

*Dr. Miroslav Angelov, Nils Bergemann, Dr. Dr. hc. Burkhard Hirsch,  
Martina Kant, Sven Lüders, Dr. Till Müller-Heidelberg, Burkhard Nedden,  
Gerhard Saborowski und Prof. Dr. Rosemarie Will*

*„Der Gedanke verdient hervorgehoben zu werden, dass der Gesetzgeber nicht nur am Rande der Verfassung herumtanzen und ständig versuchen sollte, ihre Belastungsfähigkeit auszutesten, sondern sich darum bemühen müsste, ihren Geist zu verwirklichen und zu bewahren. Nicht alles, was vielleicht gerade noch mit der Verfassung zu vereinbaren ist, ist auch klug und angemessen.“  
(Burkhard Hirsch)*

<b>A. Einleitung</b> .....	<b>4</b>
I. Zum ersten Teil: Neuregelung der verdeckten (heimlichen) Ermittlungsmaßnahmen in der Strafprozessordnung.....	4
II. Zum zweiten Teil: Die Umsetzung der europäischen Richtlinie zur Vorratsdatenspeicherung .....	5
 <b>B. Die Neuregelung der verdeckten (heimlichen) Ermittlungsmaßnahmen in der StPO</b> .7	
I. Eingriffsschwellen.....	7
1. Subsidiaritätsklauseln .....	8
2. Heimliche Ermittlungsmaßnahmen gegen Kontakt- und Begleitpersonen (§§ 100a StPO-E, 100c StPO, 100f StPO-E, 100h StPO-E, 100i StPO-E, 163e StPO, 163f StPO).....	9
3. Spezifische Eingriffsschwellen .....	9
a) Telekommunikationsüberwachung (§ 100a StPO-E) .....	9
b) Postbeschlagnahme (§§ 99, 100 StPO).....	11
c) Verkehrsdatenabfrage (§ 100g StPO-E).....	11
II. Schutz des Kernbereichs privater Lebensgestaltung.....	12
1. Kernbereichsschutz nur für Lauschangriff und Telekommunikationsüberwachung?.....	13
2. Schutz des Kernbereichs in § 100a Abs. 4 StPO-E nur teilweise mit den Vorgaben des Bundesverfassungsgerichts vereinbar.....	14
a) Vorgaben des Bundesverfassungsgerichts.....	14
(1) Überwachungsverbot bei vorhersehbarer Betroffenheit kernbereichsrelevanter Kommunikation .....	15
(2) Abbruch einer Live-Überwachung bei ungewisser Betroffenheit von kernbereichsrelevanter Kommunikation .....	16
(3) Auswertungsverbote und Löschungspflichten bei unerwarteter, zufälliger Betroffenheit von kernbereichsrelevanter Kommunikation .....	17
b) Unzureichender Kernbereichsschutz nach § 100a Abs.4 StPO-E .....	17
III. Schutz von Zeugnisverweigerungsrechten.....	18
1. Notwendigkeit eines einheitlichen Schutzes (§ 53b Abs. 1 und 2 StPO-E).....	19
2. Notwendigkeit eines absoluten Schutzes (§ 53b Abs. 2 StPO-E) .....	19
3. Keine Umgehung der Zeugnisverweigerungsrechte (§ 53b Abs. 4 StPO-E) .....	20
IV. Verfahrenssicherungen .....	21
1. Begründungspflichten.....	21
2. Verwertungsverbot für unrechtmäßig erlangte Erkenntnisse (Vorschlag: § 101 Abs. 1a StPO)..	22
3. Die Unterrichtung des anordnenden Gerichts muss auf alle durchgeführten verdeckten Ermittlungsmaßnahmen ausgedehnt werden .....	24
4. Benachrichtigung der Betroffenen (§ 101 Abs. 4-7 StPO-E) .....	24

5. Rechtsschutz gegen Ermittlungsmaßnahmen (§ 101 Abs. 9 StPO-E) mit zu kurzer Frist.....	25
6. Unzureichende Berichtspflichten zur TK-Überwachung (§ 100b Abs. 5 f. StPO-E) .....	25

## **C. Die Umsetzung der Richtlinie zur Vorratsdatenspeicherung (RL 2006/24/EG) .....27**

I. Die europarechtswidrige Richtlinie.....	27
1. Die Entstehung der Richtlinie .....	27
2. Richtlinieninhalt .....	28
3. Die Europarechtswidrigkeit der Richtlinie .....	28
II. Zur Verfassungsmäßigkeit des deutschen Umsetzungsgesetzes .....	30
1. Der Verstoß gegen Art. 10 GG (Fernmeldegeheimnis).....	31
1.1. Zweistufiger Eingriff in das Grundrecht aus Art. 10 Abs. 1 GG .....	31
1.2. Stufe 1: Die anlasslose Erhebung und Speicherung sämtlicher Verbindungsdaten als genereller Verstoß gegen das Fernmeldegeheimnis .....	32
a) Legitimität des Zwecks der Speicherungspflicht.....	32
b) Geeignetheit der Vorratsdatenspeicherung .....	33
c) Erforderlichkeit der Vorratsdatenspeicherung .....	34
d) Angemessenheit der Vorratsdatenspeicherung .....	35
aa) Die von der Vorratsdatenspeicherung erfassten Personen .....	35
bb) Adressaten der Speicherungspflicht (§ 110a Abs. 1 Satz 1 TKG-E).....	36
cc) Verbot der Anonymisierungsdienste .....	37
dd) Katalog der zu speichernden Daten (§ 113a Abs. 2 bis 5 TKG-E) .....	38
ee) Missbrauchsgefahr durch Private .....	41
e) Zwischenergebnis für die erste Stufe.....	42
1.3 Stufe 2: Zugriff auf die Vorratsdaten als Eingriff in das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG.....	42
a) Zugriffsberechtigte Behörden und Art der Informationszugriffe .....	43
b) Voraussetzungen für den Zugriff auf die vorrätig gespeicherten Verkehrsdaten.....	45
aa) Straftatenkatalog für den staatlichen Zugriff auf die Vorratsdaten (§ 100g Abs. 1 StPO-E) .....	45
bb) Zu niedrige Eingriffsschwelle .....	49
c) Unzureichende Differenzierung bezüglich der betroffenen Personen (Kontaktpersonen).....	49
d) Zwischenergebnis für die zweite Stufe .....	50
2. Verstoß gegen Art. 12 Abs. 1 GG.....	50
3. Ergebnis der verfassungsrechtlichen Prüfung.....	51

## A. Einleitung

Diese Stellungnahme befasst sich im ersten Teil mit der Neuregelung der verdeckten Ermittlungsmaßnahmen in der Strafprozessordnung, der zweite Teil hat die Regelungen zur Umsetzung der EU-Richtlinie zur Vorratsdatenspeicherung zum Gegenstand.

### I. Zum ersten Teil: Neuregelung der verdeckten (heimlichen) Ermittlungsmaßnahmen in der Strafprozessordnung

Mit dem Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen will die Bundesregierung ein in sich kohärentes Gesamtsystem strafprozessualer heimlicher Ermittlungsmethoden schaffen.

Dieser Grundgedanke des Gesetzentwurfes, einen gemeinsamen Mantel für verdeckte Ermittlungsmaßnahmen zu entwickeln, ist richtig und begrüßenswert. Es ist die einzige Möglichkeit, den in zahlreichen Urteilen des *Bundesverfassungsgerichts* eingeforderten Schutz der Menschenwürde und der Privatheit nicht nur für den Lauschangriff, sondern für alle verdeckten Ermittlungsmaßnahmen zu sichern. Die rechtsstaatliche Verpflichtung zum Schutz dieser Grundrechte endet nicht an der Wohnungstür. Hinzu kommt, dass alle verdeckten, also heimlichen Ermittlungen eine immanente Missbrauchsgefahr bergen, weil sie nur schwer oder überhaupt nicht erkannt werden und ihre rechtliche Kontrolle daher zumindest erschwert ist. Das Gutachten des Max-Planck-Institutes<sup>1</sup> und die Studie der Universität Bielefeld<sup>2</sup> zeigen das besonders eindrucksvoll.

Der Gesetzentwurf verwirklicht diesen richtigen Grundgedanken jedoch nur sehr zögerlich und unzureichend. Die Begründung legt großen Wert darauf, dass jede Beschränkung von Ermittlungsmaßnahmen die Wahrheitsfindung beeinträchtigt und damit möglicherweise Tatsachen verborgen bleiben, die nicht nur für die Strafverfolgung, sondern auch für die Verteidigung wichtig sein könnten. Dies ist ein rhetorisches Hilfsargument, dessen praktische Bedeutung wohl als nachrangig einzustufen ist. Zugleich kann dieses Argument pauschal gegen jede Beschränkung von Ermittlungsmaßnahmen und gegen jedes Zeugnisverweigerungsrecht oder Beschlagnahmeverbot vorgebracht werden.

Der vorliegende Gesetzentwurf weist nach Auffassung der HUMANISTISCHEN UNION ein einseitiges rechtspolitisches Verständnis auf: Er behauptet pauschal, dass alle verdeckten Ermittlungsmaßnahmen unverzichtbar seien und untersucht vorrangig, ob die vorgeschlagenen Beschränkungen

---

<sup>1</sup> *Albrecht/Dorsch/Krüpe*, Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen - Abschlussbericht (Studie des Max-Planck-Instituts für ausländisches und internationales Strafrecht), Freiburg 2003, S. 29 - im Folgenden: MPI-Studie

<sup>2</sup> *Backes/Gusy*, Wer kontrolliert die Telefonüberwachung? Eine empirische Untersuchung zum Richtervorbehalt bei der Telefonüberwachung (Studie der Universität Bielefeld), Frankfurt/M. 2003; vgl. hierzu auch StV 2003, Seite 249 ff. sowie ZRP 2003, Seite 275 ff.

im Sinne einer effektiven Strafverfolgung vertretbar sind. Auf die Frage, ob denn die jeweilige Ermittlungsmaßnahme wirklich unverzichtbar ist, wird an keiner Stelle eingegangen. Vielmehr versucht der Gesetzentwurf, die Grenzen des verfassungsgemäß Möglichen weitgehend auszuschöpfen. Das ist insofern nachvollziehbar, da es dem Gesetzgeber nicht gestattet ist, bei seinem Handeln die verfassungsrechtlichen Grenzen zu überschreiten. Die Arbeit des Gesetzgebers darf sich jedoch nicht auf die Auslotung verfassungsrechtlicher Grenzen beschränken. Er sollte neben den verfassungsrechtlichen Problemstellungen auch eine Antwort auf die Frage liefern, was rechtspolitisch vertretbar und erforderlich ist. So ist es durchaus fraglich, ob das heimliche Belauschen des Gesprächs engster Verwandter in der eigenen Wohnung wirklich notwendig ist, mag es nun verfassungsrechtlich gerade noch zulässig sein oder nicht. Man kann niemandem erklären, warum das vertraute Gespräch mit der eigenen Mutter weniger geschützt wird, als das mit dem Steuerberater. Der Staat und die wirksame Strafverfolgung würden keineswegs zusammenbrechen, wenn auf das Belauschen des Gesprächs eines Betroffenen mit seiner Mutter oder seiner Frau vollständig verzichtet würde, anstatt es einem feinziselierten Abwägungsgebot nach dem Maßstab des Verhältnismäßigkeitsgrundsatzes zu unterwerfen.

Der Entwurf will keine große Lösung sein – und unter rechtspolitischen Gesichtspunkten ist er es auch nicht.

## **II. Zum zweiten Teil: Die Umsetzung der europäischen Richtlinie zur Vorratsdatenspeicherung**

Die im Gesetzentwurf vorgesehene Einführung der Vorratsdatenspeicherung ebnet den Weg in den Überwachungsstaat. Mit den vorgeschlagenen Änderungen des Telekommunikationsgesetzes wird eine EU-Richtlinie über die Vorratsdatenspeicherung umgesetzt (RL 2006/24/EG), an deren formeller europäischer Rechtmäßigkeit erhebliche Zweifel bestehen. Die Umsetzung der Vorratsdatenspeicherung über eine Richtlinie wurde erst gewählt, nachdem die für den ursprünglich geplanten Rahmenbeschluss nach Art. 31 und 34 EUV erforderliche Einstimmigkeit nicht erreicht werden konnte. Ihrem Ziel und Inhalt nach dient die Vorratsdatenspeicherungsrichtlinie jedoch der Strafverfolgung (vgl. Art. 1 Abs. 1 sowie Erwägungsgrund Nr. 7 und 21 RL 2006/24/EG). Sie hätte deshalb nicht als Richtlinie auf Art. 95 EGV gestützt verabschiedet werden dürfen. Es ist zu erwarten, dass die von Irland erhobene Nichtigkeitsklage gegen die Richtlinie Erfolg haben wird<sup>3</sup>. Aus rechtspolitischer Verantwortung erscheint es deshalb angemessen, bis zur Entscheidung des EuGH über die Nichtigkeitsklage von einer Umsetzung der Richtlinie 2006/24/EG in deutsches Recht abzusehen.

Die mit dem Gesetzentwurf geplante Vorratsspeicherung von Telekommunikationsverkehrsdaten führt zu einer umfangreichen Erhebung und Speicherung von Telekommunikationsdaten aller Nutzerinnen und Nutzer dieser Kommunikationsdienste ohne jeglichen Verdacht. Sie ist deshalb

---

<sup>3</sup> EuGH, Rs. C-301/06.

ein unverhältnismäßiger Eingriff in das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG. Selbst wenn anzunehmen wäre, dass die anlasslose Erhebung und Speicherung sämtlicher Verbindungsdaten sämtlicher Kommunikationsteilnehmer nicht gegen das Fernmeldegeheimnis verstößt, sind die durch den Gesetzentwurf eingeführten strafprozessualen Zugriffsregeln in ihrer Form und in ihrem Umfang unverhältnismäßig. Darüber hinaus verstößt die Regelung zur Vorratsdatenspeicherung gegen die Berufsfreiheit der Telekommunikationsanbieter.

In Bezug auf die Vorratsdatenspeicherung setzt der Entwurf eine europarechtswidrige Richtlinie grundgesetzwidrig um. Außerdem geht der Gesetzgeber in vielen Punkten über die Vorgaben der Richtlinie hinaus, was die Eingriffsintensität der jeweiligen Vorschriften erheblich intensiviert und die Gesamtregelung verfassungswidrig macht.

## B. Die Neuregelung der verdeckten (heimlichen) Ermittlungsmaßnahmen in der StPO

### I. Eingriffsschwellen

Die Regelungen des Gesetzentwurfs werden im Ergebnis zu einer erheblichen Ausweitung der Eingriffe in das grundgesetzlich geschützte Fernmeldegeheimnis und in das Recht auf informationelle Selbstbestimmung führen. Sie werden den bereits jetzt kaum noch vorhandenen Schutz der Privatsphäre weiter aushöhlen.

Dabei hilft es nicht, dass der Entwurf an vielen Stellen versucht, durch verfahrenssichernde Maßnahmen den Schaden scheinbar zu begrenzen<sup>4</sup>. Diese Verfahrensregelungen werden im Gesetzentwurf und seiner Begründung als Grundrechtsschutz verkauft. Dabei verschleiert der Entwurf jedoch, dass er bei der Festlegung der materiellen Eingriffsschranken bzw. bei einem Verzicht auf solche Schranken fast überall tatsächlichen oder vermeintlichen Sicherheitsinteressen den Vorrang einräumt. Spätestens seit der MPI-Studie<sup>5</sup> muss die Effektivität des Grundrechtsschutzes über verfahrenssichernde Maßnahmen mit Skepsis gesehen werden. Durch verfahrensrechtliche Sicherungen lassen sich manche Grundrechtseingriffe „abfedern“ – eine konsequente Absicherung der Freiheitsrechte ist jedoch nur mit eng gefassten materiellen Eingriffsschranken möglich, die durch Verfahrensfragen nicht ersetzt werden können.

Im Ergebnis schreibt der Entwurf eine Entwicklung fort, die zahlreiche „Sicherheitspolitiker“ seit Jahren propagieren: Unter Berufung auf ein angebliches „Grundrecht auf Sicherheit“, das jedem zustehe und das zu schützen vorgreifliche Aufgabe der staatlichen Institutionen sei, werden andere grundrechtlich geschützte Freiheitsrechte relativiert und zur Disposition gestellt, wenn es für eine möglichst umfassende Wahrheitsermittlung bei der Straftatenaufklärung und zur Durchsetzung des staatlichen Strafanspruchs geboten erscheint. Die Begründungen des Entwurfs<sup>6</sup> spiegeln dieses Grundverständnis deutlich wieder und belegen das Zwischenfazit, das *Denninger* schon vor Jahren gezogen hat: „Die ‚Versicherheitlichung‘ zehrt an der Substanz ‚normativer Errungenschaften‘ rechtsstaatlichen Sicherheitsrechts“<sup>7</sup>.

---

<sup>4</sup> So besonders deutlich in dem neuen § 101 StPO-E.

<sup>5</sup> Siehe Fn. 1.

<sup>6</sup> S. 53 f.

<sup>7</sup> *Denninger* in Koch (Hrsg.), *Terrorismus – Rechtsfragen der äußeren und inneren Sicherheit*, Baden-Baden 2002, S. 90.

## 1. Subsidiaritätsklauseln

Dem eigenen Anspruch des Gesetzesvorhabens, eine Harmonisierung und Präzisierung der verdeckten Ermittlungsmaßnahmen zu erreichen, wird der Entwurf nicht gerecht. Für die einzelnen Ermittlungsmaßnahmen sind jeweils unterschiedliche Subsidiaritätsklauseln formuliert, nach denen zu entscheiden ist, ob andere, weniger in die Grundrechte eingreifende Ermittlungsmethoden vorrangig anzuwenden sind. Der Gesetzentwurf belässt es bei einer nicht nachvollziehbaren Uneinheitlichkeit der Subsidiaritätsklauseln. So wird gefordert, dass andere Maßnahmen

- a. aussichtslos (§ 100g Abs. 1 Satz 2 StPO-E),
- b. aussichtslos oder wesentlich erschwert (§ 100f Abs. 1 und 2 StPO-E; § 100g Abs. 2 StPO-E; § 100h Abs. 3 Satz 2 Nr. 2 c StPO-E, § 110a Abs. 1 Satz 3 StPO)
- c. wesentlich erschwert oder aussichtslos (§ 100a Abs. 1 StPO-E)
- d. unverhältnismäßig erschwert oder aussichtslos (§ 100c Abs. 1 StPO)
- e. erheblich weniger Erfolg versprechend oder wesentlich erschwert (§ 100h Abs. 2 StPO-E; § 163 e Abs. 1 StPO; § 163 f Abs. 1 StPO)

sein sollen. Für manche verdeckten Ermittlungsmethoden wird keinerlei Subsidiaritätsklausel angeführt (so in § 100g Abs. 1 Satz 1 StPO-E), sondern lediglich die sachliche Erforderlichkeit der Ermittlungsmethode verlangt. Andere Subsidiaritätsbestimmungen, wie „wesentlich erschwert“ oder „unverhältnismäßig erschwert“, stellen in der Praxis keine Begrenzung für den Einsatz verdeckter Ermittlungsmaßnahmen dar, weil sie zu unbestimmt sind. So wird beispielsweise von einer unverhältnismäßigen Erschwerung der Ermittlungen ausgegangen, wenn andere Aufklärungsmittel zu einem unverhältnismäßig höheren Arbeitsaufwand führen und in der Konsequenz andere Ermittlungsverfahren vernachlässigt würden. Dabei – so das bisherige Verständnis – konnte der größere Arbeitsaufwand die Maßnahme aber nur dann rechtfertigen, wenn er so umfangreich gewesen wäre, dass die Strafverfolgungsinteressen eindeutig überwogen. Allein Kostengründe hätten die Eingriffsmaßnahmen also nicht rechtfertigen können<sup>8</sup>. Das bedeutet, dass es auf die Darlegungen der – zudem mit einem Beurteilungsspielraum ausgestatteten<sup>9</sup> – Strafverfolgungsbehörden ankäme, ob bei Nichtanordnung eines großen Lauschangriffs eine Vernachlässigung von anderen Ermittlungen zu befürchten ist oder eben nicht<sup>10</sup>. Es sind angesichts dieser Interpretation berechtigte Zweifel geäußert worden, ob ein derart dehnbare Tatbestandsmerkmal eine verdeckte Maßnahme tatsächlich als letztes Mittel der Strafverfolger erscheinen lässt<sup>11</sup>. Es ist mehr als zweifelhaft, ob in der Praxis tatsächlich Erschwernisse in der Ermittlungsarbeit hingenommen werden, bevor heimliche Ermittlungsmethoden zum Einsatz kommen. Um die Wirksamkeit der Subsidiaritätsklauseln zu verbessern, sollten sie inhaltlich einheitlich und sprachlich gleich lautend formuliert werden. Vorgeschlagen wird, dass die ver-

<sup>8</sup> LR-Schäfer § 100a Rn. 13; KK-Nack § 100a Rn. 25; Meyer-Goßner, StPO, § 100a Rn. 7; HK-Lemke § 100a Rn. 11.

<sup>9</sup> BGHSt 41, 30 (33).

<sup>10</sup> Roggan in: Roggan/Kutscha (Hrsg.), Handbuch der Inneren Sicherheit, 2. Auflage 2006, S. 113; MPI-Studie S. 20. (s. oben Fn. 1)

<sup>11</sup> So zum Lauschangriff SK-StPO-Rudolphi/Wolter, § 100c Rn. 21.

deckten Ermittlungsmaßnahmen nur dann zulässig sein sollen, wenn andere weniger grundrechtsintensive Maßnahmen *aussichtslos* wären.

## 2. Heimliche Ermittlungsmaßnahmen gegen Kontakt- und Begleitpersonen (§§ 100a StPO-E, 100c StPO, 100f StPO-E, 100h StPO-E, 100i StPO-E, 163e StPO, 163f StPO)

Wird wegen einer Straftat nach den §§ 100a StPO-E (TKÜ), 100c StPO (Lauschangriff), 100f StPO-E (kleiner Lauschangriff), 100h StPO-E (längerfristige Beobachtung), 100i StPO-E (IMSI-Catcher), 163e StPO (Ausschreibung zur polizeilichen Beobachtung), 163f StPO (längerfristige Observation) ermittelt, so können die Strafverfolgungsbehörden heimliche Ermittlungsmethoden auch gegen Kontakt- und Begleitpersonen anwenden. Die entsprechenden Regelungen hat der Entwurf beibehalten bzw. neu eingeführt.

