Stellungnahme der Humanistischen Union

zum Referentenentwurf eines „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ vom 27. November 2006

Autorinnen und Autoren:
Dr. Miroslav Angelov, Nils Bergemann, Dr. Dr. hc. Burkhard Hirsch,
Martina Kant, Sven Lüders, Dr. Till Müller-Heidelberg, Burckhard Nedden,
Dr. Fredrik Roggan, Gerhard Saborowski, 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)

Inhalt:

A. Einleitung

Die Stellungnahme der Humanistischen Union zum Referentenentwurf für ein Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie zur Vorratsdatenspeicherung (2006/24/EG) ist aufgrund der knappen Stellungnahmefrist keine umfassende Bewertung. Sie konzentriert sich auf die grundsätzliche verfassungsrechtliche und rechtspolitische Bewertung des Gesetzentwurfs. Wir werden an ihr mit dem Fortgang des Gesetzgebungsprozesses weiterarbeiten.

Im ersten Teil nehmen wir zur Neuregelung der verdeckten Ermittlungsmaßnahmen in der Strafprozessordnung Stellung, im zweiten Teil befassen wir uns mit den Regelungen zur Umsetzung der EU-Richtlinie zur Vorratsdatenspeicherung.

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[1] und die Studie der Universität Bielefeld[2] 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 beeinträchtige und damit möglicherweise Tatsachen verborgen blieben, die nicht nur für die Strafverfolgung, sondern auch für die Verteidigung wichtig sein könnten. Dies ist ein rhetorisches Hilfsargument, dessen praktische Be-

---

1 *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

2 *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.

deutung 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 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 muss man doch fragen, 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 – 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 erhobe-

ne Nichtigkeitsklage gegen die Richtlinie Erfolg haben wird3. 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 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 Speicherungs- und 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.

[3] EuGH, Rs. C-301/06.

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

I. Eingriffsschwellen

Die Regelungen des Gesetzentwurfs werden im Ergebnis zur 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[4]. 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[5] 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[6] 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"[7].

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 formu-

---

4 So besonders deutlich in dem neuen § 101 StPO-E.

5 Siehe Fn. 1.

6 S. 46f.

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

liert, 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. nicht möglich oder wesentlich erschwert (§ 100i Abs. 2 StPO-E)
e. unverhältnismäßig erschwert oder aussichtslos (§ 100c Abs. 1 StPO-E)
f. weniger erfolgversprechend oder erschwert (§ 100i Abs. 3 Satz 1: § 100h Abs. 2 StPO-E)
g. erheblich weniger erfolgversprechend oder wesentlich erschwert (§ 100i Abs. 3 Satz 2 StPO-E; § 100h Abs. 3 Satz 2 Nr. 1 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 unvertretbar höherem 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[8]. Das bedeutet, dass es auf die Darlegungen der – zudem mit einem Beurteilungsspielraum ausgestatteten[9] – Strafverfolgungsbehörden ankäme, ob bei Nichtanordnung eines großen Lauschangriffs eine Vernachlässigung von anderen Ermittlungen zu befürchten ist oder eben nicht[10]. Es sind angesichts dieser Interpretation berechtigte Zweifel geäußert worden, ob ein derart dehnbares Tatbestandsmerkmal eine verdeckte Maßnahme tatsächlich als letztes Mittel der Strafverfolger erscheinen lässt[11]. 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. Vorge-

---

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

9 BGHSt 41, 30 (33).

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

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

schlagen wird, dass die verdeckten Ermittlungsmaßnahmen nur dann zulässig sein sollen, wenn andere weniger grundrechtsintensive Maßnahmen **aussichtslos** wären.

Im Übrigen ist nicht nachvollziehbar, aus welchem Grund der Entwurf eine uneinheitliche Sprachregelung selbst für ein und denselben Tatbestand verwendet (siehe Punkte b und c der obigen Aufzählung).

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 Nr. 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 unbescholtener Personen mit der verfassungsrechtlichen Rechtsprechung im Einklang steht, ist zu bezweifeln[12].

Vom Gesetzgeber ist deshalb zu erwarten, dass der Kreis der Delikte deutlich eingegrenzt wird, bei deren Verfolgung unfreiwillige Kontakt- und Begleitpersonen miterfasst werden. Zugleich erwarten wir eine gesetzliche Präzisierung des Kreises der Kontakt- und Begleitpersonen. Dieser Personenkreis sollte wesentlich enger gefasst und nicht nur durch Abwägungsgebote (wie in den §§ 100f Abs. 2 StPO-E, 100h Abs. 3 StPO-E, 100i Abs. 3 Satz 2 StPO-E, 163e Abs. 1 Satz 3 StPO, 163f Abs. 1 Satz 3 StPO) 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.