Damit eine Kontakt- oder Begleitperson zum Ziel verdeckter Ermittlungsmaßnahmen wird, reicht es aus, dass sie mit dem Beschuldigten in Verbindung steht oder von den Strafverfolgungsbehörden eine solche Verbindung angenommen wird. Beispielsweise können Freunde oder Bekannte des Verdächtigen schon dann ins Visier der Richtmikrofone geraten, wenn sich die Polizei aus deren Gesprächen einen Aufschluss über den Aufenthaltsort des Verdächtigen erhofft (vgl. § 100f Abs. 2 Satz 2 StPO-E und § 100c Abs. 3 StPO). Mit derartigen Regelungen werden regelmäßig gänzlich unbescholtene Bürgerinnen und Bürger zum Objekt schwerwiegender Grundrechtseingriffe durch verdeckte Ermittlungen. Ob eine derartige Erfassung unverdächtigter Personen mit der verfassungsrechtlichen Rechtsprechung im Einklang steht, ist nachdrücklich zu bezweifeln<sup>12</sup>.

Vom Gesetzgeber ist deshalb zu erwarten, dass der Kreis der Delikte deutlich eingegrenzt wird, bei deren Verfolgung unverdächtige Kontakt- und Begleitpersonen miterfasst werden. Zugleich ist eine gesetzliche Präzisierung des Kreises der Kontakt- und Begleitpersonen unabdingbar. Dieser Personenkreis sollte wesentlich enger gefasst und nicht nur durch Abwägungsgebote (vgl. etwa §§ 100f Abs. 2 StPO-E und 100h Abs. 2 StPO-E) sondern durch objektiv nachvollziehbare Maßstäbe bestimmt werden.

## 3. Spezifische Eingriffsschwellen

Auch die spezifischen Eingriffsschwellen der Einzelmaßnahmen sind nur teilweise mit verfassungsrechtlichen Anforderungen vereinbar und bedürfen einer Eingrenzung.

### *a) Telekommunikationsüberwachung (§ 100a StPO-E)*

Die geplante Regelung in § 100a StPO-E ergänzt in Absatz 1 allgemeine Voraussetzungen, in Absatz 2 wird der Anlasstaten-katalog überarbeitet. Während die Ergänzungen in Absatz 1 in die

---

<sup>12</sup> SächsVerfGH, LKV 1996, 273 (284 f.).

richtige Richtung weisen, ist die – im wesentlichen als Erweiterung anzusehende – Überarbeitung des Anlasstatenkataloges teilweise abzulehnen.

Sowohl der bisherige wie auch der geplante Straftatenkatalog des § 100a StPO bzw. StPO-E sind von unübersehbarer Weite. Darum ist es an der Zeit, die ständige Erweiterung der Aufzählung zu beenden und die Eingriffsvoraussetzungen der Telekommunikationsüberwachung grundlegend zu überarbeiten. Aus dem Straftatenkatalog wurden lediglich solche Delikte herausgestrichen, die in der praktischen Anwendung ohnehin kaum eine Rolle spielen<sup>13</sup>, so etwa die Fahnenflucht<sup>14</sup>. Ob eine Straftat in der Praxis überhaupt vorkommt, kann jedoch nicht das alleinige Kriterium dafür sein, ob ihr Verdacht eine solch schwere Eingriffsmaßnahme wie die Telekommunikationsüberwachung rechtfertigen kann. Entsprechend wurde jedoch offenbar verfahren.

Zwar mag für die Eingriffsvoraussetzungen zur Telekommunikationsüberwachung auf der einen Seite ein anderer Maßstab gelten, als er vom *Bundesverfassungsgericht* für den Bereich der akustischen Wohnraumüberwachung ausgefüllt worden ist<sup>15</sup>. Andererseits wiegt die Telekommunikationsüberwachung als Grundrechtseingriff wegen der Erfassung von Kommunikationsinhalten schwerer als die Verbindungsdatenabfrage nach § 100g StPO<sup>16</sup>. Für die Verbindungsdatenabfrage hält der Gesetzgeber als Anlass die Aufklärung von „Straftaten von erheblicher Bedeutung“ für ausreichend. Daher muss die Anlasstat einer Überwachung der Telekommunikationsinhalte – auch bei abstrakter Betrachtung – über diesen Bereich der „Straftaten von erheblicher Bedeutung“ hinausgehen. Ansonsten hätte die gesetzliche Systematik der Eingriffsvoraussetzungen keinen Bezug zur Schwere der mit den Überwachungsmaßnahmen verbundenen Grundrechtseingriffe.

Die vom Gesetzgeber für die Telekommunikationsüberwachung festzulegende Eingriffsschwelle muss folglich auf Straftaten abstellen, die von ihrem Gewicht zwischen einer Straftat von erheblicher Bedeutung und einer besonders schweren Straftat i.S.d. Art. 13 Abs. 3 GG liegen. Die Verwendung des Begriffs der „schweren Straftat“ in Absatz 1 Nr. 1 StPO-E ist daher als Konkretisierung des Gesagten akzeptabel. Ob allerdings die zahlreichen neu in den Straftatenkatalog aufgenommenen Straftatbestände diesen Kriterien entsprechen, erscheint zweifelhaft. Dies gilt beispielsweise für die neu aufgenommenen Fälle von Betrugs- und Urkundendelikten oder von Tatbeständen der Abgabenordnung. Will der Gesetzentwurf auf der einen Seite für eine „geringe Streubreite“ der Maßnahme sorgen<sup>17</sup>, so ist die im Erweiterungskatalog des Entwurfs erkennbare Rundreise durch das ganze Strafrecht schwer damit zu vereinbaren.

Nach § 100a Abs. 1 Nr. 2 StPO-E muss es sich um eine schwere Straftat handeln, die auch im Einzelfall schwer wiegt. Dieses Kriterium ist aufgrund der oben dargestellten notwendigen Diffe-

---

<sup>13</sup> So die BT-Drucks. 16/5846, S. 100; krit dazu *Bergemann*, DuD 2007, 581.

<sup>14</sup> §§ 16, 19 in Verbindung mit § 1 Abs. 3 des Wehrstrafgesetzes; vgl. § 100a Satz 1 Nr. 1 d StPO.

<sup>15</sup> BVerfGE 109, 279 (344).

<sup>16</sup> Vgl. BVerfGE 109, 279 (345).

<sup>17</sup> Vgl. BT-Drucks. 16/5846, S. 95.

renzung zu begrüßen. Es kann jedoch nicht als alleinige Eingrenzung zur Durchführung dieser Maßnahme ausreichen, wie sich aus dem oben Gesagten ergibt.

**b) Postbeschlagnahme (§§ 99, 100 StPO)**

Für die Beschlagnahme von Postsendungen ist bisher ein strafprozessualer Anfangsverdacht gemäß § 152 Abs. 2 StPO ausreichend<sup>18</sup>. Das Postgeheimnis ist als Grundrecht aber in gleicher Weise durch Art. 10 GG geschützt wie das Telekommunikationsgeheimnis; die Eingriffsschranken für das Postgeheimnis und das Telekommunikationsgeheimnis sind im GG identisch geregelt. Grundrechtsdogmatisch ist die bisherige Regelung daher kaum verständlich. Verfahrensrechtlich sollten die Eingriffsvoraussetzungen der §§ 99, 100 an die der Telekommunikationsüberwachung angeglichen werden.

**c) Verkehrsdatenabfrage (§ 100g StPO-E)**

Die Abfrage von Verkehrsdaten aus Telekommunikationsverbindungen wird in § 100g StPO-E neu geregelt. Diese Vorschrift ist in unmittelbarem Zusammenhang mit der geplanten Einführung der Vorratsdatenspeicherung zu sehen, insoweit ist auf Teil C dieser Stellungnahme zu verweisen.

Die Erhebung von Verkehrsdaten spielt in der Strafverfolgungspraxis seit längerem eine erhebliche Rolle. Sie ist nach der Einschätzung von Experten zu einem fast routinemäßig angewandtem Standardermittlungsinstrument geworden, bei dem die bestehenden gesetzlichen Vorgaben von den Beteiligten überwiegend nur noch in pauschalierter Form geprüft werden. Bisher gibt es keine veröffentlichte Statistik zur Anzahl der Auskunftersuchen nach § 100g StPO sowie zur Zahl der davon betroffenen Verbindungsdatensätze. In einer Stellungnahme des Landesbeauftragten für den Datenschutz in Niedersachsen gegenüber dem *Bundesverfassungsgericht* sind Zahlen über die Abfrage von Bestandsdaten mitgeteilt worden, die bereits jetzt auf verfassungswidrige Auswüchse in der Anwendungshäufigkeit der Verkehrsdatenabfragen hinweisen<sup>19</sup>: nach Auskunft der zuständigen Regulierungsbehörde TP fragten die Strafverfolgungsbehörden in 2003 etwa 2,3 Mio. mal Bestandsdaten ab.

Vor diesem Hintergrund ist daran zu erinnern, dass die §§ 100g und 100h StPO durch das Gesetz zur Änderung der StPO vom 20.12.2001 in die StPO eingefügt und bis zum 31.12.2004 befristet wurden<sup>20</sup>. Bis zu diesem Zeitpunkt fand keine Evaluierung statt. Stattdessen wurde die Geltungsdauer durch das Gesetz zur Verlängerung der Geltungsdauer der §§ 100g und 100h StPO

---

<sup>18</sup> Vgl. etwa *Meyer-Goßner*, StPO, 50. Aufl., § 99 Rdnr. 12.

<sup>19</sup> Stellungnahme des LfD Niedersachsen zur Verfassungsbeschwerde gegen die im Niedersächsischen Polizeigesetz vorgesehene präventive TKÜ (1 BvR 668/04). Der Text der Stellungnahme ist auf der Internetseite des LfD Niedersachsen abrufbar unter:  
[http://www.lfd.niedersachsen.de/master/C11884859\\_N11883546\\_L20\\_D0\\_I560.html](http://www.lfd.niedersachsen.de/master/C11884859_N11883546_L20_D0_I560.html).

<sup>20</sup> BGBl. I 2001, S. 3879.

vom 09.12.2004 bis zum 31.12.2007 verlängert<sup>21</sup>. Immerhin nahm der Bundestag eine Entschließung an, mit der die Bundesregierung aufgefordert wurde, bis zum 30.06.2007 einen Erfahrungsbericht vorzulegen. Dabei „soll auch auf Anlass, Ergebnis und Zahl der Betroffenen der Maßnahmen eingegangen werden“<sup>22</sup>. Die Bundesregierung hat bisher weder einen entsprechenden Bericht vorgelegt, noch sind der Begründung zum vorliegenden Gesetzesentwurf statistische Zahlenangaben zur Erhebung von Verkehrsdaten zu entnehmen. Die für eine Evaluierung dringend erforderliche Statistik wird wahrscheinlich erst nach der Beratung des Gesetzesentwurfs fertig gestellt sein<sup>23</sup>. Artikel 13 des Gesetzesentwurfs soll die bis 31.12.2007 geltende Befristung des Ursprungsgesetzes aufheben. Offensichtlich soll die Neuregelung des § 100g StPO-E unbefristet in Kraft treten, ohne dass vorher eine Bewertung der bisherigen Ermittlungspraxis erfolgt. Aus rechtspolitischer Sicht erscheint dies angesichts der erheblichen Erweiterung der Zugriffsbefugnisse der Strafverfolgungsbehörden und des damit verbundenen Eingriffs in das Grundrecht aus Art. 10 Abs. 1 GG äußerst bedenklich.

Für eine künftige Bewertung der Verkehrsdatenabfrage nach § 100g StPO wären die nach Absatz 4 jährlich für Berichtszwecke zu erstellenden Übersichten um folgende Angaben zu ergänzen:<sup>24</sup>

- Anzahl der Anordnungen zur Erhebung von Standortdaten in Echtzeit,
- Anzahl der bei den Anordnungen nach Abs. 1. erhobenen Verkehrsdaten,
- Anzahl der angeordneten „Funkzellenabfragen“ und der dabei erfassten Mobilfunkgeräte und Telekommunikationen,
- Dauer der für die Zukunft angeordneten Erhebungen von Verkehrsdaten,
- Kosten der Verkehrsdatenerhebung.

## II. Schutz des Kernbereichs privater Lebensgestaltung

Nachdem der Kernbereichsschutz für den Bereich des großen Lauschangriffs – wenn auch unzureichend – in die Strafprozessordnung eingefügt wurde, will der Gesetzesentwurf auf Grund der Entscheidung des *Bundesverfassungsgerichts* zum niedersächsischen SOG<sup>25</sup> auch für die Telekommunikationsüberwachung eine entsprechende Regelung in § 100a Abs. 4 StPO-E einfügen.

---

<sup>21</sup> BGBl. I 2004, S. 3231.

<sup>22</sup> BT-Drucks 15/3971, S. 3.

<sup>23</sup> Vgl. Antworten der Bundesregierung auf die Anfragen der Abgeordneten Petra Pau (BT-Prot. 15/131, S. 11975 vom 20.10.2004 sowie BT-Drucksache 16/6079, S. 53 vom 2. Juli 2007).

<sup>24</sup> Zur allgemeine Berichtspflicht s. u. IV. 6.

<sup>25</sup> BVerfG, BVerfGE 113, 348 (391 f.) = NJW 2005, 2603 (2612).

## 1. Kernbereichsschutz nur für Lauschangriff und Telekommunikationsüberwachung?

Der Gesetzentwurf weigert sich ausdrücklich, die Regelungen zum Kernbereichsschutz pauschal auf andere verdeckte Beweiserhebungsmethoden zu übertragen<sup>26</sup>. Er begründet dies mit einer besonderen Stellung des Wohnungsgrundrechts und einer daraus resultierenden Sonderstellung des Lauschangriffs im Verhältnis zu anderen verdeckten Ermittlungsmaßnahmen. Zudem wird auf die zu gewärtigenden Konsequenzen für eine funktionstüchtige Strafrechtspflege hingewiesen: Jede entsprechende Beschränkung bedürfe einer sorgfältigen Abwägung und besonderen Legitimation.

Demgegenüber ist zu betonen: Das *Bundesverfassungsgericht* hat in seiner Entscheidung vom 3. März 2004 zum Großen Lauschangriff in der Strafprozessordnung (§ 100c Abs. 1 Nr. 3 StPO a.F.)<sup>27</sup> Grundsätze für heimliche Datenerhebungen statuiert, die nach nahezu unbestrittener Auffassung der Literatur – mit ausführlicher Begründung insbesondere von *Warntjen*<sup>28</sup> – auch auf andere Rechtsmaterien und Ermittlungsmethoden übertragbar sind<sup>29</sup>. Ausgangspunkt für die dort verlangten Datenerhebungs- und Verwertungsverbote, für Überwachungsabbruch- und Lösungsgebote war der aus der Menschenwürde abgeleitete Kernbereich privater Lebensgestaltung. Dieser Kernbereich privater Lebensgestaltung fällt in den Schutzbereich der Menschenwürde und ist deshalb unantastbar, d.h. auch einer Abwägung mit anderen Rechtsgütern (etwa der Funktionstüchtigkeit der Strafrechtspflege) gerade nicht zugänglich. Dies übersieht der Entwurf, wenn er sich weigert, die entsprechenden kernbereichsschützenden Vorschriften für alle den Kernbereich möglicherweise verletzenden Ermittlungsmethoden vorzusehen. Sollte der Entwurf in der vorliegenden Form zum Gesetz liegen, so wäre hierin ein bewusster Verstoß gegen die Menschenwürdegarantie aus Art. 1 Abs. 1 GG zu sehen.

Wir halten es deshalb für erforderlich, für alle verletzungsgeneigten Maßnahmen einen vor „die Klammer gezogenen“ Kernbereichsschutz zu regeln<sup>30</sup>, der den verfassungsrechtlichen Anforderungen genügt. Dieses ist im Falle des vorgeschlagenen § 100a Abs. 4 StPO nicht hinreichend der Fall.

---

<sup>26</sup> BT-Drucks. 16/5846, S. 52.

<sup>27</sup> *BVerfG*, StV 2004, 169 = NJW 2004, 999 = BVerfGE 109, 279.

<sup>28</sup> *Warntjen*, Heimliche Zwangsmaßnahmen und der Kernbereich privater Lebensgestaltung, Baden-Baden 2007.

<sup>29</sup> *Baldus* in: Schaar (Hrsg.), Folgerungen aus dem Urteil des Bundesverfassungsgerichts zum großen Lauschangriff, S. 19 ff.; *Denninger* in: Roggan (Hrsg.), Lauschen im Rechtsstaat – Gedächtnisschrift für Hans Liskan, Berlin 2004, S. 21 ff.; *Gusy*, JuS 2004, 461; *ders.*, Polizeirecht, 6. Aufl., Tübingen 2006, S. 97; *Kötter*, DÖV 2005, 225; *Kugelman*, Polizei- und Ordnungsrecht, Berlin 2006, 217 f.; *Kutscha* in: Roggan/Kutscha (Hrsg.), Handbuch zum Recht der Inneren Sicherheit, 2. Aufl., Berlin 2006, S. 60f.; *Pieroth/Schlink/Kniesel*, Polizei- und Ordnungsrecht, 3. Aufl., München 2005, S. 277 f.; *Roggan* in: Blaschke/Förster/Lumpp/Schmidt (Hrsg.), Sicherheit statt Freiheit? Berlin 2005, S. 57 ff.; *Schenke*, Polizei- und Ordnungsrecht, 4. Aufl., Heidelberg 2005, S. 114 ff.; *Würtenberger/Heckmann*, Polizeirecht in Baden-Württemberg, 6. Aufl., Heidelberg 2005, S. 292 ff.; a. A. wohl nur *Haas*, NJW 2004, 3082 ff. und *Löffelmann*, NJW 2005, 2033 (2035).

<sup>30</sup> Vgl. etwa § 29 Abs. 6 BbgPolG m. zust. Kommentierung *Roggan*, NJ 2007, 199; ebenso *Bergemann*, DuD 2007, 581 (583).

## 2. Schutz des Kernbereichs in § 100a Abs. 4 StPO-E nur teilweise mit den Vorgaben des Bundesverfassungsgerichts vereinbar

Nach § 100a Abs. 4 StPO-E ist eine inhaltliche Überwachung der Telekommunikation unzulässig, wenn tatsächliche Anhaltspunkte für die Annahme vorliegen, dass durch die Maßnahme allein<sup>31</sup> Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden. Für den Fall der (unbeabsichtigten) Erfassung solcher Inhalte ordnet die Vorschrift ein Verwertungsverbot für das Strafverfahren<sup>32</sup> an. Entsprechende Aufzeichnungen sind zu löschen; sowohl Erlangung wie auch Löschung sind aktenkundig zu machen. In Zweifelsfragen<sup>33</sup> hat die Staatsanwaltschaft unverzüglich eine richterliche Entscheidung zur Verwertbarkeit der Erkenntnisse herbeizuführen. Die gerichtliche Entscheidung zur Unverwertbarkeit ist für das weitere Verfahren<sup>34</sup> bindend.

### a) Vorgaben des Bundesverfassungsgerichts<sup>35</sup>

Das *Bundesverfassungsgericht* hat in jüngerer Zeit, zuletzt im AWG-Beschluss<sup>36</sup>, den Bezug des Telekommunikationsgeheimnisses auf die Menschenwürde mehrfach herausgearbeitet: Bei der (am 21.12.2004 erfolgten<sup>37</sup>) Neuregelung der TKÜ-Befugnisse des Zollkriminalamts seien diejenigen Grundsätze zu beachten, die in den Urteilen vom 14.7.1999<sup>38</sup> und 3.3.2004<sup>39</sup> niedergelegt sind. Zu sichern sei insbesondere ein hinreichender Rechtsschutz für sämtliche Betroffene gegenüber der Datenerhebung und Weiterverwendung sowie die Vernichtung nicht mehr benötigter oder rechtswidrig erhobener Daten. Schließlich sei die Kennzeichnung der erhobenen Daten bei der Verwendung zu weiteren Zwecken zu regeln<sup>40</sup>. Aus diesen Ausführungen ergibt sich unmittelbar, dass auch im Bereich des Telekommunikationsgeheimnisses ein unantastbarer Kernbereich existiert, in den auch nicht im überragenden Allgemeininteresse (etwa zur Verfolgung schwerer oder schwerster Straftaten) eingegriffen werden darf. Die Tatsache, dass die Beteiligten räumlich getrennt sind und deshalb elektronische Kommunikationsmittel nutzen, schließt die Zuordnung ihres Kontakts zur unantastbaren Privatsphäre nicht aus<sup>41</sup>.

Zuletzt bekannte das *Bundesverfassungsgericht* in seinem Urteil zur sog. *präventiven* Telekommunikationsüberwachung im Niedersächsischen Gesetz über die öffentliche Sicherheit und Ordnung (NdsSOG), dass die Bürger zur höchstpersönlichen Kommunikation zwar nicht in gleicher Weise auf Telekommunikation angewiesen seien wie auf eine Wohnung. Jedoch fordere die stets

<sup>31</sup> Dazu im Einzelnen unten II. 2. b (1).

<sup>32</sup> Dazu im Einzelnen unten II. 2. b (2).

<sup>33</sup> Dazu im Einzelnen unten II. 2. b (3).

<sup>34</sup> Dazu im Einzelnen unten II. 2. b (4).

<sup>35</sup> Hierzu schon *Roggan*, StV 2006, 9 ff.

<sup>36</sup> *BVerfG*, NJW 2004, 2213 = BVerfGE 110, 33.

<sup>37</sup> BGBl. I S. 3603.

<sup>38</sup> BVerfGE 100, 313.

<sup>39</sup> *BVerfG*, StV 2004, 169 = NJW 2004, 999 = BVerfGE 109, 279.

<sup>40</sup> *BVerfG*, NJW 2004, 2213 (2222) = BVerfGE 110, 33 (76).

garantierte Unantastbarkeit der Menschenwürde auch im Gewährleistungsbereich des Art. 10 Abs. 1 GG Vorkehrungen zum Schutz individueller Entfaltung im Kernbereich privater Lebensgestaltung<sup>42</sup>. Wie bei großen Lauschangriffen bedarf es folglich auch im Bereich der Telekommunikationsüberwachung kernbereichsschützender Eingriffsregelungen bzw. der Beachtung der verfassungsgerichtlichen Maßgaben<sup>43</sup>.

Sofern die grundsätzliche Übertragbarkeit der verfassungsgerichtlichen Maßgaben aus der Lauschangriff-Entscheidung auf die TKÜ folglich außer Frage steht, ist damit jedoch noch keine Aussage darüber getroffen, *auf welche Weise* sich der obligatorische Kernbereichsschutz im Bereich der TKÜ auswirkt.

Aus dem Lauschangriff-Urteil in Verbindung mit der Abhör-Entscheidung zum NdsSOG lassen sich folgende Kautelen für eine verfassungsgemäße Durchführung einer TKÜ herleiten: In den menschenwürdedefinierten Kernbereich von Art. 10 Abs. 1 GG darf nicht erst eingegriffen werden, um anschließend seine Nicht-Betroffenheit festzustellen<sup>44</sup>. Dabei sind die Anforderungen umso strenger, je größer die Wahrscheinlichkeit ist, dass durch die Abhörmaßnahmen Gespräche höchstpersönlichen Inhalts erfasst würden. Daher sind – je nach Kommunikationspartner eines Beschuldigten oder Nachrichtennitlers – differenzierte Schutzmechanismen bei der Durchführung der Maßnahmen zu beachten. Es bietet sich insoweit eine (mindestens) dreifache Abstufung des – vorgelagerten – Schutzes von Telekommunikationen an:

*(1) Überwachungsverbot bei vorhersehbarer Betroffenheit kernbereichsrelevanter Kommunikation*

In einer *ersten Kategorie*, für Gespräche zwischen „Personen des höchstpersönlichen Vertrauens“<sup>45</sup>, muss grundsätzlich ein Überwachungsverbot gelten. Bei großen Lauschangriffen verlangt das *Bundesverfassungsgericht* „geeignete Vorermittlungen“, die den Charakter der mutmaßlich betroffenen Kommunikationen betreffen<sup>46</sup>. Es spricht nichts dagegen, diese Schutzvorkehrungen auch auf Telekommunikationsüberwachungen zu übertragen. Das wird im Regelfall bedeuten, dass die Polizei vor Beginn einer Maßnahme die Anschlussnummern der Vertrauenspersonen<sup>47</sup> der in § 100a StPO genannten Betroffenen in Erfahrung zu bringen hat (Bestandsdatenerhebung<sup>48</sup>). Zwar bedeutet dies stets eine Datenerhebung bei Dritten. Im Vergleich zur Gefahr der inhaltlichen Kenntnisnahme von vertraulichen Kontakten ist solcherlei Vorermittlung jedoch

<sup>41</sup> Gusy in: Schaar (Hrsg.), Folgerungen aus dem Urteil des Bundesverfassungsgerichts zur akustischen Wohnraumüberwachung, Bonn 2005, S. 51.

<sup>42</sup> BVerfGE 113, 348 (391 f.) = NJW 2005, 2603 (2612) m. Anm. Lepsius, Jura 2006, 929 ff.

<sup>43</sup> So etwa LG Ulm, StV 2006, 8 f.

<sup>44</sup> Vgl. dazu BVerfG, StV 2004, 169 (173) = NJW 2004, 999 (1004) = BVerfGE 109, 279 (323).

<sup>45</sup> BVerfG, StV 2004, 169 (172) = NJW 2004, 999 (1004) = BVerfGE 109, 279 (321).

<sup>46</sup> BVerfG, StV 2004, 169 (173) = NJW 2004, 999 (1004.) = BVerfGE 109, 279 (323).

<sup>47</sup> Dabei ist der Kreis der Vertrauenspersonen nicht vollständig deckungsgleich mit den Zeugnisverweigerungsberechtigten nach §§ 52 f. StPO, vgl. BVerfG, StV 2004, 169 (173) = NJW 2004, 999 (1004) = BVerfGE 109, 279 (322); krit. dazu WeBlau, in: Roggan (Hrsg.), Lauschen im Rechtsstaat, Berlin 2004, S. 61 ff.

vorzugswürdig. Beim Zustandekommen entsprechender Verbindungen gilt die verfassungsgerichtliche Maßgabe, dass schon bei tatsächlichen Anhaltspunkten für die Annahme, dass eine TKÜ Inhalte erfasst, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, eine Überwachung nicht zu rechtfertigen ist und folglich zu unterbleiben hat<sup>49</sup>. Gewiss nicht zufällig recurriert das *Gericht* auf eine Wendung, die sich beispielsweise in § 152 Abs. 2 StPO findet: Es sollen der einschlägigen Umschreibung zufolge zwar keine bloßen Vermutungen für das Vorliegen eines Umstandes ausreichen, wohl aber die nach kriminalistischen Erfahrungen bestehende Möglichkeit<sup>50</sup>. Von einem solchen Verdachtsgrad sagt das *Bundesverfassungsgericht* an anderer Stelle, dass diese Schwelle niedrig liegt<sup>51</sup>. Für Verbindungen zwischen Vertrauenspersonen gilt folglich eine Vermutung der Zugehörigkeit der entsprechenden Kontakte zum Kernbereich privater Lebensgestaltung<sup>52</sup>.

Etwas anderes kann also überhaupt nur dann gelten, wenn die Polizei im Einzelfall über Hinweise darauf verfügt, dass Kommunikationen, die am absoluten Schutz des Kernbereichs des TK-Geheimnisses nicht teilhaben, voraussichtlich erfasst werden (können). Das gilt namentlich dann, wenn ein Straftatverdacht auch gegen die Vertrauensperson des Verdächtigen besteht. Für den auch dann nicht auszuschließenden Fall der Betroffenheit von höchstpersönlicher Kommunikation sind Abbruch- und Lösungsverpflichtungen anzuordnen. Die bloße Aufzeichnung der Kommunikationen und ihre zeitversetzte Auswertung kommen nicht in Betracht.

*(2) Abbruch einer Live-Überwachung bei ungewisser Betroffenheit von kernbereichsrelevanter Kommunikation*

Auch in einer *zweiten Kategorie*, bei der Überwachung von Telekommunikationen mit unterstelltem „Sozialbezug“<sup>53</sup>, sind generell Vorkehrungen für den unerwarteten Fall der Betroffenheit des absolut geschützten Kernbereichs des Telekommunikationsgrundrechts zu treffen. Es handelt sich hier insbesondere um solche Kommunikationen, die dem persönlichen Nahbereich eines Verdächtigen nicht von vornherein zuzurechnen sind und insbesondere um solche Verbindungen, bei denen der Kommunikationspartner den mithörenden Ermittlungspersonen nicht bekannt ist. Zweifelsfrei wird es sich bei dieser Kategorie um die quantitativ größte Gruppe von überwachten Gesprächen handeln. Auch hier sind Abbruch- und ggf. Lösungsverpflichtungen vorzusehen. Das Regel-Ausnahme-Verhältnis aus der ersten Kategorie ist hier jedoch umgekehrt: Eine (Live-)Überwachung und Aufzeichnung ist generell zulässig, es sei denn, dass sich im Einzelfall die Betroffenheit des unantastbaren Kernbereichs des TK-Geheimnisses herausstellt.

---

<sup>48</sup> Vgl. § 2 Nr. 3 TDSV.

<sup>49</sup> *BVerfG*, 1 BvR 668/04 v. 27.7.2005, Abs. 163.

<sup>50</sup> Vgl. nur *Meyer-Goßner*, StPO, 48. Aufl., München 2005, § 152 Rdnr. 4.

<sup>51</sup> *BVerfG*, wistra 2002, 135 (136). Es ließe sich folglich formulieren, dass bereits ein Anfangsverdacht für die Betroffenheit des Kernbereichs privater Lebensgestaltung ausreicht, um ein Überwachungsverbot auszulösen.

<sup>52</sup> Ebenso *Bergemann* in: Roggan (Hrsg.), Lauschen im Rechtsstaat, Berlin 2004, S. 80.

<sup>53</sup> *BVerfG*, StV 2004, 169 (172) = NJW 2004, 999 (1003) = BVerfGE 109, 279 (319).

*(3) Auswertungsverbote und Löschungspflichten bei unerwarteter, zufälliger Betroffenheit von kernbereichsrelevanter Kommunikation*

Die Aufzeichnung bzw. Speicherung von Kommunikationen ohne gleichzeitige Live-Überwachung durch Strafverfolgungsorgane kann nur in einer *dritten Kategorie* zulässig sein: Bei der mutmaßlichen Überwachung von Kommunikationen aus dem – im weitesten Sinne – sozialen Bereich. Betroffen sein können etwa geschäftliche Kontakte oder sonstige flüchtige Bekanntschaften, daneben aber insbesondere Verbindungen zwischen (Mit-) Beschuldigten. Wie in der ersten Kategorie setzt die Einordnung der zu erfassenden Kommunikationen die vorherige Erforschung ihres mutmaßlichen Charakters voraus. Ohne polizeiliche Erkenntnisse, dass voraussichtlich nur Gespräche mit Sozialbezug betroffen sein werden, kommt eine solche Art der Beweiserhebung nicht in Betracht. Allerdings ist anlässlich der Aufzeichnung nicht ausgeschlossen, dass unerwartet ein kernbereichsrelevanter Kommunikationsinhalt betroffen ist. Bei einer „ersten Sichtung“ des Datenmaterials ist folglich zu beachten, dass eine weitere Auswertung dann ausscheidet, wenn unerwartet ein Gespräch zwischen vertrauten Personen aufgenommen wurde. Etwas anderes kann in entsprechenden Fällen nur dann gelten, wenn die Polizei vorab oder spätestens anlässlich der Auswertung erfährt, dass im Einzelfall kein kernbereichsrelevanter Kommunikationsinhalt betroffen ist. Das schließt ein „Filtern“ einer entsprechenden Aufnahme nach straftatbezogener und menschenwürderelevanter (zu löschender) Gesprächsinhalte aus. Denn dies bedeutete unvermeidbar eine (abermalige) Verletzung des unantastbaren Kernbereichs des Telekommunikationsgeheimnisses.

***b) Unzureichender Kernbereichsschutz nach § 100a Abs.4 StPO-E***

Die Regelung des § 100a Abs.4 StPO-E ist verfassungswidrig, soweit sie den Schutz des Kernbereichs privater Lebensgestaltung im Zuge laufender Abhörmaßnahmen auf Verwertungsverbote beschränkt.

Für sich betrachtet begegnet die Regelung des § 100a Abs. 4 Satz 1 StPO-E keinen Bedenken: Die in ihr genannten Kommunikationen sind unzweifelhaft der ersten Kategorie zuzurechnen und verdienen damit den Schutz eines Überwachungsverbots. Unzulänglich ist allerdings, dass außer für diese idealtypische Konstellation keine weiteren Regelungen zum Kernbereichsschutz vorgesehen werden. Der Kernbereichsschutz greift nur in den Fällen, in denen von vornherein tatsächliche Anhaltspunkte dafür vorliegen, dass *allein* kernbereichsrelevante Gespräche betroffen sein werden. Alle anderen Konstellationen, bei denen nur *unter anderem* mit der Betroffenheit des Kernbereichs privater Lebensgestaltung zu rechnen ist, werden im Gesetzentwurf nicht berücksichtigt. Diese Mischkonstellationen (Kommunikationen der zweiten Kategorie) sind jedoch als die mit Abstand am häufigsten vorkommenden Situationen bei einer praktizierten TKÜ anzusehen. Für diesen quantitativ bedeutsamen Bereich der TK fehlt eine gesetzlich festge-

schriebene Verpflichtung, entsprechende – nicht ohne weiteres vorhersehbare – kernbereichsrelevante Gespräche von einer Überwachung auszunehmen<sup>54</sup>.

Eine planmäßige Inkaufnahme des Abhörens von solchen Interaktionen ist mit der Unantastbarkeit des menschenwürde definierten Kernbereichs des Telekommunikationsgeheimnisses nicht zu vereinbaren. Vorzusehen wäre vielmehr die gesetzliche Verpflichtung, dass in solchen Konstellationen die Überwachung unverzüglich abubrechen ist. Das impliziert ein vorzusehendes Gebot der „Live-Kontrolle“ der überwachten Gespräche, denn nur dann ist das planmäßige Risiko des Aufzeichnens von entsprechenden Gesprächen zu verhindern.

Insbesondere ist überraschend, dass die geplante Regelung (überhaupt) kein Gebot zum Abbruch der Überwachung vorsieht. Auf diese Weise wird der obligatorische Kernbereichsschutz, jedenfalls was den Abbruch einer Überwachung angeht, vollständig auf die die TKÜ durchführenden Polizeibeamten delegiert. Diese wäre mit der verfassungsgerichtlich entwickelten Verpflichtung zur Minimierung des Risikos der Verletzung von *unantastbaren* Verfassungswerten<sup>55</sup> offensichtlich nicht zu vereinbaren. Oder, mit anderen Worten: Raum für einen tkü-spezifisch kupierten Kernbereichsschutz lässt die Rechtsprechung des *Bundesverfassungsgericht* offensichtlich nicht.

Zu begrüßen ist allerdings, dass der Wortlaut des Entwurfs – im Gegensatz zum Referentenentwurf – nunmehr die Unverwertbarkeit von Daten, die unter Verstoß gegen Erhebungsverbote erlangt wurden, festschreibt. Das *Bundesverfassungsgericht* verbietet insoweit „jede“ Verwertung<sup>56</sup>. Aus Gründen der Klarstellung sollte diese Formulierung in den Gesetzestext übernommen werden.

### III. Schutz von Zeugnisverweigerungsrechten

Die im Gesetzentwurf vorgenommene Unterscheidung verschiedener Klassen von Zeugnisverweigerungsberechtigten gewährleistet keinen hinreichenden Grundrechtsschutz für die Betroffenen und wird als sachwidrig abgelehnt. Außerdem sollten die Schutzansprüche der Zeugnisverweigerungsberechtigten nicht durch weiche Abwägungsklauseln relativiert oder zu weite Ausnahmeregelungen im Falle angeblicher Tatbeteiligungen aufgeweicht werden. Der Schutz der Zeugnisverweigerungsberechtigten muss sich auf alle verdeckten Ermittlungsmaßnahmen beziehen<sup>57</sup>.

---

<sup>54</sup> Derselbe – zu beanstandende – Befund findet sich auch in anderen Gesetzen, etwa § 23a Abs. 4a ZFdG.

<sup>55</sup> BVerfGE 109, 279 (315).

<sup>56</sup> BVerfGE 109, 279 (328).

<sup>57</sup> Vgl. dazu die Beiträge in *Wolter/Schenke* (Hrsg.), Zeugnisverweigerungsrechte bei (verdeckten) Ermittlungsmaßnahmen, Berlin 2002.

## 1. Notwendigkeit eines einheitlichen Schutzes (§ 53b Abs. 1 und 2 StPO-E)

Der Entwurf knüpft an das in § 53 StPO vorgesehene Zeugnisverweigerungsrecht für Berufsgeheimnisträger an. Er unterscheidet jedoch, anders als § 53 StPO, zwischen Geistlichen, Strafverteidigern sowie Abgeordneten in Abs. 1 auf der einen Seite und Rechtsanwälten, Steuerberatern, Ärzten und ähnlichen Personen sowie Journalisten in Abs. 2 auf der anderen Seite. Bei der erstgenannten Gruppe sollen Ermittlungsmaßnahmen schlicht unzulässig sein, bei der zweiten Gruppe soll dies „im Rahmen der Prüfung der Verhältnismäßigkeit unter Würdigung des öffentlichen Interesses“ zulässig sein. Diese Unterscheidung ist unberechtigt. Das Zeugnisverweigerungsrecht ist zu Recht in § 53 StPO unterschiedslos für diese Personen garantiert, weil neben dem Interesse derjenigen Menschen, die sich diesen Personen anvertrauen, auch ein überragendes Allgemeininteresse daran besteht, dass das Vertrauensverhältnis zu allen in § 53 StPO genannten Personen uneingeschränkt bestehen bleibt. Ermittlungsmaßnahmen, durch die voraussichtlich Erkenntnisse erlangt würden, über die der betroffene Berufsgeheimnisträger das Zeugnis verweigern dürfte, sollten daher in § 53b StPO-E unterschiedslos für unzulässig erklärt werden<sup>58</sup>.

Dasselbe gilt für die Zeugnisverweigerungsrechte aus persönlichen Gründen nach § 52 StPO. Die Entscheidung des *Bundesverfassungsgerichts* zum Großen Lauschangriff hat deutlich gemacht, dass gerade diese Personen, bei denen es um den Kernbereich privater Lebensgestaltung geht, aus Gründen der Menschenwürde genauso zu schützen sind wie Berufsgeheimnisträger<sup>59</sup>. § 53b Abs. 1 StPO-E sollte sich daher – unter vollständiger Streichung des Abs. 2 – auf alle in §§ 52, 53 StPO genannten Personen beziehen.

## 2. Notwendigkeit eines absoluten Schutzes (§ 53b Abs. 2 StPO-E)

Schon unter Bestimmtheitsgesichtspunkten unzulänglich ist die in § 53b Abs. 2 StPO-E enthaltene Abwägungsklausel, die trotz ihrer beachtlichen Länge nicht verbergen kann, dass ihr jeder objektiv messbare Maßstab fehlt, der auch nur ein Minimum an Voraussehbarkeit ermöglichen würde, ob eine Ermittlungsmaßnahme zulässig ist oder nicht. Es sind weder rechtliche, noch allgemein gültige gesellschaftliche oder ethische Regeln erkennbar, nach denen die Verhältnismäßigkeit im Einzelnen, zwischen irgendeiner Straftat einerseits und z.B. dem unbelauschten Gespräch mit dem Arzt andererseits, frei von subjektiver Willkür entschieden werden könnte.

Gegen solche Regelungen, die in Wirklichkeit die Sachentscheidung völlig der Exekutive überlassen, hat sich das *Bundesverfassungsgericht* schon 1957 mit dem sog. Elfes-Urteil entschieden gewandt und diese in grundrechtsrelevanten Bereichen für unzulässig erklärt: Der Gesetzgeber dürfe "sich seines Rechts, die Schranken der Freiheit zu bestimmen, nicht dadurch begeben, dass

<sup>58</sup> Ebenso *Bergemann*, DuD 2007, 581 (584).

<sup>59</sup> BVerfGE 109, 279 (328 ff.).

er mittels einer vagen Generalklausel die Grenzziehung im einzelnen dem Ermessen der Verwaltung überlässt."<sup>60</sup>

Dem Gesetzgeber muss dringend geraten werden, die drastische Einschränkung des Zeugnisverweigerungsrechts zu überdenken. Zumindest müssten die Maßstäbe der Verhältnismäßigkeit konkretisiert und auch in diesen Fällen zwingend vorgesehen werden, dass ein Eindringen in den Kernbereich der privaten Lebensführung absolut unzulässig ist<sup>61</sup>, dass ein Verstoß gegen die gesetzlichen Bestimmungen die Verwendung der erzielten Erkenntnisse in jeder Weise unzulässig macht<sup>62</sup> und dass bei der Berührung von Zeugnisverweigerungsrechten die Freigabe erzielter Erkenntnisse für jede Art der Verwendung durch ein Gericht erfolgen muss.

Das zugrunde liegende Regelungskonzept mit der im Einzelfall vorzunehmenden Verhältnismäßigkeitsprüfung erscheint schließlich für die Praxis schwer handhabbar, insbesondere wenn man berücksichtigt – wie auch in der Begründung<sup>63</sup> ausgeführt –, dass die Prüfung zu unterschiedlichen Zeitpunkten des Verfahrens zu unterschiedlichen Ergebnissen führen kann.

### 3. Keine Umgehung der Zeugnisverweigerungsrechte (§ 53b Abs. 4 StPO-E)

Die Regelung in § 53b Abs. 4 StPO-E lässt das bekannte Problem offen, dass gegen Journalisten, die an der Veröffentlichung eines Amtsgeheimnisses beteiligt sind, ein Strafverfahren eingeleitet werden kann, um das ihnen zustehende Zeugnisverweigerungsrecht zu nehmen. Regelmäßiges Ziel solcher Ermittlungsverfahren ist es, redaktionelle Unterlagen beschlagnahmen und verdeckte Ermittlungen einleiten zu können. Dem Bundestag liegen zum Schutz der Pressefreiheit eine Reihe von Gesetzesentwürfen vor<sup>64</sup>, die bisher nicht verabschiedet wurden. Das ist hier erneut anzumahnen.

Es darf nicht dazu kommen, dass Zeugnisverweigerungsrechte (und damit auch Beschlagnahmeverbote) dadurch unterlaufen werden, indem man die zeugnisverweigerungsberechtigten Personen für der Täterschaft oder der Beihilfe verdächtig erklärt. Die Regelung in § 53b Abs. 4 StPO-E ermöglicht eine Umgehung des umfassenden Schutzes der Berufsheimnisträger bereits dann, wenn lediglich ein einfacher Anfangsverdacht der Tatbeteiligung gegen den Berufsheimnisträger vorliegt. Gem. § 152 Abs. 2 StPO genügen hierfür zureichende tatsächliche Anhaltspunkte. Diese Schwelle des Anfangsverdachts liegt niedrig<sup>65</sup>. Bereits bei abstrakter Betrachtung lässt sich damit der Schutz der Zeugnisverweigerungsberechtigten auf äußerst einfache Weise aushebeln. Bevor der Gesetzgeber derart weitreichende Eingriffe in Grundrechte vornimmt, müsste

---

<sup>60</sup> *BVerfG*, NJW 57, 297 ff.; vgl. auch *BVerwG*, NJW 55, 1693.

<sup>61</sup> Siehe oben II.

<sup>62</sup> Siehe unten IV. 2.

<sup>63</sup> Siehe BT-Drucks. 16/5846, S. 89.

<sup>64</sup> BT-Drucks. 16/956; BT-Drucks. 16/576 sowie BR-Drucks. 650/06.

<sup>65</sup> *BVerfG*, wistra 2002, 135 (136).

zumindest eine empirisch belastbare Evaluation der Frage nachgehen, ob es in der Praxis bereits zu einer Fehlanwendung entsprechender Vorschriften oder sogar zu Missbrauchsfällen gekommen ist.

Als Eingriffskriterium für § 53b Abs. 4 StPO-E ist daher mindestens eine Formulierung zu fordern, nach der **bestimmte Tatsachen** die Annahme einer Tatbeteiligung rechtfertigen.

Ähnlich stellt sich die Thematik bei § 97 Abs. 5 StPO-E dar. Auch diese Regelung bezieht sich auf die bereits zu § 53b Abs. 4 angesprochene Möglichkeit einer Aushebelung der Pressefreiheit, insbesondere bei der Beteiligung von Journalisten bei der Veröffentlichung von Amtsgeheimnissen. Das Problem bleibt trotz der hier vorgeschlagenen Ergänzung ungelöst.