---

12 *SächsVerfGH*, LKV 1996, 273 (284 f.).

a) Telekommunikationsüberwachung § 100a StPO-E

Die geplante Regelung in § 100a StPO-E ergänzt in Absatz 1 allgemeine Voraussetzungen, in Absatz 2 wird der Anlasstatenkatalog überarbeitet. Während die Ergänzungen in Absatz 1 in die 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[13], so etwa die Fahnenflucht[14]. 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[15]. Andererseits wiegt die Telekommunikationsüberwachung als Grundrechtseingriff wegen der Erfassung von Kommunikationsinhalten schwerer als die Verbindungsdatenabfrage nach § 100g StPO[16]. 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[17], so ist die im Erweite-

---

13 So die Gesetzesbegründung zur Fahnenflucht und Straftaten gegen NATO-Truppen auf S. 88.

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

15 BVerfGE 109, 279 (344).

16 Vgl. BVerfGE a.a.O. (S. 345).

17 Vgl. Begründung, S. 83.

rungskatalog des Entwurfs erkennbare Rundreise durch das ganze Strafrecht schwer damit zu vereinbaren.

Nach Abs. 1 muss es sich um eine schwere Straftat handeln, die auch im Einzelfall schwer wiegt. Dieses Kriterium ist aufgrund der oben dargestellten notwendigen Differenzierung 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 hinreichend. 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, wir verweisen dazu auf Teil C dieser Stellungnahme.

Die Erhebung von Verkehrsdaten spielt in der Strafverfolgungspraxis seit längerem eine erhebliche Rolle. Sie ist nach der Einschätzung von Experten zu einem fast routinemäßig angewendeten Standardermittlungsinstrument geworden, bei dem die bestehenden gesetzlichen Vorgaben von den Beteiligten überwiegend nur noch in pauschalierter Form geprüft werden. Bisher gibt es aber keine veröffentlichte Statistik zur Anzahl der Auskunftsersuchen 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[18]: nach Auskunft der zuständigen Regulierungsbehörde TP fragten die Strafverfolgungsbehörden in 2003 etwa 2,3 Mio. mal Bestandsdaten ab. Da die Abfrage von Bestandsdaten in der Regel eine TKÜ bzw. Verbindungsdatenabfrage vorbereiten, ist davon auszugehen, dass die Abfrage von Verkehrsdatensätzen in vergleichbarer Höhe stattfand.

---

[18] Stellungnahme des LfD Niedersachsen zur Verfassungsbeschwerdeverfahren 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.

Vor diesem Hintergrund erinnern wir daran, 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[19]. Bis zu diesem Zeitpunkt fand keine Evaluierung statt. Statt dessen wurde die Geltungsdauer durch das Gesetz zur Verlängerung der Geltungsdauer der §§ 100g und 100h StPO vom 09.12.2004 bis zum 31.12.2007 verlängert[20]. 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“[21]. Der Begründung zum vorliegenden Gesetzesentwurf sind keinerlei statistische Zahlenangaben zur Erhebung von Verkehrsdaten zu entnehmen. Ob die für eine Evaluierung notwendige Statistik noch nachgereicht werden kann, erscheint zweifelhaft[22]. 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 Evaluierung erfolgt. Aus rechtspolitischer Sicht erscheint dies angesichts der erheblichen Erweiterung der Zugriffsbefugnisse der Strafverfolgungsbehörden und des damit verbundenen Eingriff 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:[23]

- 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 Gesetzentwurf auf Grund der Entscheidung des Bundesverfassungsgerichts zum niedersächsischen SOG[24] auch für die Telekommunikationsüberwachung eine entsprechende Regelung in § 100a Abs. 4 StPO-E einfügen.

---

19 BGBl. I 2001, S. 3879.

20 BGBl. I 2004, S. 3231.

21 BT-Drs. 15/3971, S. 3.

22 Vgl. Antwort der Bundesregierung auf die Anfrage der Abgeordneten Petra Pau (BT-Prot. 15/131 vom 20.10.2004, S. 11975).