## IV. Verfahrenssicherungen

Der Grundgedanke, allgemeine Verfahrensregeln für möglichst alle verdeckten Maßnahmen zu formulieren, ist richtig. Die vorgeschlagenen Regelungen erfüllen aber nur teilweise die verfassungsrechtlichen Erfordernisse.

### 1. Begründungspflichten

Nach der 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, hätte erwartet werden können, dass der Entwurf konkrete Begründungspflichten regelt<sup>66</sup>. So konstatiert die Untersuchung von *Backes* und *Gusy* eine Erosion des Richtervorbehaltes und den „weitgehenden Verzicht der Richter selbst, die ihnen vom Gesetz aufgebene eigenständige und grundrechtsorientierte Prüfung der staatsanwaltschaftlichen Anträge auf Telefonüberwachung vorzunehmen“<sup>67</sup>.

Dennoch will der Entwurf – außer in den Fällen des § 100d StPO – auf eine gesetzlich normierte Pflicht zur einzelfallbezogenen Begründung verzichten. Nach der Entwurfsbegründung soll hiervon abgesehen werden, „da die Anordnungsvoraussetzungen für die Telekommunikationsüberwachung, insbesondere mit Blick auf die bei der akustischen Wohnraumüberwachung erforderliche qualifizierte Kernbereichsprognose, insgesamt geringer sind.“<sup>68</sup> Diese Begründung ist nicht nachzuvollziehen. Es besteht kein logischer Zusammenhang zwischen den materiellen Anforde-

<sup>66</sup> MPI-Studie S. 231; hierzu kritisch *Bizer*, KrimJ 2003, 280; *Bergemann*, in: Roggan (Hrsg.), *Lauschen im Rechtsstaat*, Berlin 2004, S. 71.

<sup>67</sup> *Backes/Gusy* u. a., StV 2003, 249 (252).

<sup>68</sup> Siehe BT-Drucks. 16/5846, S. 112.

rungen eines Grundrechtseingriffs und den Anforderungen an die Ausgestaltung der schriftlichen Begründung des richterlichen Beschlusses. Der Verweis auf die verfassungsrechtliche Rechtsprechung ist – wie sich aus den empirischen Erkenntnissen zur gängigen Praxis ergibt – leider (!) nicht ausreichend, um die Gerichte zur Ausübung ihrer Kontrollpflichten anzuhalten<sup>69</sup>.

Abzulehnen sind auch Formulierungen wie in § 100b Abs. 2 Satz 2 Nr. 1 StPO-E, die zwar die formalen Anforderungen an richterliche Beschlüsse betreffen, in Wirklichkeit aber eine Aufweicheung in materieller Hinsicht zur Folge haben. Nach dieser Vorschrift sind in der Anordnung künftig der Name und die Anschrift des Betroffenen nur noch „soweit möglich“ anzugeben. Dies würde Maßnahmen auch gegen „Unbekannt“ erlauben und die Prüfung der Anordnungsvoraussetzungen beeinträchtigen.

## 2. Verwertungsverbot für unrechtmäßig erlangte Erkenntnisse (Vorschlag: § 101 Abs. 1a StPO)

Wie die Studien des MPI und der Universität Bielefeld gezeigt haben<sup>70</sup>, ist die richterliche Kontrolle geheimer Ermittlungsmethoden völlig unzureichend, um die Einhaltung gesetzlicher Bestimmungen in diesem Bereich sicherzustellen. Dies belegen auch die ununterbrochen immer wieder erforderlich werdenden Entscheidungen des *Bundesverfassungsgerichts* im Bereich unzulässiger Wohnungsdurchsuchungen<sup>71</sup> und generell unzureichender Sicherung der Grundrechte im Rahmen von Ermittlungsmaßnahmen<sup>72</sup>.

Das allein Erfolg versprechende Mittel, die strikte Einhaltung gesetzlicher Vorgaben zum Schutz der Grundrechte bei verdeckten Ermittlungsmaßnahmen sicherzustellen, ist ein striktes und uneingeschränktes Verwertungsverbot für alle Erkenntnisse, die auf unzulässige Weise gewonnen worden sind<sup>73</sup>. Solange verdeckt tätige Ermittlungsbehörden darauf hoffen können, gewonnene Erkenntnisse (auch, aber nicht nur personenbezogene Daten) nutzen zu können, werden möglicherweise die Grenzen der Befugnisse weitest möglich – unter Hinnahme des Risikos einer Überschreitung – ausgereizt. Wenn unzulässig gewonnene Erkenntnisse einem strikten Verwertungsverbot unterliegen, haben die Ermittlungsbehörden einen zusätzlichen Anreiz, den Rand des Zulässigen nicht zu überschreiten.

Die Gesetzesbegründung führt aus, dass die Regelungen über Erhebungs- und Verwertungsverbote auch deshalb nicht zu sehr eingeschränkt werden dürften, weil sie die Wahrheitsermittlung beschränken könnten und damit „nicht nur das rechtsstaatliche Gemeinwesen, sondern auch das

---

<sup>69</sup> Krit. dazu auch *Bergemann*, DuD 2007, 581 (585).

<sup>70</sup> Siehe oben Fn. 1 und 2.

<sup>71</sup> Jüngst *BVerfG*, NJW 2006, 3411 f.

<sup>72</sup> Vgl. statt vieler etwa zur Wohnungsdurchsuchung *BVerfGE* 103, 142; zur DNA-Analyse *BVerfGE* 103, 21.

<sup>73</sup> So auch schon *Hirsch*, *Ausfernde Telefonüberwachung im Strafverfahren*, in: *Grundrechte-Report* 1998, Seite 131 ff. und *Müller-Heidelberg*, *Deutschlands Überwachungskultur*, in: *Grundrechte-Report* 2004, S. 101 ff.

Recht des Beschuldigten auf ein faires, rechtsstaatliches Verfahren beeinträchtigen, weil die aufgrund von Erhebungs- und Verwertungsverböten nicht erlangten Erkenntnisse nicht nur der Anklage sondern auch der Verteidigung entzogen sind.“<sup>74</sup> Diese Erwägung liegt schon deshalb neben der Sache, weil z.B. eine Telekommunikationsüberwachung zur Strafverfolgung durchgeführt wird, jedoch wohl kaum im Interesse der Verteidigung des Beschuldigten. Überdies ließe sich das im Entwurf angesprochene Risiko einer Beschränkung der Verteidigungsmöglichkeiten dadurch ausschließen, dass die Verwertbarkeit der durch eine rechtswidrige Eingriffsmaßnahme erlangten Erkenntnisse von der Zustimmung des Beschuldigten abhängig gemacht würde.

Ein striktes Verwertungsverbot unzulässig erlangter Erkenntnisse widerspricht weder dem System der Strafprozessordnung noch erschwert es die verfassungsrechtlich gebotene Strafverfolgung in unangemessener Weise: Nach § 136a Abs. 3 StPO gibt es schon immer ein absolutes Verwertungsverbot, wenn die Freiheit der Willensentschließung und der Willensbetätigung des Beschuldigten durch Misshandlung, Ermüdung, körperlichen Eingriff, Verabreichung von Mitteln, Quälerei, Täuschung, Hypnose oder Drohung beeinträchtigt worden ist und so auf unzulässige Weise Aussagen erreicht wurden.

Daher wird folgende allgemeine Regelung für ein umfassendes Verwertungsverbot vorgeschlagen:

*§ 101 Abs. 1a:*

*Erkenntnisse, die aufgrund von Maßnahmen gemäß Abs. 1 gewonnen worden sind, sind sowohl in dem Verfahren, in dem diese Maßnahmen angeordnet wurden, als auch für sämtliche anderen etwaigen Verfahren und Maßnahmen unverwertbar, wenn die Maßnahme unter Verstoß gegen die Vorschriften der Strafprozessordnung entweder angeordnet oder durchgeführt worden ist. Dies gilt auch für nachträgliche Feststellungen der Rechtswidrigkeit. Ist eine Maßnahme zunächst zulässig und wird später unzulässig, so gilt das Verwertungsverbot ab dem Zeitpunkt der Unzulässigkeit.*

Schließlich ist die Regelung über die Verwertung von Erkenntnissen aus staatsanwaltschaftlich angeordneten Eilmaßnahmen zu bemängeln. Wenn nämlich diese Eilmaßnahme vom Gericht nicht bestätigt wird, dann liegen offenbar ihre gesetzlichen Voraussetzungen nicht vor. Die Maßnahme war in diesem Falle rechtswidrig. Sie muss daher rückwirkend aufgehoben werden, ihre Ergebnisse sind unverwertbar. Es ist nicht akzeptabel, dass der Entwurf regeln will, dass solche rechtswidrig erlangten Erkenntnisse als Ermittlungsansätze verwendet werden können. Es muss – wie dargelegt – besonders in diesem Falle ein umfassendes Verwertungsverbot gelten.

---

<sup>74</sup> BT-Drucks. 16/5846, S. 59

### 3. Die Unterrichtung des anordnenden Gerichts muss auf alle durchgeführten verdeckten Ermittlungsmaßnahmen ausgedehnt werden

Die Erweiterung der Unterrichtungspflicht auch auf Verlauf und Ergebnisse der Maßnahme ist nachdrücklich zu begrüßen. Nur so erhalten die Gerichte die erforderlichen Rückmeldungen, die sie bei weiteren Entscheidungen bei derselben Maßnahme – z.B. über Verlängerungsanträge – oder generell bei künftigen Entscheidungen für eine sachgerechte Wahrnehmung der mit dem Richtervorbehalt bezweckten rechtsstaatlichen Kontrolle der Maßnahmen benötigen.

Allerdings ist eine solche Pflicht nur bei der Telekommunikationsüberwachung (§ 100b Absatz 4 Satz 2 StPO-E) und bei der akustischen Raumüberwachung (§ 100d Abs. 4 StPO-E) vorgesehen. Im Interesse einer fundierteren gerichtlichen Kontrolle sollte die im § 100b Abs. 4 Satz 2 StPO-E vorgesehene Regelung auf alle übrigen verdeckten Ermittlungsmaßnahmen ausgedehnt werden. Zumindest müsste die Regelung aber bei solchen Überwachungsmaßnahmen Anwendung finden, die in den Schutzbereich des Art. 10 GG eingreifen: Neben § 100b Abs. 4 Satz 2 StPO-E wären dies § 99 (Postbeschlagnahme), § 100g (Verkehrsdatenerhebung), ebenso bei der diesem Bereich zumindest nahe liegenden Maßnahme gemäß § 100i (IMSI-Catcher).

### 4. Benachrichtigung der Betroffenen (§ 101 Abs. 4–7 StPO-E)

§ 101 Abs. 4 StPO-E spricht bei den zu benachrichtigenden Personen in Ziff. 4b von "sonstigen überwachten Personen" und in Nr. 5 ff. von "erheblich mitbetroffenen Personen". Diese Begriffe sind unklar. Unter "sonstige überwachte Person", die nicht Beschuldigte sind, sollte jede Person verstanden werden, die in irgendeiner Weise in den Lauschangriff geraten ist, deren Grundrechte also verletzt worden sein können. Als erheblich mitbetroffene Person sollte zumindest auch jede Person verstanden werden, die ein Zeugnisverweigerungsrecht hat oder gegen die die erzielten Erkenntnisse in irgendeinem Verfahren als Ermittlungsansätze verwendet wurden.

Die Regelung des Absatzes 5 lässt bei Maßnahmen nach § 110a StPO (Verdeckter Ermittler) die Verschiebung der Benachrichtigung auch dann zu, wenn sonst die weitere Einsetzung des Ermittlers gefährdet wäre. Es liegt auf der Hand, dass es in diesen Fällen danach kaum jemals zu einer Benachrichtigung kommen dürfte. Das *Bundesverfassungsgericht* hat jedenfalls bei dem Lauschangriff eine solche Klausel für verfassungswidrig erklärt<sup>75</sup>. Eine Benachrichtigung über andere Ermittlungsmaßnahmen darf nicht deswegen ausscheiden, weil daran auch ein verdeckter Ermittler beteiligt war. Es ist unverständlich, weshalb der Gesetzentwurf dies nicht berücksichtigt.

Es ist nicht zu erkennen, warum mit einer Benachrichtigung jedenfalls bis zu 12 Monate gewartet werden kann, ehe ein Gericht eingeschaltet werden muss. Die Frist von 6 Monaten sollte für alle in Betracht kommenden Fälle genügen.

---

<sup>75</sup> BVerfGE 109, 279 (366).

Das Ende der Benachrichtigungspflicht nach 5 Jahren gem. Absatz 7 ist nicht akzeptabel. Sie wäre allenfalls in dem Sinn denkbar, dass eine Benachrichtigung spätestens nach 5 Jahren erfolgen muss. Wir schlagen daher folgende Formulierung vor:

*§ 101 Abs. 7:*

*Spätestens fünf Jahre nach Beendigung der Maßnahme sind die Beteiligten gem. Abs. 4 zu benachrichtigen.*

Für den Großen Lauschangriff würden durch diese Regelungen die bisherigen Benachrichtigungspflichten wesentlich gelockert werden. Eine Verfallsfrist gibt es bisher nicht. Bei einer Zurückstellung von mehr als 18 Monaten muss das *OLG* über eine weitere Verlängerung entscheiden. Diese Regelungen sollten erhalten bleiben und zumindest auch für die Aufzeichnung des gesprochenen Wortes außerhalb einer Wohnung und für Maßnahmen der Telekommunikationsüberwachung gelten.

Nochmals überprüft werden sollte auch die Vollständigkeit des Kataloges der Maßnahmen, auf Grund derer eine Benachrichtigungspflicht besteht. So werden nach der geplanten Regelung beispielsweise nicht alle Betroffenen des Einsatzes von *IMSI-Catchern* benachrichtigt, da dort nur die Zielperson genannt ist.

#### **5. Rechtsschutz gegen Ermittlungsmaßnahmen (§ 101 Abs. 9 StPO-E) mit zu kurzer Frist**

Die vorgeschlagene Regelung des Rechtsschutzes gegen verdeckte Ermittlungsmaßnahmen ist ausdrücklich zu begrüßen.

Die Frist von 14 Tagen für den Antrag auf Überprüfung der Rechtmäßigkeit der Maßnahme erscheint allerdings wesentlich zu kurz. Sie sollte mindestens auf einen Monat heraufgesetzt werden. Hierbei ist zu berücksichtigen, dass die verdeckte Ermittlungsmaßnahme dem Betroffenen bislang nicht bekannt war. Anders als etwa beim Strafbefehl – bei dem eine ähnlich kurze Frist für den Einspruch gilt – ist der Betroffene vorher nicht angehört worden (§ 33 Abs. 4 StPO). Die Benachrichtigung dürfte für diesen damit in der Regel überraschend kommen. Anders als im laufenden gerichtlichen Verfahren hatte er zudem bislang keine Gelegenheit, sich einen Verteidiger zu suchen. Damit dürften viele Betroffene, denen zumeist jede juristische Ausbildung fehlt, mit einer so kurzen Frist überfordert sein.

#### **6. Unzureichende Berichtspflichten zur TK-Überwachung (§ 100b Abs. 5 f. StPO-E)**

Die im § 100b Abs. 5 f. StPO-E vorgesehene erweiterte statistische Erhebung über Maßnahmen der Telekommunikationsüberwachung ist zu begrüßen. Sie ist für Evaluierungszwecke unerlässlich. Eine solche Regelung mit jeweils bereichsspezifischen statistischen Erhebungen ist für alle übrigen verdeckten Ermittlungsmaßnahmen, die im § 101 Abs. 1 aufgeführt sind, erforderlich,

wenigstens aber für alle Maßnahmen, die in den Schutzbereich des Art. 10 GG eingreifen (siehe oben).

In Absatz 5 fehlt eine Bestimmung darüber, bis wann die Jahresstatistik zu veröffentlichen ist. Neben der Veröffentlichung im Internet sollte sie auch formell dem Bundestag zugeleitet werden. Bei den zu veröffentlichenden Daten fehlt die Angabe, in welcher Weise die Überwachung "relevant" war, ob die Beteiligten benachrichtigt wurden und ob in dem vorhergehenden Bericht mitgeteilte Zurückstellungen der Benachrichtigung inzwischen nachgeholt wurden oder nicht. Schließlich sollten die durch die Maßnahme entstandenen Kosten angegeben werden. Ohne diese Angaben ist eine wirkliche Beurteilung der Angemessenheit der Überwachung nicht möglich.

Die Verpflichtung, die Anzahl „der Beteiligten der überwachten Telekommunikation“ anzugeben, bezieht sich nur auf die betroffenen Anschlussinhaber. Tatsächlich betroffen sind aber nicht nur die jeweiligen Anschlussinhaber, sondern auch alle Kommunikationspartner, die von diesem Anschluss angerufen wurden oder die von sich aus den fraglichen Anschluss angerufen haben. Dass deren Anzahl beträchtlich höher ist als die Anzahl der Beteiligten, belegt die MPI-Studie<sup>76</sup>, auf die im Entwurf wiederholt eingegangen wird. Danach wurden bei 21 % der Maßnahmen nach § 100a StPO jeweils 1.000 bis 5.000 Gespräche, in weiteren 8 % jeweils über 5.000 Gespräche, in einem Einzelfall sogar 30.500 Gespräche abgehört<sup>77</sup>. Für die mit der Berichtspflicht nach Abs. 6 bezweckte Evaluierung wäre es unbedingt erforderlich, auch die Zahl der in diesem Sinn von einer TKÜ Betroffenen mitzuerfassen.

Zu kritisieren ist schließlich, dass Angaben zum Erfolg der Maßnahmen, die im Referentenentwurf noch vorgesehen waren (dort Abs. 6 Nr. 5 und 6), nun nicht mehr erhoben werden sollen. Sie sind für eine sachgerechte Erfolgskontrolle aber unverzichtbar. Es kann nicht Aufgabe von Gutachtern sein, derartige Angaben mühsam stichprobenweise per Interview und Aktenrecherche im Nachhinein zu ermitteln, vielmehr ist es eine *genuine* Aufgabe des Gesetzgebers, den Erfolg der von ihm beschlossenen Regelungen selbst zu beobachten und ggf. zeitnah die notwendigen Konsequenzen für notwendige Änderungen zu ziehen. Dies gilt in besonderer Weise, wenn es sich um Regelungen handelt, die – wie die Telekommunikationsüberwachung – tief die Freiheitsrechte der Bürgerinnen und Bürger einschneiden. Für diese Erfolgskontrolle müssen die Angaben zum Erfolg der Einzelmaßnahmen zur Verfügung stehen. Das in der Begründung des Referentenentwurfs angeführte Gegenargument des zusätzlichen Aufwandes<sup>78</sup> überzeugt jedenfalls nicht.

---

<sup>76</sup> Siehe oben Fn. 1.

<sup>77</sup> A.a.O., S. 444.

<sup>78</sup> Referentenentwurf, S. 103.

## C. Die Umsetzung der Richtlinie zur Vorratsdatenspeicherung (RL 2006/24/EG)

### I. Die europarechtswidrige Richtlinie

#### 1. Die Entstehung der Richtlinie

Nach den Anschlägen vom 11. März 2004 in Madrid hat sich die Diskussion um die Einführung einer europaweit harmonisierten Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten intensiviert. Auf dem EU-Gipfel am 25. März 2004 wurde eine Erklärung gegen den Terrorismus angenommen und der Rat erhielt den Auftrag, Rechtsvorschriften für die Vorratsdatenspeicherung durch die Telekommunikationsanbieter zu erarbeiten. Der von Irland, Frankreich, Schweden und Großbritannien vorgelegte und auf Art. 31 Abs. 1 Buchstabe c und 34 Abs. 2 Buchstabe b EUV gestützte Entwurf eines entsprechenden Rahmenbeschlusses wurde sehr kontrovers diskutiert, scheiterte letztlich aber an der fehlenden Einstimmigkeit<sup>79</sup>. Daraufhin legte die Europäische Kommission am 21. September 2005 einen Entwurf für eine entsprechende Richtlinie nach Art. 95 EGV vor. Trotz der mehrfach geäußerten Bedenken gegen die Rechtmäßigkeit der gewählten Rechtsgrundlage sowie gegen den Regelungsinhalt wurde der Entwurf bereits am 14. November 2005 in erster Lesung verabschiedet<sup>80</sup>. Nachdem der zur Annahme der Richtlinie notwendige Mehrheitsbeschluss des Rates der Justiz- und Innenminister am 21. Februar 2006 zu Stande kam, ist die „Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG“ (Vorratsdatenspeicherungsrichtlinie) am 3. Mai 2006 in Kraft getreten.

Der Bundestag hat von der Bundesregierung gefordert, bei der Umsetzung der Richtlinie zur Vorratsdatenspeicherung nicht über die Vorgaben der Richtlinie hinaus zu gehen<sup>81</sup>. Die Bundesregierung erklärte ihrerseits, dieser Forderung folgen zu wollen. Mit dem vorgelegten Gesetzentwurf hat sie sich von diesem Versprechen verabschiedet.

---

<sup>79</sup> Ratsdokument 8958/04.

<sup>80</sup> Im Europäischen Parlament wurde die Richtlinie mit den Stimmen der Sozialdemokraten und Christdemokraten (378 Stimmen, 197 Gegenstimmen, 30 Enthaltungen) verabschiedet. Zwischen der Vorlage des Richtlinienentwurfs und der entscheidenden Lesung lagen lediglich drei Monate.

<sup>81</sup> BT-Drucks. 16/545, S. 4. Der Deutsche Bundestag hat im Übrigen lange die Einführung einer Vorratsdatenspeicherung abgelehnt, der Bundesrat hat sich hingegen als ihr Befürworter erwiesen. Zu den früher geäußerten Positionen des Bundestages, der Bundestagsfraktionen und des Bundesrates zur Vorratsdatenspeicherung vgl. BT-Drucks. 15/3773, BT-Drucks. 15/4748; BT-Drucks. 15/4597; BT-Drucks. 16/128; BT-Drucks. 16/237; BT-Drucks. 16/545, BT-Drucks. 16/690, BT-Drucks. 16/1622; BR-Drucks. 275/02; BR-Drucks. 755/03. Zur wissenschaftlichen Auseinandersetzung mit dem Thema in Deutschland vgl. *Breyer*, Die systematische Aufzeichnung und Vorhaltung von Telekommunikations-Verkehrsdaten für staatliche Zwecke in Deutschland, Berlin 2005; *ders.*, RDV 2003, S. 218f.; *ders.*, RDV 2004, S. 147f.; *Büllingen*, DuD 2005, S. 349f.; *Hoffmann-Riem*, AöR 123 (1998), S. 513f.; *Westphal*, EuZW 2006, S. 555f.

## 2. Richtlinieninhalt

Nach der Vorratsdatenspeicherungsrichtlinie müssen die Mitgliedsstaaten dafür Sorge tragen, dass die Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste sowie die Betreiber öffentlicher Kommunikationsnetze verpflichtet werden, die im Zuge der Bereitstellung ihrer Dienste erfassten Verkehrsdaten über den betrieblichen Bedarf hinaus, also *ohne einzelfallbezogenen Anlass*, auf Vorrat zu speichern. Diese Daten sind unter bestimmten Voraussetzungen den zuständigen Behörden zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten zur Verfügung zu stellen (Art. 1 Abs. 1, Art. 3 Abs. 1 RL 2006/24/EG). Mit den gespeicherten Daten sollen die eindeutige Rückverfolgung und Identifizierung der Quelle und des Adressaten einer Nachricht nach Datum, Uhrzeit, Dauer und Art der Nachrichtenübermittlung sowie die Bestimmung der Endeinrichtung und des Standorts mobiler Geräte möglich werden (Art. 5 Abs. 1 RL). Gespeichert werden sollen beispielsweise die Rufnummer des anrufenden und des angerufenen Anschlusses, der Beginn und das Ende der Verbindung, bei mobilem Telefonieren auch die Kennung der Mobilfunkkarten und der Endgeräte, bei Diensten der elektronischen Post die E-Mail-Adresse und die Benutzererkennung des Absenders und des Empfängers der übermittelten Nachricht, bei Internetnutzung die zugewiesenen Internetprotokolladressen usw. Die Richtlinie gibt eine Speicherdauer von mindestens sechs Monaten und höchstens zwei Jahren für diese Verbindungsdaten vor. Daten, die Aufschluss über die Kommunikationsinhalte geben, dürfen nicht auf Vorrat gespeichert werden (Art. 5 Abs. 2 RL). Die Umsetzung der Richtlinie in das nationale Recht soll bis zum 15. September 2007 erfolgen (Art. 15 Abs. 1 S. 1 RL).

## 3. Die Europarechtswidrigkeit der Richtlinie

Bereits an der formellen Rechtmäßigkeit der Vorratsdatenspeicherungsrichtlinie bestehen erhebliche Zweifel. Die Richtlinie wird auf Art. 95 EGV gestützt. Diese Norm bietet eine Rechtsgrundlage für Maßnahmen zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedsstaaten, welche die Errichtung und das Funktionieren des Binnenmarktes zum Gegenstand haben. In seiner Rechtsprechung verlangt der EuGH, dass eine auf der Grundlage von Art. 95 EGV erlassene Richtlinie tatsächlich den primären Zweck haben soll, die Voraussetzungen für die Errichtung und das Funktionieren des Binnenmarktes zu verbessern<sup>82</sup>. Dabei hat der EuGH strenge Maßstäbe entwickelt: Eine bloße Feststellung von Unterschieden zwischen den nationalen Vorschriften und eine abstrakte Gefahr der Entstehung von Wettbewerbsverzerrungen rechtfertigen demnach nicht die Berufung auf Art. 95 EGV als Rechtsgrundlage einer Richtlinie<sup>83</sup>.

---

<sup>82</sup> *EuGH*, Urteil vom 5. Oktober 2000, Rs. C-376/98, Deutschland/EP und Rat („Tabakwerbeverbotrichtlinie“), Slg. 2000, I-8419, Rn. 86.

<sup>83</sup> *Streinz*, Europarecht, 7. Aufl., Heidelberg 2005, S. 361.

Ziel und der Inhalt der Vorratsdatenspeicherungsrichtlinie betreffen aber in erster Linie die Vorsorge zur Strafverfolgung<sup>84</sup>. Die Angleichung nationaler Rechtsvorschriften zwecks Verbesserung des Binnenmarktes kann bei der Vorratsdatenspeicherung, wenn überhaupt, lediglich als sekundärer Zweck bezeichnet werden<sup>85</sup>. Auch die politische Diskussion um die Vorratsspeicherung von Verkehrsdaten erfolgte auf europäischer Ebene stets im Kontext der polizeilichen und justiziellen Zusammenarbeit in Strafsachen. Der Wechsel zur Handlungsform der Richtlinie wurde erst vollzogen, nachdem die für den ursprünglich vorgelegten Entwurf eines Rahmenbeschlusses nach Art. 31 und 34 EUV erforderliche Einstimmigkeit nicht erreicht werden konnte.

Die Vorratsdatenspeicherungsrichtlinie ist wegen ihrer fehlenden Rechtsgrundlage deshalb als formell nichtig anzusehen. Es ist zu erwarten, dass die von Irland erhobene Nichtigkeitsklage gegen die Richtlinie Erfolg haben wird<sup>86</sup>. Diese Prognose wird durch die neuere Rechtsprechung des EuGH bekräftigt. Im Urteil vom 30. Mai 2006 zur Übermittlung von Flugpassagierdaten in die USA erklärte der EuGH in ähnlicher Konstellation die ebenfalls auf Art. 95 EGV gestützten Rechtsetzungsakte mangels Rechtsgrundlage für nichtig<sup>87</sup>.

Hinzu kommen erhebliche Zweifel, ob der Inhalt der Richtlinie dem Maßstab von Art. 8 EMRK standhält. Bei der Prüfung der Eingriffe in das durch Art. 8 EMRK gewährleistete Grundrecht auf Privatsphäre und private Telekommunikation orientiert sich der EuGH an der Rechtsprechung des EMGR<sup>88</sup>. Eingriffe in dieses Grundrecht sind zulässig, insoweit sie gesetzlich vorgesehen sind und Maßnahmen darstellen, die in einer demokratischen Gesellschaft zum Schutz der nationalen Sicherheit, der öffentlichen Ordnung sowie zur Verhütung von Straftaten und zum Schutz der Rechte und Freiheiten anderer notwendig sind (Art. 8 Abs. 2 EMRK). Durch die Verpflichtung zur vorrätigen Speicherung der Kommunikationsdaten sämtlicher Nutzer greift die Richtlinie in das Gemeinschaftsgrundrecht auf Achtung des Privatlebens und der Korrespondenz aus Art. 8 EMRK unverhältnismäßig ein. Eine Erfassung sämtlicher Telekommunikation aller EU-Bürger ohne konkreten Anlass und ohne jeglichen Tatverdacht kann in einer demokratischen Rechtsordnung nicht als notwendig angesehen werden.

Sollte die Vorratsdatenspeicherungsrichtlinie vom EuGH für nichtig erklärt werden, bestünde für die Mitgliedsstaaten keine Umsetzungspflicht mehr. Aus rechtspolitischer Sicht erscheint es deswegen sachgerecht, bis zur Entscheidung des EuGH über die Nichtigkeitsklage von Irland von der Umsetzung der Richtlinie 2006/24/EG in nationales Recht abzusehen. Die Opposition im Deutschen Bundestag hat dies schon mit Nachdruck gefordert: „Der Schaden, der dadurch entstünde, dass eine nichtige Richtlinie zunächst in nationales Recht umgesetzt würde und das

---

<sup>84</sup> Vgl. Art. 1 Abs. 1 sowie Erwägungsgründe Nr. 7 und 21 RL 2006/24/EG.

<sup>85</sup> Wenn die Zielsetzung eines gemeinschaftlichen Rechtsaktes zwei Komponenten hat und eine davon als überwiegende erscheint, dann ist der Rechtsakt auf die Rechtsgrundlage zu stützen, die die wesentliche Zielsetzung erfordert. Vgl. *EuGH*, Urteil vom 30. Januar, Rs. C-36/98, Spanien/Rat, Slg. 2001, I-779, Rn. 59.

<sup>86</sup> *EuGH*, Rs. C-301/06.

<sup>87</sup> *EuGH*, Urteil vom 30. Mai 2006, Rs. C 317/04 und C-318/04, EP/Rat = NJW 2006, S. 2029f.

Umsetzungsgesetz dann wieder zurückzunehmen wäre, ist erheblich. Eine u.U. verzögerte Umsetzung ist deshalb unter dem Gesichtspunkt der Verhältnismäßigkeit hinzunehmen<sup>89</sup>. Die Bundesregierung wird außerdem aufgefordert, im Falle eines neuen EU-Rahmenbeschlusses wegen der verfassungsrechtlichen Bedenken gegen die Vorratsdatenspeicherung nicht zuzustimmen.

## II. Zur Verfassungsmäßigkeit des deutschen Umsetzungsgesetzes

Wegen der erheblichen Einschränkungen des Rechts auf vertrauliche Telekommunikation sowie des Rechts auf Achtung des Privatlebens, die mit einer Umsetzung der Richtlinie 2006/24/EG verbunden wären, erscheint es mehr als zweifelhaft, ob eine verfassungskonforme Umsetzung in das deutsche Recht überhaupt möglich ist.

Mit dem vorliegenden Umsetzungsentwurf würden die schon jetzt bestehenden exzessiven Speicherungs-, Zugriffs- und Verwendungsmöglichkeiten telekommunikationsrelevanter Daten erheblich erweitert<sup>90</sup>. Die bisherige Berechtigung der Telekommunikationsunternehmen, bestimmte Daten für die Zwecke einer korrekten Abrechnung zu speichern, werden in eine Pflicht umgewandelt, fast alle anfallenden Verbindungsdaten sowie die Nutzungs- und Standortdaten zu erfassen, zu speichern und ggf. den Strafverfolgungsbehörden sowie den Verfassungsschutzbehörden und den Geheimdiensten auf Anordnung unverzüglich zur Verfügung zu stellen. Damit soll es zu Zwecken einer wirksamen Strafverfolgung schnell nachvollziehbar sein, wer, wann, mit wem, wie lange, von wo aus und über welches Telekommunikationsmedium kommuniziert hat<sup>91</sup>. Da den zugreifenden Behörden keine Schranken bei der Auswertung dieser Daten auferlegt sind, wird die Erstellung von Kommunikations- und Bewegungsprofilen der Telekommunikationsteilnehmer möglich. Eine Entschädigung für die Inanspruchnahme der Telekommunikationsunternehmen bei der Erhebung der Verkehrsdaten ist nicht vorgesehen.

Der vorgelegte Gesetzentwurf widerspricht mit diesen Regelungen tragenden Prinzipien des Datenschutzes (Datensparsamkeit, Zweckbindungsgebot, hohe Anforderungen bei der Anwendung des Verhältnismäßigkeitsgrundsatzes) und schränkt das Grundrecht auf Fernmeldegeheimnis und auf informationelle Selbstbestimmung unverhältnismäßig ein. Insbesondere mit der

---

<sup>88</sup> Vgl. *EuGH*, Rs. 136/79, „National Panasonic“, Slg. 1980, S. 2033; *EuGH*, Rs. 46/87 und 227/88, „Hoechst“, Slg. 1989, 2859f.

<sup>89</sup> BT-Drucks. 16/1622, S. 6.

<sup>90</sup> Gegenwärtig dürfen die Telekommunikationsanbieter nur die zur Abrechnung und Beweissicherung erforderlichen Verbindungsdaten für bis zu sechs Monate speichern (§ 97 Abs. 3 TKG). E-Mail-Daten beispielsweise werden dabei nicht erfasst. Die sonstigen Verbindungsdaten können auf Wunsch gelöscht werden. Mit der Wahl eines sogenannten Flatrate-Tarifs können Benutzerinnen und Benutzer eine Speicherung vermeiden. Die Vorschriften des § 100 Abs. 1 und 3 TKG erlauben eine weitgehende Erhebung und Verwendung von Verkehrsdaten zur Erkennung und Beseitigung technischer Störungen sowie zum Aufdecken und Unterbinden von rechtswidrigen Inanspruchnahmen der Telekommunikationsnetze und -dienste. Was den derzeit zulässigen staatlichen Zugriff auf die gesammelten Daten betrifft, vgl. §§ 100g, 100i (IMSI-Catcher), 100a (inhaltliche Überwachung) StPO sowie die relevanten geheimdienst- und verfassungsschutzrechtlichen.

<sup>91</sup> Vgl. Pressemitteilung des BMJ vom 8. November 2006.

vorgesehenen Verwendung der gespeicherten Daten für die Verfolgung mittelschwerer und mittels Telekommunikationseinrichtungen begangener Straftaten (vgl. § 100g Abs. 1 StPO-E) sowie zu Zwecken der Gefahrenabwehr und der Aufgabenerfüllung der Geheimdienste wird das Gesetz unverhältnismäßig. Der Gesetzentwurf öffnet Tür und Tor für spätere Erweiterungen des staatlichen Zugriffs auf die Vorratsdaten. Angesichts der großen Bandbreite und der zeitlichen Tiefe der vorrätigen Verbindungsdaten erscheint die Zugriffsregelung mit ihrem generellen Verweis auf die in § 100a Abs. 2 StPO-E aufgezählten Straftaten ebenfalls nicht angemessen.

Vor diesem Hintergrund stellt sich die Frage nach der Verfassungsmäßigkeit der einzelnen Regelungen im Gesetzentwurf.

### 1. Der Verstoß gegen Art. 10 GG (Fernmeldegeheimnis)

Der Schutzbereich des Telekommunikationsgeheimnisses umfasst sowohl den Inhalt der Telekommunikation als auch die näheren Umstände des Fernmeldeverhältnisses<sup>92</sup>. „Dazu gehört insbesondere, ob, wann und wie oft zwischen Personen oder Endeinrichtungen Telekommunikationsverkehr stattgefunden hat oder versucht wurde. Anderenfalls wäre der grundrechtliche Schutz unvollständig, denn die Verbindungsdaten haben einen eigenen Aussagegehalt. Sie können im Einzelfall erhebliche Rückschlüsse auf das Kommunikations- und Bewegungsverhalten zulassen. Häufigkeit, Dauer und Zeitpunkt von Kommunikationsverbindungen geben Hinweise auf Art und Intensität von Beziehungen und ermöglichen auf den Inhalt bezogene Schlussfolgerungen“<sup>93</sup>.

Der Schutz des Art. 10 Abs. 1 GG erstreckt sich auch auf den Informations- und Datenverarbeitungsprozess, der sich an zulässige Kenntnisnahmen anschließt und den Gebrauch, der von den erlangten Kenntnissen gemacht wird<sup>94</sup>.

#### *1.1. Zweistufiger Eingriff in das Grundrecht aus Art. 10 Abs. 1 GG*

Ein Eingriff in das Fernmeldegeheimnis liegt vor, wenn staatliche Stellen sich ohne Zustimmung der Betroffenen Kenntnis von dem Inhalt oder den Umständen eines fernmeldetechnisch vermittelten Kommunikationsvorgangs verschaffen<sup>95</sup>. Die im Gesetzentwurf vorgesehenen Regelungen zur Umsetzung der Richtlinie 2006/24/EG greifen zweistufig in das Fernmeldegeheimnis ein. Auf der *ersten Stufe* erfolgt der Eingriff in das Kommunikationsgeheimnis mit der gesetzlich angeordneten Verpflichtung der Anbieter öffentlicher Telekommunikationsdienste, die anfallenden Verbindungsdaten für 6 Monate zu speichern (vgl. § 113a Abs. 1 S. 1 TKG-E). Die Tatsache, dass die Erhebung und Speicherung der Daten durch die Telekommunikationsunternehmen erfolgt,

---

<sup>92</sup> BVerfGE 67, 157 (172).

<sup>93</sup> BVerfG, NJW 2006, 976 (978). Vgl. auch BVerfGE 107, 299 (320); 113, 348 (365).

<sup>94</sup> BVerfGE 100, 313 (359).

<sup>95</sup> BVerfGE 107, 299 (313).

ändert an ihrer Qualität als staatlichem Eingriff in das Fernmeldegeheimnis nichts. Die vorgesehene Erfassung und Speicherung ist hoheitlich angeordnet, die Unternehmen verfügen dabei über keinen Handlungsspielraum<sup>96</sup>. Auf der *zweiten Stufe* erfolgt der Eingriff in das Grundrecht aus Art. 10 Abs. 1 GG durch die Regelungen, die einen staatlichen Zugriff auf die auf Vorrat gespeicherten Verkehrsdaten und ihre Verwendung ermöglichen. Die Telekommunikationsunternehmen werden ausdrücklich verpflichtet, die erfassten und gespeicherten Daten den zuständigen staatlichen Stellen auf Ersuchen unverzüglich zur Verfügung zu stellen (§ 113b S. 1 TKG-E). Aufgrund der in den §§ 100g, 100a StPO-E sowie 113b S. 1 TKG-E vorgesehenen Normen können sich dann zahlreiche staatliche Stellen ohne Wissen und Zustimmung der Beteiligten von den Umständen aller gespeicherten Telekommunikationsvorgänge ein genaues Bild machen.

Der Zugriff auf die umfangreichen Verbindungsdaten erlaubt einen umfassenden Einblick in das Kommunikationsverhalten der Betroffenen, deren Identität feststellbar ist. Auf beiden Stufen greift der Gesetzesvorschlag intensiv in Art. 10 GG ein. Dabei ermöglicht die Vielzahl der erfassten Daten Rückschlüsse auf Kommunikationsstrukturen, z. T. auch auf den Inhalt der Telekommunikation<sup>97</sup>. Die Bewertung der zahlreichen Standortdaten erlaubt außerdem die Erstellung genauer Bewegungsprofile der Betroffenen.

Wegen der Unterschiedlichkeit der Eingriffe auf der ersten und zweiten Stufe wird ihre Verfassungsmäßigkeit nacheinander geprüft.

### *1.2. Stufe 1: Die anlasslose Erhebung und Speicherung sämtlicher Verbindungsdaten als genereller Verstoß gegen das Fernmeldegeheimnis*

#### *a) Legitimität des Zwecks der Speicherungspflicht*

Zweifel bestehen zunächst einmal an der Legitimität des Zwecks der Vorratsdatenspeicherung. Nach der Begründung des BMJ soll die pauschale Speicherung sämtlicher elektronischer Kommunikationsvorgänge die Verfügbarkeit der Verkehrs- und Standortdaten für die Zwecke einer eventuellen späteren Strafverfolgung, aber auch für die Zwecke der Gefahrenabwehr und der Aufgabenerfüllung der Nachrichtendienste sicherstellen<sup>98</sup>.

In einer freiheitlichen Demokratie darf die Spurensicherung nur im Verdachtsfall erfolgen. Der Staat darf nicht jeden Bürger vorsorglich als potenziellen Verbrecher behandeln. Nach etablierter Rechtsprechung und Rechtspraxis ist eine vorsorgliche Überwachung für künftige Strafverfolgungsmaßnahmen bisher in der Bundesrepublik Deutschland an das Vorhandensein einer konkreten Gefahrenlage oder einer negativen Kriminalprognose der betroffenen Personen gebunden. Mit einer anlass- und verdachtslosen Speicherung sämtlicher Verbindungsdaten würde praktisch

---

<sup>96</sup> Vgl. BVerfGE 107, 299 (313).

<sup>97</sup> Vgl. BVerfGE 113, 348 (365).

allen Benutzerinnen und Benutzern elektronischer Telekommunikationsmittel unterstellt, sie könnten in der Zukunft zum Objekt staatlicher Strafverfolgung werden. Dieser Generalverdacht schränkt nicht nur das Recht auf vertrauliche Kommunikation ein, sondern stellt auch grundlegende Prinzipien des Datenschutzes, die Sparsamkeit und Zweckgebundenheit von staatlich angeordneter Datenspeicherung, auf den Kopf.

Vor diesem Hintergrund erscheint es aus verfassungsrechtlicher Sicht bedenklich, dass Daten, die ansonsten nicht vorliegen würden, zu allgemeinen Sicherheitszwecken gespeichert werden sollen. Man darf zu Zwecken einer eventuellen späteren Strafverfolgung die Entstehung einer umfangreichen Sammlung personenbezogener Daten auch deswegen nicht zulassen, weil auf diese Weise die Unschuldsvermutung partiell wegfallen würde. Maßnahmen wie die Vorratsdatenspeicherung, die eine verdachtlose „vorbeugende Verbrechensbekämpfung“ bzw. eine „Strafverfolgungsvorsorge“ gewährleisten sollen, dienen daher keinem legitimen Zweck. Vielmehr verstößt diese gesetzgeberische Zwecksetzung gegen die Unschuldsvermutung bei der Strafverfolgung, von der auch das Grundgesetz ausgeht.

Nach einem vom Bundesverfassungsgericht entwickelten Grundsatz „muss der Zweck, zu dem Eingriffe in das Fernmeldegeheimnis vorgenommen werden dürfen, bereichsspezifisch und präzise bestimmt werden. Eine Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder nicht bestimmaren Zwecken wäre damit unvereinbar“<sup>99</sup>. Das Bundesverfassungsgericht hat ausdrücklich festgestellt, dass das Grundgesetz eine „globale und pauschale Überwachung“ zu Zwecken der Auslandsaufklärung nicht zulässt<sup>100</sup>. Es leuchtet wenig ein, warum dies bei der Strafverfolgungsvorsorge und bei der Gefahrenabwehr anders sein soll. Die allgemeine Zweckbestimmung des Gesetzentwurfs, die Speicherung und die weitere Verarbeitung der Verbindungsdaten diene der Strafverfolgung, der Gefahrenabwehr und der Aufgabenerfüllung der Nachrichtendienste, genügt vor diesem Hintergrund nicht den verfassungsrechtlichen Anforderungen<sup>101</sup>. Der Gesetzentwurf regelt in § 113b S. 1 TKG-E ausdrücklich nur den Zweck der Datenübermittlung durch die Provider, der Zweck der Datenspeicherung wird dagegen offen gelassen. Dies könnte dazu führen, dass die Telekommunikationsanbieter die vorrätig gespeicherten Daten unsanktioniert für ihre eigene Zwecke nutzen.

### *b) Geeignetheit der Vorratsdatenspeicherung*

Zweifel an der Geeignetheit ergeben sich daraus, da Kriminelle oder Terroristen mit relativ einfachen Mitteln die Überwachungsmaßnahmen unterlaufen können. Dazu bräuchten die Betroffenen lediglich ihre Kommunikationsgeräte über Dritte erwerben oder auf öffentliche Kommunika-

---

<sup>98</sup> Vgl. BT-Drucks. 16/5846, Begründung zum Gesetzentwurf, S. 70.

<sup>99</sup> BVerfGE 100, 313 (360).

<sup>100</sup> BVerfGE 100, 313 (376).