23 Zur allgemeine Berichtspflicht s.u. IV. 6.

24 *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[25]. 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.)[26] Grundsätze für heimliche Datenerhebungen statuiert, die nach nahezu unbestrittener Auffassung der Literatur auch auf andere Rechtsmaterien und Ermittlungsmethoden übertragbar sind[27]. Ausgangspunkt für die dort verlangten Datenerhebungs- und Verwertungsverbote, für Überwachungsabbruch- und Löschungsgebote 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 übersehen die Autoren des Entwurfes, wenn sie sich weigern, die entsprechenden kernbereichsschützenden Vorschriften für alle den Kernbereich möglicherweise verletzenden Ermittlungsmethoden vorzusehen. Sollte der Gesetzgeber bei dieser Auffassung bleiben, verstößt er gegen die Schutzpflicht aus Art. 1 Abs. 1 GG.

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

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 Maßnah-

---

25 S. 45 ff. Ref-E.

26 *BVerfG*, StV 2004, 169 = NJW 2004, 999 = BVerfGE 109, 279.

27 *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 Lisken, Berlin 2004, S. 21 ff.; *Gusy*, JuS 2004, 461; *ders*., Polizeirecht, 6. Aufl., Tübingen 2006, S. 97; *Kötter*, DÖV 2005, 225; *Kugelmann*, 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).

me allein[28] Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden. Für den Fall der (unbeabsichtigten) Erfassung solcher Inhalte ordnet die Vorschrift ein Verwertungsverbot für das Strafverfahren[29] an. Entsprechende Aufzeichnungen sind zu löschen; sowohl Erlangung wie auch Löschung sind aktenkundig zu machen. In Zweifelsfragen[30] hat die Staatsanwaltschaft unverzüglich eine richterliche Entscheidung zur Verwertbarkeit der Erkenntnisse herbeizuführen. Die gerichtliche Entscheidung zur Unverwertbarkeit ist für das weitere Verfahren[31] bindend.

a) Vorgaben des Bundesverfassungsgerichts[32]

Das *Bundesverfassungsgericht* hat in jüngerer Zeit, zuletzt im AWG-Beschluss[33], den Bezug des Telekommunikationsgeheimnisses auf die Menschenwürde mehrfach herausgearbeitet: Bei der (am 21.12.2004 erfolgten[34]) Neuregelung der TKÜ-Befugnisse des Zollkriminalamts seien diejenigen Grundsätze zu beachten, die in den Urteilen vom 14.7.1999[35] und 3.3.2004[36] 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[37]. 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[38].

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 garantierte Unantastbarkeit der Menschenwürde auch im Gewährleistungsbereich des Art. 10 Abs. 1 GG Vorkehrungen zum Schutz individueller Entfaltung im Kernbe-

---

28 Dazu im Einzelnen unten II. 2. b (1).

29 Dazu im Einzelnen unten II. 2. b (2).

30 Dazu im Einzelnen unten II. 2. b (3).

31 Dazu im Einzelnen unten II. 2. b (4).

32 Hierzu schon *Roggan*, StV 2006, 9 ff.

33 *BVerfG*, NJW 2004, 2213 = BVerfGE 110, 33.

34 BGBl. I S. 3603.

35 BVerfGE 100, 313.

36 *BVerfG*, StV 2004, 169 = NJW 2004, 999 = BVerfGE 109, 279.

37 *BVerfG*, NJW 2004, 2213 (2222) = BVerfGE 110, 33 (76).

38 *Gusy* in: Schaar (Hrsg.), Folgerungen aus dem Urteil des Bundesverfassungsgerichts zur akustischen Wohnraumüberwachung, Bonn 2005, S. 51.

reich privater Lebensgestaltung[39]. Wie bei großen Lauschangriffen bedarf es folglich auch im Bereich der Telekommunikationsüberwachung kernbereichsschützender Eingriffsregelungen bzw. der Beachtung der verfassungsgerichtlichen Maßgaben[40].

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[41]. 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 Nachrichtenmittlers – 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“[42], muss grundsätzlich ein Überwachungsverbot gelten. Bei großen Lauschangriffen verlangt das *Bundesverfassungsgericht* „geeignete Vorermittlungen“, die den Charakter der mutmaßlich betroffenen Kommunikationen betreffen[43]. 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[44] der in § 100a StPO genannten Betroffenen in Erfahrung zu bringen hat (Bestandsdaten-Erhebung[45]). Zwar bedeutet dies stets eine Datenerhebung bei Dritten. Im Vergleich zur Gefahr der inhaltlichen Kenntnisnahme von vertraulichen Kontakten ist solcherlei Vorermittlung jedoch vorzugswürdig. Beim Zustandekommen entsprechender Verbindungen gilt die verfassungsgerichtliche Maßgabe, dass schon bei tatsächlichen Anhaltspunk-

---

39 BVerfGE 113, 348 (391 f.) = NJW 2005, 2603 (2612) m. Anm. *Lepsius*, Jura 2006, 929 ff.

40 So etwa *LG Ulm*, StV 2006, 8 f.

41 Vgl. dazu *BVerfG*, StV 2004, 169 (173) = NJW 2004, 999 (1004) = BVerfGE 109, 279 (323).

42 *BVerfG*, StV 2004, 169 (172) = NJW 2004, 999 (1004) = BVerfGE 109, 279 (321).