<sup>101</sup> BVerfGE 107, 299 (321).

tionsmittel – wie Internetcafés, Straßentelefonzellen, Mailkonten außerhalb der EU und den USA oder vorausbezahlte international einsetzbare SIM-Karten – zurückgreifen<sup>102</sup>. Darüber hinaus muss auch die Möglichkeit berücksichtigt werden, Anonymisierungsdienste einzusetzen. Die Methoden einer anonymen Nutzung der Telekommunikation werden eher besonders gefährliche Straftäter als Kleinkriminelle oder gar Unbeteiligte gebrauchen. Für die Verfolgung besonders schwerer Straftaten erscheint die Speicherung von Vorratsdaten daher wenig geeignet, da die eigentliche „Zielgruppe“ der Maßnahme sich ihr entziehen wird. Wenn die vorhandenen Verbindungsdaten keiner Person eindeutig zugeordnet werden können, dann ist ihre Verwertbarkeit bei einer strafrechtlichen Ermittlung oder bei Maßnahmen zur Gefahrenabwehr sehr gering. Auch eine erhebliche gesetzliche Beschränkung oder ein Verbot von Anonymisierungsdiensten, worauf das Umsetzungsgesetz praktisch abzielt, könnte daran nichts ändern, da sich die anonyme Nutzung von Telekommunikationsnetzen technisch kaum verhindern lässt<sup>103</sup>.

Die vorhandenen empirischen Angaben lassen ebenfalls Zweifel daran entstehen, ob die Vorratsdatenspeicherung in einem großen Maße zur Verbesserung der Strafverfolgung beitragen kann. In der Praxis scheitern demnach nur wenige Ermittlungsverfahren an Telekommunikationsverkehrsdaten, zumal die Strafverfolgungsbehörden oft nur an den Bestandsdaten interessiert sind<sup>104</sup>.

### *c) Erforderlichkeit der Vorratsdatenspeicherung*

Bedenken bestehen auch hinsichtlich der Erforderlichkeit der vorgesehenen Vorratsdatenspeicherung zur Terrorismus- und Verbrechensbekämpfung. Mit dem sogenannten „Quick-freeze-Verfahren“ oder „Data Preservation“, das u.a. in den USA praktiziert wird, steht ein milderer Mittel zur Verfügung, durch das die Ziele des Gesetzgebers weitgehend zu erreichen wären<sup>105</sup>. Dabei werden die Daten einer verdächtigen Person nach der Aufforderung durch die Strafverfolgungsorgane ab sofort gespeichert, der Zugriff auf diese Daten ist dann nach Erlass einer richterlichen Anordnung möglich. Dieses Verfahren erfüllt allerdings nur dann in gleichem Maße den angestrebten Zwecken, wenn es um eine Beobachtung / Ermittlung andauernden strafwürdigen Verhaltens geht, die fraglichen Verbindungsdaten also in der Gegenwart und Zukunft anfallen. Für

---

<sup>102</sup> Vgl. *Wissenschaftliche Dienste des Deutschen Bundestages*, Gutachten 282/06, S. 13. Ausführlich zu den technischen Umgehungsmöglichkeiten bei den verschiedenen Telekommunikationsdiensten *Breyer*, Die systematische Aufzeichnung und Vorhaltung von Telekommunikations-Verkehrsdaten für staatliche Zwecke in Deutschland, Berlin 2005, S. 14f.

<sup>103</sup> Vgl. dazu *Breyer*, Die systematische Aufzeichnung und Vorhaltung von Telekommunikations-Verkehrsdaten für staatliche Zwecke in Deutschland, Berlin 2005, S. 189.

<sup>104</sup> Ausführlich dazu *Breyer*, Die systematische Aufzeichnung und Vorhaltung von Telekommunikations-Verkehrsdaten für staatliche Zwecke in Deutschland, Berlin 2005, S. 188f. und *Büllingen*, DuD 2005, S. 349 (351, 353).

<sup>105</sup> Zum sogenannten „Quick-freeze-Verfahren“ vgl. *Büllingen*, DuD 2005, S. 349 (350).

einen Zugriff auf in der Vergangenheit angefallene Daten ist das „Data Preservation“-Verfahren nutzlos und nicht im gleichen Maße förderlich wie die generelle Vorratsdatenspeicherung<sup>106</sup>.

Trotzdem ist zu bemerken, dass erhebliche Zweifel an der Notwendigkeit der Speicherdauer von sechs Monaten bestehen. Erfahrungsgemäß betreffen die Zugriffe der berechtigten Behörden in ähnlichen Konstellationen fast ausschließlich die ersten drei Monate der Speicherung<sup>107</sup>. Unter dem Gesichtspunkt der Erforderlichkeit wäre daher eine dreimonatige Speicherfrist hinreichend – allerdings würde die Umsetzung sich damit gegen die minimale Speicherungsfrist aus Art. 6 der Richtlinie 2006/24/EG wenden.

#### *d) Angemessenheit der Vorratsdatenspeicherung*

##### *aa) Die von der Vorratsdatenspeicherung erfassten Personen*

Eine Unterscheidung der betroffenen Personen, deren Daten auf Vorrat gespeichert werden sollen, nimmt der Gesetzesentwurf nicht vor. Es fehlt jegliche Differenzierung nach fahndungsrelevanten Personengruppen, vielmehr sollen die Daten aller Telekommunikationsteilnehmer gleichermaßen gespeichert werden. Da der Speichervorgang – zumindest die personenbezogenen Daten betreffend – einen Grundrechtseingriff darstellt und dabei jegliche Unterscheidung zwischen Tatverdächtigen, Kontaktpersonen und völlig unbeteiligten Bürgern unterbleibt, erscheint diese gesetzgeberische Lösung völlig unangemessen. „Im Ergebnis wird damit pauschal die gesamte Ebene der bei der Frage der rechtlichen Zulässigkeit maßgeblichen Verarbeitungsebene Speicherung/Nichtspeicherung der zukünftigen rechtsstaatlichen Gestaltung entzogen. Damit zeichnet sich ein überwachungsstaatliches Szenario ab, bei dem zukünftig über einzelne Zugriffe seitens bestimmter Institutionen verhandelt wird, wohingegen die Frage der staatlichen Verfügbarkeit der Daten selbst dem Streit entzogen sind. Eine derartige Regelung ist mit den verfassungsfesten Schutzkonzeptionen von Artikel 10 GG als auch Artikel 2 Absatz 2 GG unvereinbar“<sup>108</sup>.

Die Regelungen des Gesetzentwurfes stehen damit im Gegensatz zu wichtigen verfassungsrechtlichen Grundsätzen des Datenschutzes<sup>109</sup>. Durch die Vorratsdatenspeicherung werden Strukturprinzipien wie Datensparsamkeit, Datenvermeidung und Zweckbindungsgebot als Ausfluss des Verhältnismäßigkeitsprinzips ausgehöhlt. Die Datenerhebung erfolgt unabhängig von einem im Einzelfall bestehenden Tatverdacht. Es werden alle Kommunikationsvorgänge sämtlicher Kommunikationsteilnehmer auf Vorrat gespeichert. Wenn es einerseits „kein belangloses Datum“<sup>110</sup> mehr gibt und die Vorratsdatenspeicherung andererseits ermöglicht, dass

<sup>106</sup> In diesem Sinne auch die Begründung zum Gesetzentwurf, BT-Drucks. 16/5846, S. 31: „Das schnelle Einfrieren der benötigten Verkehrsdaten durch die Dienstanbieter auf Zuruf der Strafverfolgungsbehörden geht notwendig ins Leere, wenn die relevanten Verkehrsdaten überhaupt nicht gespeichert oder zwischenzeitlich bereits gelöscht wurden und daher nicht gesichert werden können“.

<sup>107</sup> Vgl. dazu *Westphal*, EuZW 2006, S. 555 (558).

<sup>108</sup> *Humanistische Union*, Stellungnahme vom 12.12.2005, S. 6.

<sup>109</sup> BVerfGE, 65, 1 (44, 46).

Datum"<sup>110</sup> mehr gibt und die Vorratsdatenspeicherung andererseits ermöglicht, dass praktisch alle Verkehrs- und Standortdaten von allen Telekommunikationsteilnehmern gespeichert werden, dann liegt die Verfassungswidrigkeit der jeweiligen Vorschriften auf der Hand.

Im „IMSI-Catcher“-Beschluss hat das Bundesverfassungsgericht in Zusammenhang mit der bevorstehenden Gesamtregelung der strafprozessualen heimlichen Ermittlungsmaßnahmen darauf hingewiesen, dass zu prüfen ist, „ob und in welchem Umfang von einer neuerlichen Ausdehnung heimlicher Ermittlungsmethoden im Hinblick auf Grundrechtspositionen unbeteiligter Dritter Abstand zu nehmen ist“<sup>111</sup>. Dass dies durch den vorgestellten Gesetzentwurf geschieht, ist nicht ersichtlich.

#### *bb) Adressaten der Speicherungspflicht (§ 110a Abs. 1 Satz 1 TKG-E)*

In § 113a Abs. 1 Satz 1 TKG-E wird der Kreis der zur Speicherung Verpflichteten festgelegt. Danach sind zur Speicherung im Inland oder in einem anderen Mitgliedsstaat der Europäischen Union diejenigen verpflichtet, die Telekommunikationsdienste für Endnutzer erbringen. Gespeichert werden müssen nur Verkehrsdaten, die vom jeweiligen Diensteanbieter bei der Nutzung seines Dienstes erzeugt oder verarbeitet werden. Für die Anbieter, die Telekommunikationsdienste erbringen, ohne selbst Verkehrsdaten zu erzeugen oder zu verarbeiten, besteht die Pflicht, die Speicherung sicherzustellen (§ 113a Abs. 1 S. 2 TKG-E). Bei der Festlegung der Adressaten der Speicherungspflicht werden zahlreiche unbestimmte Begriffe verwendet. Es stellt sich daher die Frage, ob das Bestimmtheitsgebot ausreichend berücksichtigt wurde.

Bei der Rechtsanwendung können durchaus Zweifel entstehen, ab wann von einer „Erzeugung“ und „Verarbeitung“ von Daten ausgegangen wird. Vergleichbare Anwendungsschwierigkeiten gab es beispielsweise beim Streit darum, ob der Mautsystembetreiber Toll Collect GmbH im Sinne des TKG Telekommunikationsdienste erbringt und dementsprechend Normadressat des §100g StPO wäre<sup>112</sup>. Vergleichbare Streitfälle werden mit dem Gesetzentwurf nicht beseitigt, sondern eher noch verstärkt.

In der Begründung des Gesetzentwurfs wird zum Begriff des „Verarbeitens“ erklärt, dass er weit zu verstehen sei und etwa auch die Fälle erfasse, in denen ein Mobilfunknetzbetreiber die von einem Teilnehmer eines anderen Netzbetreibers initiierte Verbindung „übernimmt“ und die Verbindung zu seinem eigenen Endnutzer herstellt<sup>113</sup>. Welche anderen Leistungen noch unter dem Begriff des „Verarbeitens“ in Zusammenhang mit der Vorratsdatenspeicherung zu subsumieren wären, ist offen.

---

<sup>110</sup> BVerfGE, 65, 1 (45).

<sup>111</sup> BVerfGE 2 BvR 1345/03 („IMSI-Catcher“), Rn. 84.

<sup>112</sup> Vgl. *Fraenkel/Hammer*, DuD 2006, S. 499f.

<sup>113</sup> BT-Drucks. 16/5846, Begründung zum Regierungsentwurf, S. 69.

Weiterhin sieht die geplante Regelung keine Begrenzung der Speicherungspflicht auf solche Betreiber vor, die Telekommunikationsdienste *geschäftsmäßig* erbringen. Deshalb bleibt unklar, ob auch Privatpersonen zur Speicherung verpflichtet sind, wenn sie kostenlos einen öffentlichen WLAN-Zugang, einen E-Mail-Dienst oder Ähnliches anbieten. Vor diesem Hintergrund ist anzunehmen, dass es in der Praxis zu zahlreichen Anwendungsproblemen kommen wird, da die Adressaten der Speicherungspflicht nicht hinreichend bestimmt sind. Im Rahmen des Art. 10 GG kommt aber dem Bestimmtheitsgebot eine besondere Bedeutung zu: Umfang und Voraussetzungen der Einschränkungen müssen sich klar aus dem Gesetz ergeben.

### *cc) Verbot der Anonymisierungsdienste*

Das Gesetz sieht eine Speicherungspflicht auch für diejenigen vor, die so genannte Anonymisierungsdienste betreiben und anbieten (vgl. § 113a Abs. 6 TKG-E)<sup>114</sup>. Darunter werden Programme verstanden, die Internetverbindungen durch ein verteiltes Netz von Servern leiten. Durch die Nutzung von mehreren Servern kann die Quelle einer Nachricht derart verschleiert werden, dass die Identität des Nutzers nicht mehr feststellbar ist<sup>115</sup>.

Dem Wortlaut des relevanten § 113a Abs. 6 TKG-E ist allerdings nicht direkt zu entnehmen, dass die Anonymisierungsdienste darunter zu subsumieren sind. Lediglich in der Begründung des Gesetzentwurfs wird ausgeführt, dass die Anbieter von Anonymisierungsdiensten öffentlich zugängliche Telekommunikationsdienste im Sinne von § 3 Nr. 24 TKG erbringen und daher von der Speicherungspflicht betroffen seien. Die Anonymisierungsdienste wiesen eine Doppelnatur auf, da ihre Tätigkeit sowohl in der Durchleitung der Nachricht als auch in der Ersetzung der Ausgangskennung des Telekommunikationsnutzers besteht. Diese Dienste seien daher sowohl Telemedien als auch Telekommunikationsdienste<sup>116</sup>. Die Rechtsfolge wäre, dass mit § 113a Abs. 6 TKG-E die Anonymisierungsdienste praktisch verboten werden. Wenn die Anbieter von Internetanonymisierungsdiensten die entsprechenden in § 113a TKG-E aufgelisteten Daten, also auch alle in der Kette der Anonymisierung vergebenen IP-Adressen, speichern sollen, bedeutet dies praktisch, dass eine „Re-Anonymisierung“ möglich wird.

Eine Speicherungspflicht für Betreiber von Anonymisierungsdiensten ergibt sich nicht unmittelbar aus der Richtlinie 2006/24/EG. Die Richtlinie bezieht sich lediglich auf elektronische Telekommunikationsdienste, nicht aber auf Teledienste, wozu Anonymisierungsdienste bisher gezählt werden. Sie gilt für Verkehrs- und Standortdaten sowie für alle damit in Zusammenhang stehende Daten, die zur Feststellung der Benutzer erforderlich sind (Art. 1 Abs. 2 RL). Art. 5 RL regelt die Daten, die vorrätig gespeichert werden müssen, für Telefone, Mobilfunk, Internetzugänge, E-Mails und die Internet-Telephonie. Die Anonymisierungsdienste lassen sich keiner die-

---

<sup>114</sup> Vgl. BT-Drucks. 16/5846, Begründung zum Regierungsentwurf, S. 71.

<sup>115</sup> Vgl. *Spindler/Schmitz/Geis*, TDG-Kommentar, München 2004, S. 292f.

<sup>116</sup> BT-Drucks. 16/5846, Begründung zum Regierungsentwurf, S. 72.

ser Datenkategorien zuordnen. Insoweit geht eine Verpflichtung zur Vorratsdatenspeicherung für die Anbieter von Anonymisierungsdiensten über die Anforderungen der Richtlinie hinaus.

Darüber hinaus stellen die Anonymisierungsdienste keine Telekommunikations-, sondern Telemediendienste dar. Gemäß § 1 Abs. 1 TMG sind Telemediendienste „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 § Nr. 25 des Telekommunikationsgesetzes oder Rundfunk nach § 2 des Rundfunkstaatsvertrages sind“. Die Zuordnung der Anonymisierungsdienste zu den Telemedien ist dadurch begründet, dass bei Ihnen die Umschreibung der IP-Adressen auf der Anwendungsebene und nicht auf der Ebene des Transportprotokolls stattfindet. Da die Verschlüsselung der Inhalte und die Tarnung der IP-Adressen auf der Inhaltsebene erfolgt, entsteht die Gefahr, dass Telekommunikationsinhalte bekannt werden, was der Intention des Richtlinien- und des Gesetzgebers widerspricht<sup>117</sup>.

Auch wenn man sich der Begründung des Regierungsentwurfs anschließen würde und die Anonymisierungsdienste auch als Telekommunikationsdienste einstuft, stellt sich erneut die Frage nach der Geeignetheit der Vorratsdatenspeicherung, die angestrebten Ziele zu erreichen. Da bei der Anonymisierung eine Kaskade von zahlreichen Telekommunikationsvorgängen entsteht, an der viele selbstständige Betreiber beteiligt sind, wäre eine Prüfung der bei jedem einzelnen Teilnehmer gespeicherten Daten notwendig. Der für die Sammlung und Auswertung der Daten erforderliche Aufwand wäre enorm groß.

Schließlich führt der Gesetzentwurf einen Widerspruch zur geltenden Rechtslage ein, wonach die Anbieter von Telemediendiensten verpflichtet sind, ihren Nutzern die Inanspruchnahme sowie die Bezahlung der Dienste anonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist (vgl. § 13 Abs. 6 Telemediengesetz (TMG), früher § 4 Abs. 6 TDDSG).

#### *dd) Katalog der zu speichernden Daten (§ 113a Abs. 2 bis 5 TKG-E)*

Eng mit den Vorschriften, die den Adressatenkreis der Speicherungspflicht regeln, sind die Normen verbunden, die die zu speichernden Daten festlegen. Der Katalog der zu speichernden Daten (§ 113a Abs. 2 bis 5 TKG-E) entspricht größtenteils der Forderung des Deutschen Bundestages sowie der Ankündigung der Bundesregierung, bei der Umsetzung der Richtlinie keine über die Mindestanforderungen der Richtlinie hinausgehenden Pflichten zu regeln<sup>118</sup>. Allerdings erscheint es bezüglich einzelner Daten zweifelhaft, ob ihre Speicherung über die Richtlinie hinaus geht und ob ihr Nutzen im Vergleich zu den negativen Folgen der Vorratsdatenspeicherung verhältnismäßig ist. Dies betrifft beispielsweise die Pflicht zur Speicherung der ersten Aktivierung des

---

<sup>117</sup> Vgl. Stellungnahme des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein vom 27.06.2007, S. 22.

<sup>118</sup> Vgl. BT-Drucks. 16/545, S. 4.

jeweiligen Dienstes bei vorausbezahlten Diensten wie beispielsweise Prepaid-SIM-Karten oder Flatrate-Tarifen für den Internetzugang (§ 113a Abs. 2 Nr. 4 d) TKG-E); die Pflicht zur Speicherung erfolgloser Anrufsversuche (Art. 3 Abs. 2 RL, § 113a Abs. 5 TKG-E)<sup>119</sup>; die Erhebung von Daten in Echtzeit (§ 100g Abs. 1 S. 3 StPO-E); die Speicherungspflicht der Anbieter von E-Mail-Diensten bezüglich jedes Zugriffs auf das elektronische Postfach (§ 113a Abs. 3 Nr. 3 TKG-E); die Angaben über die Hauptstrahlrichtung der Funkantennen beim Mobilfunk (§ 113a Abs. 7 TKG-E). Bei all diesen Daten ist sehr zweifelhaft, ob ihr praktischer Nutzwert den Grundrechtseingriff durch ihre Speicherung rechtfertigen kann. Außerdem lässt der Katalog der zu speichernden Daten trotz seiner detaillierten Aufzählungen zahlreiche Fragen offen, ob bestimmte Dienste bzw. Daten wie etwa Hot-Spots, Skype usw. davon erfasst werden.

Mit der im Gesetzentwurf vorgesehenen Speicherung der Kennung eines ankommenden Anrufs (§ 113a Abs. 2 Nr. 1 TKG-E) wird die bisherige, umstrittene „Zielwahlsuche“ (§ 100g Abs. 2 StPO) teilweise entbehrlich. Für jedes Benutzerkonto werden künftig nicht nur alle abgehenden, sondern auch alle ankommenden Verbindungen gespeichert. Die Speicherung aller Verbindungsdaten bei Sendern und Empfängern zeigt einmal mehr, wie umfassend die künftige Vorratsdatenspeicherung von Verkehrsdaten ist und mit welcher Intensität sie in die Grundrechte eingreift<sup>120</sup>.

Nach § 113a Abs. 2 Nr. 4 Buchst. c TKG-E sind die Standortdaten des anrufenden und des angerufenen Anschlusses bei Beginn der Verbindung zu speichern. Da ein betriebsbereites Mobiltelefon in geringen zeitlichen Abständen Signale an die nächststehende Funkzelle sendet, kann der Standort des Apparats bzw. seines Nutzers relativ genau bestimmt werden<sup>121</sup>. Durch die Möglichkeit der Ortung eines eingeschalteten Mobiltelefons können genaue Bewegungsprofile erstellt werden. Die Tatsache, dass die Speicherung der Standortdaten durch die Telekommunikationsunternehmen nur beim Beginn der Verbindung erfolgt, ändert daran nichts, denn § 100g Abs. 1 S. 3 StPO-E soll künftig die Erhebung von Standortdaten durch die Strafverfolgungsbehörden in Echtzeit ermöglichen, auch wenn das Mobiltelefon gerade nicht genutzt wird<sup>122</sup>. Damit würde das eingeschaltete Mobiltelefon „zu einer Art ungewolltem Peilsender“<sup>123</sup>, der die Bewegung

---

<sup>119</sup> Daten in Zusammenhang mit erfolglosen Anrufversuchen (vgl. Art. 2 Abs. 2 f RL 2006/24/EG) müssen gespeichert werden, wenn sie von den Anbietern im Zuge der Bereitstellung von Kommunikationsdiensten oder zu Rechnungszwecken erzeugt und verarbeitet werden (vgl. Art. 3 Abs. 2 und Erwägungsgrund 12 der RL 2006/24/EG; § 110a Abs. 5 TKG-E). Zu kritisieren ist dabei, dass auf diese Weise dem Angerufenen erschwert wird, sich einer Speicherung zu entziehen, auch wenn er gezielt einen Kommunikationsvorgang ablehnt und beispielsweise nicht ans Telefon geht. Mit der Speicherung erfolgloser Verbindungsversuche wird das Risiko stark erhöht, unbegründet unter Verdacht zu geraten.

<sup>120</sup> Die Ausführungen in der Begründung des Gesetzentwurfs, wonach die Zielwahlsuche „entfällt“ (BT-Drucks. 16/5846, Begründung zum Regierungsentwurf, S. 54), sind hier irreführend. Kritisch dazu Zoller, Goldammer's Archiv für Strafrecht (GA) 2007, S. 393 (397f.).

<sup>121</sup> Um eine genauere Ermittlung des Standortes eines Mobiltelefons zu ermöglichen, verpflichtet § 113a Abs. 7 TKG-E die Anbieter zur Angabe der geografischen Lage der jeweiligen Funkzelle sowie der Hauptstrahlrichtung der Funkantennen.

<sup>122</sup> BT-Drucks. 16/5846, Begründung zum Regierungsentwurf, S. 51.

<sup>123</sup> Zöller, CILIP 85 (3/2006), S. 21 (26).

seines Nutzers meldet. Somit wird auch die aus verfassungsrechtlicher Sicht äußerst bedenkliche Ermittlungsmethode des sogenannten „stillen SMS“ de facto legalisiert<sup>124</sup>.

Entsprechend den Vorgaben der Richtlinie (Art. 5 Abs. 2 RL) sieht der Gesetzesentwurf generell vor, dass keine Daten gespeichert werden dürfen, die Aufschluss über den Inhalt der Kommunikation geben<sup>125</sup>. Zum einen kann eine Trennung zwischen Inhaltsdaten und „reinen“ Verbindungsdaten in vielen Fällen technisch kaum erfolgreich vorgenommen werden. Insbesondere bei E-Mail und SMS wird diese Trennung sehr schwierig sein, weil beide Dienste diese Daten auf Protokollebene vermischen<sup>126</sup>. Zum anderen können auf Grund einer umfangreichen Sammlung von Verkehrs-, Standort- und Bestandsdaten Kommunikationsinhalte durchaus nachgebildet werden. Nach § 113a Abs. 4 Nr. 1 TKG-E sollen die den Nutzern für jede Internetsitzung zugewiesenen dynamischen und statischen IP-Adressen künftig gespeichert werden. Bei entsprechenden Auswertungen auf Grund beschlagnahmter Webserver könnten die darauf erfassten URLs mit den IP-Adressen abgeglichen werden und Kenntnisse über die Kommunikationsinhalte einzelner Nutzer gewonnen werden. Mit Hilfe ausgefeilter technischer Methoden zur Analyse der Verkehrsdaten lassen sich daraus detaillierte Informationen über soziale Netzwerke, Freundeskreise, persönliche Präferenzen etc. gewinnen sowie speziell im Internetbereich Profile über einzelne Nutzer erstellen. Experten weisen darauf hin, dass aus der Dauer eines http-Aufrufs eines Webservers darauf geschlossen werden kann, welche Teile einer Internetseite bzw. eines Online-Angebotes die Nutzer in Anspruch genommen haben. Die Verbindungsdaten lassen damit Rückschlüsse auf die Inhalte der Verbindung zu<sup>127</sup>.

Ebenfalls ist zu berücksichtigen, dass die weitgehenden technischen Möglichkeiten einer automatischen Verarbeitung von Verkehrsdaten deren längerfristige Speicherung und Auswertung zu einem ähnlich intensiven Grundrechtseingriff werden lassen, wie die Speicherung von Kommunikationsinhalten. Das Bundesverfassungsgericht hat schon im Volkszählungsurteil betont, dass es bei der Bemessung der Intensität eines Grundrechtseingriffs nicht allein auf die Art der Angaben, sondern auf ihre Nutzbarkeit und Verwendungsmöglichkeit ankommt<sup>128</sup>. Indem Verkehrsdaten in digitalisierter, standardisierter Form erfasst werden, bestehen für sie ungleich mehr Möglichkeiten ihrer automatisierten Auswertung und Verarbeitung als bei Inhaltsdaten<sup>129</sup>. Der Nutzen von Inhaltsdaten ist zudem sehr eingeschränkt, wenn sie keiner konkreten Person zugeordnet werden können, was aber auf Grund der Verkehrsdaten möglich wird. Daher ist die Behauptung, der durch die Vorratsdatenspeicherung erfolgende Grundrechtseingriff sei geringer

---

<sup>124</sup> BT-Drucks. 16/5846, Begründung zum Regierungsentwurf, S. 51.

<sup>125</sup> Für den Internetbereich dürfte dies bedeuten, dass z.B. URLs, FTP-Transfers sowie Chats nicht gespeichert werden müssen, da es sich dabei um Inhaltsdaten handelt.

<sup>126</sup> Vgl. [www.heise.de/ct/hintergrund/meldung/69995](http://www.heise.de/ct/hintergrund/meldung/69995).

<sup>127</sup> Vgl. [www.heise.de/newsticker/meldung/83054](http://www.heise.de/newsticker/meldung/83054).

<sup>128</sup> BVerfGE 65, 1 (45).

<sup>129</sup> Breyer, Die systematische Aufzeichnung und Vorhaltung von Telekommunikations-Verkehrsdaten für staatliche Zwecke in Deutschland, Berlin 2005, S. 212.

einzustufen, weil es sich dabei „nur“ um Verkehrsdaten handle, in ihrer Pauschalität irreführend<sup>130</sup>.

Nach alledem ist festzuhalten, dass die Pflicht zur Speicherung und Aufbewahrung der in § 113a Abs. 2 bis 5 TKG-E aufgelisteten Daten zu einer sehr umfangreichen Sammlung von sensiblen personenbezogenen Daten führt. Auf deren Grundlage können umfassende Kommunikations- und Bewegungsprofile jedes Nutzers von Telekommunikationsdiensten erstellt werden. Der erwartete Nutzen für die Verbesserung der Strafverfolgung ist im Vergleich zur Intensität der Beeinträchtigung der Kommunikationsfreiheit und der Privatsphäre sämtlicher Kommunikationsnutzer verhältnismäßig gering. Die entsprechenden Regelungen im Gesetzesentwurf verstößen daher gegen den Verhältnismäßigkeitsgrundsatz.

#### *ee) Missbrauchsgefahr durch Private*

Die massenhafte Speicherung von Verkehrs- und Standortdaten erhöht das Risiko eines Datenmissbrauchs<sup>131</sup>. Sobald die Datensammlungen einmal vorhanden sind, werden staatlicherseits als auch von Privaten zunehmende Versuchungen bestehen, diese Daten für andere Zwecke zu nutzen oder die Daten an andere Interessenten zu übermitteln. Dies ist den Verfassern des Gesetzesentwurfes nicht entgangen, denn § 113a Abs. 10 S. 2 TKG-E verpflichtet die Telekommunikationsanbieter, durch technische und organisatorische Maßnahmen sicherzustellen, dass der Zugang zu den gespeicherten Daten ausschließlich hierzu besonders ermächtigten Personen möglich sein soll. Wie diese Maßnahmen konkret aussehen sollen und welche diese „besonders ermächtigten“ Personen sein sollen, wird aber nicht geregelt und bleibt offensichtlich im freien Ermessen der verpflichteten Telekommunikationsdiensteanbieter. Für die Benutzerinnen und Benutzer der Dienste bleibt das Risiko eines unberechtigten Zugriffs durch die Mitarbeiter der Telekommunikationsunternehmen bestehen<sup>132</sup>. Die Tatsache, dass die Speicherung automatisch, also ohne jede Kenntnisnahme durch Personen erfolgen soll, kann dieses Risiko nicht mindern<sup>133</sup>. Technische Fehler führten bereits mehrfach zur Offenlegung von zahlreichen Kundendaten, die plötzlich im Internet zugänglich waren. Wenn aber sensible personenbezogene Daten auch nur für kurze Zeit zugänglich sind, können sich die Betroffenen gegen einen potenziellen Missbrauch ihrer Verbindungsdaten kaum mehr entziehen. Dafür, dass ein solcher Missbrauch keinesfalls nur theoretisch denkbar ist, existieren leider schon zahlreiche Beispiele, etwa für den unberechtigten Zugriff einzelner Unternehmensmitarbeiter auf Telekommunikationsdaten oder für den Verkauf

---

<sup>130</sup> Ausführlich dazu *Breyer*, Die systematische Aufzeichnung und Vorhaltung von Telekommunikations-Verkehrsdaten für staatliche Zwecke in Deutschland, Berlin 2005, S. 213f.

<sup>131</sup> Vgl. *ULD Schleswig-Holstein*, Stellungnahme vom 04.10.2006, S. 4.

<sup>132</sup> Zur ähnlichen Problematik der derzeit nach § 110 TKG einzurichtenden Überwachungsschnittstellen vgl. *Breyer*, Die systematische Aufzeichnung und Vorhaltung von Telekommunikations-Verkehrsdaten für staatliche Zwecke in Deutschland, Berlin 2005, S. 228.

solcher Daten an andere Unternehmen. Die sogenannte „Telefonüberwachungsaffäre“, die im letzten Jahr in Italien für Schlagzeilen sorgte, ist ein weiteres markantes Beispiel solcher Missbrauchsgefahren. Wegen des hohen kommerziellen Werts der Verkehrsdaten ist auch nicht auszuschließen, dass die zur Speicherung Verpflichteten selbst gern die gesammelten Daten anderweitig als im Gesetz vorgesehen nutzen würden<sup>134</sup>. Auf diese Weise könnte die Vorratsdatenspeicherung zu kontraproduktiven Effekten bei der Verbrechensbekämpfung führen, weil sie das Begehen bestimmter Straftaten erleichtern würde<sup>135</sup>. Ein wirksames präventives Datenschutzmanagement erscheint daher im behandelten Zusammenhang zwingend geboten. Der Gesetzesentwurf enthält allerdings keine Vorkehrungen, die dieses gewährleisten können<sup>136</sup>.

#### *e) Zwischenergebnis für die erste Stufe*

Die durch das Umsetzungsgesetz vorgesehene Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten stellt wegen der pauschalen Erfassung umfangreicher Telekommunikationsdaten einer Vielzahl von Personen ohne jeglichen Verdacht einen unverhältnismäßigen Eingriff in das Grundrecht auf Fernmeldegeheimnis aus Art. 10 Abs. 1 GG dar. Mit der umfangreichen anlasslosen Speicherung sensibler Verkehrs- und Standortdaten und den damit verbundenen Gefahren würde es in einem gewissen Sinne keine unbeobachtete Telekommunikation mehr geben. Es bliebe kaum ein Telekommunikationsvorgang, der dem staatlichen Zugriff entzogen ist. Eine freie und unbefangene Telekommunikation wäre unter diesen Umständen nicht mehr möglich. In der Phase der Datenspeicherung wird die Aufzeichnung des Fernmeldeverkehrs weder rechtlich noch tatsächlich begrenzt.

### ***1.3. Stufe 2: Zugriff auf die Vorratsdaten als Eingriff in das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG***

Auch wenn anzunehmen wäre, dass die anlasslose Erhebung und Speicherung sämtlicher Verbindungsdaten aller Kommunikationsteilnehmer generell nicht gegen das durch Art. 10 Abs. 1 GG gewährleistete Fernmeldegeheimnis verstößt, sind die im Entwurf geregelten Zugriffs- und

---

<sup>133</sup> Die entsprechende Bemerkung in der Begründung zum Gesetzesentwurf steht in einem gewissen Widerspruch zur Verpflichtung zu Sicherungsmaßnahmen in § 113a Abs. 10 S. 2 TKG-E. Vgl. BT-Drucks. 16/5846, Begründung zum Regierungsentwurf, S. 31.

<sup>134</sup> Vgl. für entsprechende Beispiele *Breyer*, Die systematische Aufzeichnung und Vorhaltung von Telekommunikations-Verkehrsdaten für staatliche Zwecke in Deutschland, Berlin 2005, S. 231.

<sup>135</sup> Diesbezüglich ist zu bemerken, dass dem Grundgesetz eine Schutzpflicht des Staates zu entnehmen ist, in solchen sensiblen Bereichen wie der Umgang mit personenbezogenen Daten vor Beeinträchtigungen durch Private zu schützen oder sie mindestens nicht zu erleichtern. Dementsprechend bestehen Regelungen, die die Erfüllung dieser Schutzpflicht sichern (vgl. z. B. § 88 Abs. 2 TKG, wonach die Telekommunikationsdienstleister zum Schutz des Fernmeldegeheimnisses verpflichtet sind). Mit dem vorgelegten Gesetzesentwurf wird aber dieser Schutzpflicht keinesfalls Genüge getan.

Verwendungsmöglichkeiten der auf Vorrat gespeicherten Daten selbständige unverhältnismäßige Eingriffe in das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG.

Das Bundesverfassungsgericht hat in ständiger Rechtsprechung besondere Anforderungen an den staatlichen Informationszugriff auf personenbezogene Telekommunikationsdaten gestellt. Bei der Bemessung der Intensität des Grundrechtseingriffs sind danach die Gestaltung der Eingriffsschwellen, die Bestimmung der zugriffsberechtigten Behörden, die Zahl der Betroffenen und ihre Identifizierbarkeit, die Intensität der Beeinträchtigungen, die Missbrauchsgefahren sowie die aus dem Bestimmtheitsgebot folgende Notwendigkeit einer hinreichenden und normenklaren Bestimmung des Zwecks der Datenerhebung und -verwendung zu berücksichtigen<sup>137</sup>.

### *a) Zugriffsberechtigte Behörden und Art der Informationszugriffe*

Die Vorratsdatenspeicherungsrichtlinie eröffnet den Mitgliedsstaaten Ermessensspielräume, was die Bestimmung der zugriffsberechtigten Behörden und der Zugriffsvoraussetzungen und -verfahren betrifft (Art. 4 RL 2006/24/EG). Damit wird den Unterschieden in den jeweiligen mitgliedstaatlichen Rechtsordnungen, die die Struktur und die Kompetenzen der nationalen Strafverfolgungsbehörden regeln, Rechnung getragen. Eine Möglichkeit zur Verwendung der Vorratsdaten von anderen Behörden und zu anderen Zwecken als für die der Strafverfolgung sieht die Richtlinie nicht vor (vgl. Art. 4 und Art. 11 RL 2006/24/EG i.V.m. Art. 15 Abs. 1 der Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG)<sup>138</sup>.

Demgegenüber regelt der Regierungsentwurf Zugriffsmöglichkeiten auf die vorrätig gespeicherten Daten nicht nur für die Strafverfolgungsbehörden, sondern auch für die Verfassungsschutzbehörden des Bundes und der Länder, die Nachrichtendienste und die übrigen mit der Abwehr von erheblichen Gefahren beauftragten Behörden (§ 113b TKG-E). Die entsprechenden Regelungen in den jeweiligen Gesetzen sollen zusätzlich geändert werden und eine Bezugnahme auf den künftigen § 113a TKG enthalten (§ 113b TKG-E)<sup>139</sup>. Damit geht der Gesetzentwurf auch in diesem Punkt über die Vorgaben der Richtlinie deutlich hinaus und intensiviert die Intensität des mit der Vorratsdatenspeicherung herbeigeführten Grundrechtseingriffs erheblich. Insbesondere die geplanten Befugnisse der Nachrichtendienste, auf die vorrätig gespeicherten Daten zuzugreifen, wären wegen der diesbezüglichen geringen Rechtsschutzmöglichkeiten der Betroffenen mit dem Grundgesetz nicht vereinbar.

---

<sup>136</sup> So auch das *ULD Schleswig-Holstein*, Stellungnahme vom 04.10.2006, S. 4.

<sup>137</sup> Vgl. BVerfGE 100, 313 (376); 107, 299 (320); 113, 348 (282).

<sup>138</sup> In diesem Sinne auch die Schlussanträge der Generalanwältin Kokott vom 18.7.2007 im EuGH-Verfahren zur Rechtssache C-275/06, Nr. 123-124

<sup>139</sup> Nach der geltenden Rechtslage dürfen die Nachrichtendienste sowie die Verfassungsschutzämter auf bestimmte Verkehrsdaten zugreifen. Vgl. § 100g StPO, § 3 Nr. 3 TKG, §§ 112, 113 TKG, § 8a Abs. 2 Nr. 4 BVerfSchG, § 2a S. 1 BNDG, § 10 4a S. 1 MADG.

In der Begründung zum ursprünglichen Gesetzesentwurf des Bundesjustizministeriums wurde versucht, die Verhältnismäßigkeit der Gesamregelung gerade mit dem Argument zu retten, dass die Geheimdienste keinen Zugriff auf die Vorratsdaten erhalten. Danach sollte eine Übermittlung der gespeicherten Vorratsdaten für andere Zwecke als zur Verfolgung von Straftaten nicht zulässig sein. Damit sei – so die Begründung des Referentenentwurfs – „insbesondere eine Übermittlung der allein auf der Grundlage des § 110a TKG-E gespeicherten Daten für Zwecke der Gefahrenabwehr, der Aufgabenerfüllung der Dienste oder auch zur Erfüllung zivilrechtlicher Ansprüche“ ausgeschlossen<sup>140</sup>. Die Gründe für die Änderung dieser Rechtsauffassung beim Verfassen des Regierungsentwurfs sind nicht ersichtlich<sup>141</sup>.

Der Regierungsentwurf sieht außerdem grundlegende Änderungen bezüglich der Art des staatlichen Zugriffs auf Verkehrsdaten vor. Durch die Neufassung des § 100g Abs. 1 StPO-E soll der bisherige Auskunftsanspruch der Strafverfolgungsbehörden gegenüber den Telekommunikationsunternehmen in eine umfassende Erhebungsbefugnis für Verkehrsdaten umgewandelt werden<sup>142</sup>. Ihnen soll es künftig erlaubt sein, selbst und in Echtzeit Verkehrs- und Standortdaten zu erheben und zu verwerten. Die Auskunftspflichtung der Dienstanbieter bleibt davon unberührt<sup>143</sup>. Mit dem Verzicht auf das Tatbestandsmerkmal „im Falle einer Verbindung“ und mit der Zulassung der Echtzeiterhebung von Standort- und Verbindungsdaten bei der mobilen Telephonie wird künftig die Erstellung von Bewegungsprofilen einzelner Personen möglich sein. Dies stellt einen tiefgehenden Eingriff in das Grundrecht auf vertrauliche Telekommunikation dar, für dessen Rechtfertigung keine Gründe ersichtlich sind. Zu bemerken ist dazu, dass auch in diesem Punkt eine Verschärfung der Regelung im Vergleich zum ersten Referentenentwurf besteht. Ursprünglich war die Verkehrsdatenabfrage in Echtzeit nur bei in § 100a Abs. 2 StPO bezeichneten Straftaten vorgesehen. Die Regelung des § 100g Abs. 1 S. 3 StPO weitet die Echtzeitabfrage auf alle im § 100g Abs. 1 S. 1 Nr. 1 StPO bezeichneten Straftaten aus.

Bedenken bestehen auch hinsichtlich des staatlichen Zugriffs auf die dynamischen IP-Adressen im Internetbereich<sup>144</sup>. De lege lata ist diesbezüglich die Norm des § 113 Abs. 1 TKG relevant. Danach sind die Anbieter von Telekommunikationsdiensten verpflichtet, den zuständigen Stellen Auskunft über die nach den §§ 95 und 111 TKG erhobenen Bestandsdaten zu erteilen, soweit dies für die Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder für die Erfüllung der Aufgaben der Verfassungsschutzbehörden, des Bundesnachrichtendienstes oder des Militärischen Abschirmdienstes erforderlich ist. Nach allgemeiner Auffassung ist die Norm bei Auskunftersuchen bezüglich statischer IP-Adressen

---

<sup>140</sup> Begründung Ref.-E., S. 151.

<sup>141</sup> Gleichwohl werden die Verhältnismäßigkeitsprobleme in der Begründung zum Regierungsentwurf erkannt (vgl. BT-Drucks. 16/5846, Begründung zum Regierungsentwurf, S. 74).

<sup>142</sup> BT-Drucks. 16/5846, Begründung zum Regierungsentwurf, S. 50.

<sup>143</sup> § 100g Abs. 2 S. 1 StPO-E i.V.m. § 100b Abs. 3 StPO-E.

<sup>144</sup> § 113a Abs. 2 Nr. 5, Abs. 3 Nr. 1-3 und Abs. 4 Nr. 1, 3 TKG-E sehen die Speicherung von IP-Adressen bei den verschiedenen Internetkommunikationsvorgängen vor, ohne dabei nach statischen und dynamischen IP-Adressen zu differenzieren.

einschlägig, weil diese Adressen als Bestandsdaten im Sinne von § 3 Nr. 3 TKG anzusehen sind<sup>145</sup>. Demgegenüber stellen die dynamischen IP-Adressen aber Verkehrsdaten dar, u.a. weil sie in keinem unmittelbaren Zusammenhang mit dem jeweiligen Vertragsverhältnis stehen. Dementsprechend dürfen derzeit Auskunftersuchen bezüglich dynamischen IP-Adressen nach Maßgabe der §§ 100g und 100h StPO angeordnet werden. Die relevante Rechtsprechung ist allerdings uneinheitlich<sup>146</sup>. Eine gesetzliche Klarstellung, dass der Zugriff auf die dynamischen IP-Adressen nur unter den Voraussetzungen des § 110g StPO-E zulässig ist, erscheint wegen ihrer hohen Aussagekraft daher notwendig<sup>147</sup>. Darauf verzichtet aber der Regierungsentwurf, was der Sensibilität der aufgrund der dynamischen IP-Adressen zu erlangenden Informationen nicht gerecht ist<sup>148</sup>. Eine uneinheitliche Rechtspraxis, bei der unter Umständen auch zur inhaltlichen Überwachung der Internetnutzung kommen kann, erscheint somit vorprogrammiert<sup>149</sup>.

#### *b) Voraussetzungen für den Zugriff auf die vorrätig gespeicherten Verkehrsdaten*

##### *aa) Straftatenkatalog für den staatlichen Zugriff auf die Vorratsdaten (§ 100g Abs. 1 StPO-E)*

Gemäß Art. 1 Abs. 1 Richtlinie 2006/24/EG bezweckt sie die verbindliche Speicherung und die Sicherung der Verfügbarkeit der Verkehrsdaten zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten. Es wird nicht ausdrücklich festgelegt, was unter „schwere Straftaten“ zu verstehen ist<sup>150</sup>, den EU-Mitgliedsstaaten stehen daher Ermessensspielräume zu.

Nach § 100g Abs. 1 StPO-E darf Auskunft über die gespeicherten Verkehrsdaten zur Verfolgung von Straftaten von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Abs. 2 StPO-E bezeichnete Straftat, sowie zur Verfolgung von mittels Telekommunikation begangenen

<sup>145</sup> Gercke, in: F. Roggan/M. Kutscha (Hrsg.), Handbuch zum Recht der inneren Sicherheit, 2. Aufl., Berlin 2006, S. 170.

<sup>146</sup> Vgl. einerseits *LG Bonn*, DuD 2004, S. 628 und andererseits *LG Hamburg*, MMR 2005, S. 711, *LG Stuttgart*, NJW 2005, S. 614.

<sup>147</sup> Diesbezüglich heißt es in der Stellungnahme des Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein zum Regierungsentwurf vom 27.06.2007, S. 14: „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.“

<sup>148</sup> Die Begründung zum Regierungsentwurf betrachtet die dynamischen IP-Adressen pauschal als Bestandsdaten und verweist auf eine angeblich gefestigte Rechtsprechung, die zur Anwendbarkeit des § 113 TKG gelange. Vgl. BT-Drucks. 16/5846, S. 26-27.

<sup>149</sup> Vgl. Zöller, GA 2007, S. 393 (407).

<sup>150</sup> Vgl. auch die Erklärung des Europarates zum Begriff der „schweren Straftat“, Ratsdokument 5777/06 ADD 1 REV 1 vom 17.02.2006, <http://register.consilium.europa.eu/pdf/de/06/st05/st05777-ad01re01.de06.pdf>. Diese Erklärung kann allerdings die fehlende Definition in der Richtlinie nicht ersetzen, da der Rat nicht befugt ist, durch einen eigenen Beschluss eine Richtlinie zu ergänzen.

Straftaten verlangt werden. Der Verweis auf § 100a Abs. 2 StPO-E ist also nur beispielhaft, d.h. es kann auch andere Straftaten von „erheblicher Bedeutung“ geben, zu deren Verfolgung ein Zugriff auf die gespeicherten Daten möglich sein soll<sup>151</sup>. Kriterien für die Bestimmung dieser weiteren Straftaten sind dem Text des Gesetzentwurfs nicht zu entnehmen.

Die Begründung des Gesetzentwurfs betont zu Recht die inhaltlichen Unterschiede bei den Begriffen „schwere Straftat“, „Straftat von erheblichen Bedeutung“ und „besonders schwere Straftat“. Der Begriff der „schweren Straftat“ nähme eine Zwischenstellung ein. Hierunter könnten solche Straftaten verstanden werden, die eine Mindesthöchststrafe von fünf Jahren Freiheitsstrafe aufweisen, in Einzelfällen aufgrund der besonderen Bedeutung des geschützten Rechtsgutes oder des besonderen öffentlichen Interesses an der Strafverfolgung aber auch eine geringere Freiheitsstrafe<sup>152</sup>.

Der Gesetzentwurf lässt jedoch einen Zugriff auf die gespeicherten Verbindungsdaten schon bei Straftaten von erheblicher Bedeutung zu, und nicht erst bei schweren Straftaten, wie Art. 1 Abs. 1 der Richtlinie ausdrücklich verlangt. Die Begründung versucht dies mit einer wenig überzeugenden Sprachequiblistik zu rechtfertigen, indem der in der Richtlinie verwendete Begriff der „schweren Straftat“ mit dem Begriff der „Straftat von erheblicher Bedeutung“ nach der StPO gleichgesetzt wird. Die deutsche Übersetzung des englischen Begriffs „serious crime“ sei unglücklich gewählt worden. Dieser Begriff diene in europäischen Rechtsinstrumenten dazu, Tatbestände auszugrenzen, die lediglich die Schwere von Ordnungswidrigkeiten oder Bagatelldelinquenz erreichen, und sei im europäischen Kontext sinngemäß als „ernsthafte Straftat“ zu übersetzen und nicht mit schwerer Kriminalität zu assoziieren<sup>153</sup>.

Dabei wird erstens verkannt, dass europäische Rechtsakte in allen sprachlichen Fassungen gleich verbindlich sind. Zweitens ist zu bemerken, dass eine etablierte europarechtliche Terminologie im Bereich des Strafrechts – wegen der geringen Kompetenzen der EU in diesem Bereich – kaum existiert. Vielmehr ist es üblich, in den jeweiligen Regelungsinstrumenten entsprechende Begriffbestimmungen aufzunehmen<sup>154</sup>. Diese Auffassung kann drittens auch angesichts der Entstehungsgeschichte der Richtlinie nicht überzeugen – während des Rechtsetzungsprozesses hatte das Europäische Parlament die Begrenzung auf schwere Straftaten mühsam erreicht. Viertens ist auch die Behauptung abwegig, dass Art. 1 der Richtlinie 2006/24/EG keine Schwelle für den Zugriff auf die zu speichernden Daten vorgäbe, sondern lediglich den Zweck der Richtlinie umschreibe<sup>155</sup>. In der Diskussion um die europäische Rechtsgrundlage der Richtlinie wurde jedoch angeführt, dass mit der Richtlinie eine Harmonisierung der Regelungen zur Speicherung von

---

<sup>151</sup> In § 113b TKG-E, der ausweislich der Begründung den Zweck der Datenspeicherung und Datenverwendung regeln soll, wird lediglich die „Verfolgung von Straftaten“ genannt.

<sup>152</sup> BT-Drucks. 16/5846, Begründung zum Regierungsentwurf, S. 40.

<sup>153</sup> BT-Drucks. 16/5846, Begründung zum Regierungsentwurf, S. 53.

<sup>154</sup> Vgl. beispielsweise Art. 2 Abs. 1 des Rahmenbeschlusses des Rates vom 13. Juni 2002 über den Europäischen Haftbefehl und die Übergabeverfahren zwischen den Mitgliedsstaaten 2002/584/JI (ABl. EU Nr. L 190, S. 1).

Verbindungsdaten für alle Mitgliedsstaaten erreicht werden solle. Die mit der Richtlinie angestrebte Harmonisierung besteht gerade darin, dass Telekommunikationsverbindungsdaten zum Zweck der Ermittlung und Verfolgung von schweren Straftaten zur Verfügung stehen. Indem der Gesetzentwurf einen Zugriff auf die Verbindungsdaten bereits beim Verdacht auf Straftaten von erheblicher Bedeutung zulassen will, geht er über die Vorgaben aus Art. 1 Abs. 1 der Richtlinie 2006/24/EG hinaus.

Zweifelhaft ist auch, ob der interpretationsbedürftige Bezug auf „Straftaten von erheblicher Bedeutung“ in § 100g Abs. 1 Nr. 1 StPO-E dem Bestimmtheitserfordernis gemäß Art. 10 Abs. 1 GG genügt. Entsprechend dem aus dem Rechtsstaatsprinzip ableitbaren Bestimmtheitsgebot müssen sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Einzelnen erkennbar aus dem Gesetz ergeben<sup>156</sup>. Die Begründung zum Gesetzesentwurf geht davon aus, dass eine solche Straftat mindestens dem Bereich der mittleren Kriminalität zuzurechnen sein, den Rechtsfrieden empfindlich stören und dazu geeignet sein müsse, das Gefühl der Rechtssicherheit der Bevölkerung zu beeinträchtigen<sup>157</sup>. Sowohl der Normtext als auch die Begründung enthalten unbestimmte Begriffe, die eine sehr weite Auslegung erlauben und damit für die Rechtsanwendung keine feste Grundlage bieten. Dem Gebot der Normklarheit, das bei Eingriffen in das Fernmeldegeheimnis besonders zu berücksichtigen ist, wird somit nicht Genüge getan. Vielmehr erscheint es wegen des intensiven Grundrechtseingriffs verfassungsrechtlich geboten, die betreffenden Straftaten in einem enger verfassten, abschließenden Katalog aufzulisten<sup>158</sup>. Indem der Gesetzentwurf die relevanten Straftaten nicht klar definiert, verstößt er auch gegen den Grundsatz der konkreten Zweckbestimmung beim Zugriff auf personenbezogene Daten.

Es ist außerdem fragwürdig, ob der generelle Verweis auf den umfangreichen Straftatenkatalog des § 100a Abs. 2 StPO-E angesichts der „Streubreite“ der Vorratsdatenspeicherung angemessen ist. Der Gesetzgeber müsste prüfen und begründen, ob die Verwendung der durch die Vorratsdatenspeicherung gewonnenen Daten bei der Verfolgung aller im § 100a Abs. 2 StPO-E aufgezählten Straftaten dem Verhältnismäßigkeitsgrundsatz entspricht.

Zu kritisieren ist ferner, dass die Subsidiaritätsklausel des § 100g Abs. 1 S. 2 StPO-E nur die Kategorie der mittels Telekommunikationseinrichtungen begangenen Straftaten betrifft. Der Zugriff auf die gespeicherten Verkehrsdaten ist also im Fall einer der im § 100a Abs. 2 StPO-E genannten Straftaten nicht an die Voraussetzung gebunden, dass die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos

---

<sup>155</sup> BT-Drucks. 16/5846, Begründung zum Regierungsentwurf, S. 53.

<sup>156</sup> Zu den verfassungsrechtlichen Bedenken bezüglich des Begriffs „Straftat von erheblicher Bedeutung“ vgl. *Gercke*, in: F. Roggan/M. Kutscha (Hrsg.), *Handbuch zum Recht der inneren Sicherheit*, 2. Aufl., Berlin 2006, S. 159f. Das Bundesverfassungsgericht hat allerdings den Begriff im Hinblick auf § 110g StPO als hinreichend bestimmt angesehen (BVerfGE 107, 299, 322).

<sup>157</sup> BT-Drucks. 16/5846, Begründung zum Regierungsentwurf, S. 40.

<sup>158</sup> Hier bietet sich eine Lösung nach dem Vorbild des Katalogs des Rahmenbeschlusses zum Europäischen Haftbefehl an. Vgl. dazu *Westphal*, *EuZW*, S. 555 (558).

wäre und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht. Ist schon die praktische Bedeutung der Subsidiaritätsklausel in § 100g Abs. 1 S. 2 zweifelhaft<sup>159</sup>, so wird bei der Verfolgung von Straftaten von erheblicher Bedeutung gänzlich auf den Vorrang offener Ermittlungsmethoden verzichtet.

Bezüglich der mittels Telekommunikationsmittel begangenen Straftaten sieht der Gesetzesentwurf nicht vor, dass sie auch schwere Straftaten bzw. Straftaten von erheblicher Bedeutung sein müssen und geht damit erneut über die Vorgaben der Richtlinie hinaus (vgl. Art. 1 Abs. 1 RL). Der Mangel an einschränkenden Merkmalen im Hinblick auf die Schwere oder Erheblichkeit der Anlasstat bei mittels Telekommunikationseinrichtungen begangener Straftaten könnte dazu führen, dass ein Zugriff auf die umfangreichen und aussagekräftigen Verkehrsdaten auch bei Bagatelldelikten, etwa bei einer Beleidigung per Telefon, erfolgt. Dies lässt die Regelung des § 100g Abs. 1 S. 1 Nr. 2 StPO-E unverhältnismäßig erscheinen und widerspricht dem vom Bundesverfassungsgericht entwickelten Grundsatz der möglichst grundrechtsschonenden Umsetzung von europäischen Rechtsakten<sup>160</sup>. Der Verweis in der Begründung auf einen Beschluss des Bundesverfassungsgerichts<sup>161</sup>, wonach die Erhebung von Verkehrsdaten bei mittels Telekommunikationseinrichtungen begangenen Straftaten nicht erheblichen verfassungsrechtlichen Bedenken begegnen soll, kann die im Entwurf enthaltene gesetzgeberische Lösung nicht rechtfertigen<sup>162</sup>. Bei dem erwähnten Beschluss handelt es sich um eine Nichtannahme-Entscheidung des Gerichts. Sie bezieht sich konkret auf die bisher geltende Rechtslage und ist auf die Vorratsdatenspeicherung wegen ihrer neuartigen grundrechtseingreifenden Intensität nicht übertragbar<sup>163</sup>.

Noch weniger hinreichend bestimmt ist der Zweck des staatlichen Zugriffs seitens der Verfassungsschutzämter, der Geheimdienste und der anderen zugriffsberechtigten Behörden. An einem Katalog von Straftaten bzw. Gefahren, die den Informationseingriff rechtfertigen sollen, fehlt es hier. Nach geltender Rechtslage sind diese Behörden bei Ausübung ihrer Befugnisse in Zusammenhang mit dem Zugriff auf Verkehrsdaten an keinen konkreten Straftatenverdacht bzw. an keine konkrete Gefahrenlage gebunden. Teilweise sind die relevanten Regelungen noch zu schaffen (vgl. § 113b TKG-E). Damit wird die Grundlage für spätere Erweiterungen des staatlichen Zugriffs auf die Verkehrsdaten geschaffen.

Zusammenfassend ist festzustellen, dass mit der Verwendung der gesammelten Daten zur Aufklärung mittelschwerer und mittels Telekommunikationseinrichtungen begangener Straftaten eine unverhältnismäßige Lösung vorgeschlagen wurde, die über die Vorgaben der Vorratsdatenspeicherungsrichtlinie hinaus geht.

---

<sup>159</sup> Vgl. Abschnitt B I Nr. 1 dieser Stellungnahme.

<sup>160</sup> Vgl. *BVerfG*, NJW 2005, S. 2289 („Europäisches Haftbefehlsgesetz“).

<sup>161</sup> Vgl. *BVerfG*, 2 BvR 1085/05 vom 17.06.2006, Absatz Nr. 17-18.

<sup>162</sup> BT-Drucks. 16/5846, Begründung zum Regierungsentwurf, S. 52.

<sup>163</sup> Außerdem fordert das Bundesverfassungsgericht auch in diesem Fall die Einhaltung des Verhältnismäßigkeitsgrundsatzes. Die nicht näher begründete Aussage, wonach sich der Anspruch eines Beschuldigten auf

### *bb) Zu niedrige Eingriffsschwelle*

Für den Zugriff auf die von den Telekommunikationsanbietern gespeicherten Daten zu Zwecken der Strafverfolgung ist lediglich ein Anfangsverdacht vorgesehen (§ 100g Abs. 1 S. 1 StPO-E). Die Praxis zeigt, dass es nicht selten vorkommt, dass ein Anfangsverdacht allein auf Grund der Tatsache, dass jemand auf einer E-Mail-Userliste steht, angenommen wird. Diese niedrige Eingriffsschwelle ist angesichts des breiten Betroffenenkreises und der Vielzahl der gespeicherten Daten unangemessen. Zweifelhaft ist außerdem, ob das damit einhergehende Ausmaß der vorgesehenen Zugriffsbefugnisse in einem angemessenen Verhältnis zu ihrem tatsächlichen Nutzen steht<sup>164</sup>.

Beim Zugriff auf die vorrätigen Verkehrsdaten zu Zwecken der Abwehr von erheblichen Gefahren und zur Aufgabenerfüllung der Verfassungsschutzämter und der Geheimdienste sind die Eingriffsschwellen ebenfalls niedrig angesetzt bzw. sehr allgemein formuliert. Die Begriffe „erhebliche Gefahr“ (§113b TKG-E), „schwerwiegende Gefahr“ (§ 8a Abs. 2 BVerfSchG, § 2a S. 2 BNDG) und „schwerwiegende Gefährdung“ (§ 4a S. 1 MADG) sind ungeeignet, zu bestimmen, wann der Zugriff auf die Daten zulässig sein soll.

### *c) Unzureichende Differenzierung bezüglich der betroffenen Personen (Kontaktpersonen)*

Nach § 100a Abs. 3 StPO-E darf sich die Anordnung auch gegen eine Person richten, von der auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennimmt oder weitergibt oder dass der Beschuldigte ihren Anschluss benutzt. Diese Vorschrift bezieht sich auf die Telekommunikationsüberwachung, soll aber auf die Erhebung von Verkehrsdaten entsprechend angewandt werden (§ 100g Abs. 1 S. 1 StPO-E). Die Verkehrsdatenabfragen wird deshalb regelmäßig weitere Telekommunikationspartner betreffen, die zufällig den gleichen Rechner oder den gleichen Telefonanschluss nutzen und die an der jeweiligen Straftat gänzlich unbeteiligt sind. Aufgrund dieser hohen „Streubreite“ der betroffenen Personen erscheint die Regelung für Kontaktpersonen und Nachrichtenmittler nicht ausreichend bestimmt. Es fehlt ein handhabbarer Maßstab für die Prüfung, beim Vorliegen welcher konkreten Tatsachen eine Unterstützung des Beschuldigten durch eine Drittperson mittels Kommunikationsmittel anzunehmen ist. Selbst eine restriktive Auslegung der vorgeschlagenen Regelung könnte das Bestimmtheitsdefizit nicht beseitigen.

---

vertrauliche Telekommunikation beim Einsatz einer Telekommunikationsanlage als Tatmittel mindern soll, kann nicht überzeugen (vgl. BVerfG, 2 BvR 1085/05 vom 17.06.2006, Absatz Nr. 17).

<sup>164</sup> Mehr dazu bei *Breyer*, Die systematische Aufzeichnung und Vorhaltung von Telekommunikations-Verkehrsdaten für staatliche Zwecke in Deutschland, Berlin 2005, S. 178f., 265f.

Dasselbe gilt ebenfalls für die Normen, die die entsprechenden Befugnisse bezüglich der Erhebung und Verwertung von Verkehrsdaten durch die Verfassungsschutzämter, die Nachrichtendienste und die übrigen zugriffsberechtigten Behörden regeln (vgl. beispielsweise § 8a Abs. 3 i.V.m. Abs. 2 Nr. 4 BVerfSchG, § 4a MADG, § 2a S. 3 BNDG<sup>165</sup>).

#### *d) Zwischenergebnis für die zweite Stufe*

Die Regelung der Zugriffsmöglichkeiten auf die Vorratsdaten zur Verfolgung mittelschwerer und aller mittels Telekommunikationseinrichtungen begangener Straftaten sowie bei der Gefahrenabwehr und der Aufgabenerfüllung der Geheimdienste ist unverhältnismäßig und geht über die Vorgaben der Richtlinie hinaus. Dies wird noch dadurch verstärkt, dass für die Verwendung von Vorratsdaten bereits ein Anfangsverdacht reicht und die Differenzierung bezüglich der Kontaktpersonen bzw. Nachrichtenmittler unzureichend ist.

## **2. Verstoß gegen Art. 12 Abs. 1 GG**

Mit der Verpflichtung der Telekommunikationsunternehmen zur Speicherung der in § 113a Abs. 2 bis 5 TKG-E bezeichneten Daten wird in ihre Unternehmensfreiheit als Unterfall der Berufsfreiheit (Art. 12 Abs. 1 GG) eingegriffen. Um die Speicherungspflichten zu erfüllen, müssten die Dienstanbieter erhebliche Investitionen vornehmen und ggf. neues Personal anstellen<sup>166</sup>. Außerdem werden zusätzliche Betriebskosten entstehen. Davon würden insbesondere die kleineren Telekommunikationsunternehmen besonders hart betroffen, so dass Insolvenzen als Folge der neuen Gesetzeslage durchaus möglich erscheinen.

Weitere Eingriffe in die Unternehmensfreiheit stellen die in § 113a Abs. 7 TKG-E enthaltene Verpflichtung der Telekommunikationsunternehmen, Angaben zu ihrer Netzplanung zu machen, und das praktische Verbot von Anonymisierungsdiensten (§113a Abs. 6 TKG-E) dar. Aufgrund des zu erwartenden Vertrauensverlustes in die Sicherheit und Vertraulichkeit von Telekommunikationsdiensten müssen die Unternehmen befürchten, dass viele Kunden ihr Kommunikationsverhalten und deshalb die Inanspruchnahme ihrer Dienstleistungen einschränken werden bzw. Kunden dadurch verloren gehen, indem sie ihre Kommunikation über ausländische Dienstanbieter abwickeln, die nicht den Regeln der Vorratsdatenspeicherung unterworfen sind.

Der Eingriff in die Unternehmensfreiheit der zur Speicherung verpflichteten Telekommunikationsanbieter wird besonders dadurch intensiviert, dass der Gesetzesentwurf keine Entschädigung

---

<sup>165</sup> Diese Regelungen sollen entsprechend § 113b TKG-E, der eine ausdrückliche Bezugnahme auf den künftigen § 113a TKG fordert, geändert werden.

<sup>166</sup> Nach Berechnungen des BITKOM würde die Vorratsdatenspeicherung für die Industrie Anfangsinvestitionen in Höhe von 150 Mio. Euro verursachen (BITKOM, Presseinformation vom 15. März 2005). Die Begründung des Gesetzesentwurfs geht hingegen aufgrund der Angaben eines großen Telekommunikationsanbieters davon aus, dass der zusätzliche Investitionsaufwand nicht erheblich sein wird (vgl. Begründung zum Referentenentwurf, S. 71).

vorsieht<sup>167</sup>. Der Deutsche Bundestag hatte einst die Bundesregierung ausdrücklich aufgefordert, zeitnah einen Gesetzesentwurf für eine angemessene Entschädigung der Telekommunikationsunternehmen vorzulegen<sup>168</sup>. Die Kosten für die Inanspruchnahme bei der Erfüllung hoheitlicher Ermittlungsmaßnahmen sollten nach dem Willen des Bundestages nicht auf die Unternehmen abgewälzt werden. Ob dies mit der geplanten Änderung des JVEG in ausreichendem Maße geschehen wird, bleibt abzuwarten. Jedenfalls stellt die Verpflichtung der Telekommunikationsunternehmer zur Speicherung und Weitergabe von Verkehrsdaten ohne eine Entschädigung für die daraus entstehenden Zusatzkosten und für die sonstigen wirtschaftlichen Nachteile eine unverhältnismäßige Einschränkung der Unternehmensfreiheit dar und ist somit verfassungswidrig. Ein Blick ins Ausland zeigt, dass die Verfassungsgerichte von Österreich und Frankreich schon in diesem Sinne entschieden haben<sup>169</sup>.

### 3. Ergebnis der verfassungsrechtlichen Prüfung

Die Umsetzung zur Vorratsdatenspeicherung verstößt mehrfach gegen grundrechtliche Schutzgarantien. Die Vorratsdatenspeicherung ist bereits mit ihrem Ansatz, sämtliche Verbindungsdaten aller Kommunikationsteilnehmer anlasslos zu speichern, verfassungswidrig. Eine verfassungskonforme Umsetzung kann insoweit nicht gelingen.

---

<sup>167</sup> Bemerkenswert ist diesbezüglich, dass der ursprüngliche Richtlinienentwurf eine Entschädigung vorsah, die bei den späteren Beratungen entfallen ist. Vgl. dazu *Köcher/Kaufmann*, DuD 2006, S. 360 (364).

<sup>168</sup> Vgl. BT-Drucks. 16/545, S. 4.

<sup>169</sup> *Conseil constitutionnel*, DC 2000-441 vom 28.12.2000; *Österreichischer Verfassungsgerichtshof*, G 37/02-16 vom 27.02.2003.