43 *BVerfG*, StV 2004, 169 (173) = NJW 2004, 999 (1004.) = BVerfGE 109, 279 (323).

44 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 *Weßlau*, in: Roggan (Hrsg.), Lauschen im Rechtsstaat, Berlin 2004, S. 61 ff..

45 Vgl. § 2 Nr. 3 TDSV.

ten 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[46]. Gewiss nicht zufällig rekurriert 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[47]. Von einem solchen Verdachtsgrad sagt das *Bundesverfassungsgericht* an anderer Stelle, dass diese Schwelle niedrig liegt[48]. Für Verbindungen zwischen Vertrauenspersonen gilt folglich eine Vermutung der Zugehörigkeit der entsprechenden Kontakte zum Kernbereich privater Lebensgestaltung[49].

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 Löschungsverpflichtungen anzuordnen. Die bloße Aufzeichnung der Kommunikationen und ihre zeitversetzte Auswertung kommen nicht in Betracht.

(2) Abbruch einer Liveüberwachung bei ungewisser Betroffenheit von kernbereichsrelevanter Kommunikation

Auch in einer *zweiten Kategorie*, bei der Überwachung von Telekommunikationen mit unterstelltem „Sozialbezug“[50], 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. Löschungsverpflichtungen 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.

---

46 *BVerfG*, 1 BvR 668/04 v. 27.7.2005, Abs. 163.

47 Vgl. nur *Meyer-Goßner*, StPO, 48. Aufl., München 2005, § 152 Rdnr. 4.

48 *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.

49 Ebenso *Bergemann* in: Roggan (Hrsg.), Lauschen im Rechtsstaat, Berlin 2004, S. 80.

50 *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. Es ist mit den verfassungsgerichtlichen Maßgaben auch nicht vereinbar, die Unverwertbarkeit auf das weitere Strafverfahren zu begrenzen. Unter dem Gesichtspunkt des verfahrensmäßigen Grundrechtsschutzes ist es unzulänglich, die Herbeiführung einer richterlichen Entscheidung über Zweifelsfragen den Strafverfolgungsbehörden zu überlassen. Schließlich kann eine richterlich festgestellte Unverwertbarkeit der Erkenntnisse nicht auf das „weitere Verfahren" beschränkt sein.

(1) Fehlen einer gesetzlichen Verpflichtung zum Überwachungsabbruch (§ 100a Abs. 4 Satz 1 StPO-E)

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.

Absolut unzulänglich ist allerdings, dass außer für diese idealtypische Konstellation keine weiteren Regelungen zum Kernbereichsschutz vorgenommen wurden. 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 festgeschriebene Verpflichtung, entsprechende – nicht ohne weiteres vorhersehbare – kernbereichsrelevante Gespräche von einer Überwachung auszunehmen.

Eine planmäßige Inkaufnahme des Abhörens von solchen Interaktionen ist mit der Unantastbarkeit des menschenwürdedefinierten Kernbereichs des Telekommunikationsgeheimnisses nicht zu vereinbaren. Vorzusehen wäre vielmehr die gesetzliche Verpflichtung, dass in solchen Konstellationen die Überwachung unverzüglich abzubrechen 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.

Die hier genannten Zweifel werden auch nicht durch die „Zweifelsfalls-Regelung" des § 100a Abs. 4 Satz 5 StPO-E ausgeräumt, denn diese Restriktion erfasst nicht diejenigen Fälle, bei denen die Betroffenheit des Kernbereichs privater Lebensgestaltung für die die Überwachung durchführenden Hilfsbeamten der Staatsanwaltschaft offensichtlich ist, etwa in Fällen der Erfassung von Gesprächen zwischen Eheleuten über Details des Ehelebens. Hier wäre ein unterlassener Überwachungsabbruch eine vorsätzliche Verletzung des Kernbereichs von Art. 10 Abs. 1 GG.

Es überrascht außerdem, 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. Oder anders verstanden: Soll die künftige Überwachung von Telekommunikationen völlig ohne Verpflichtung zum Überwachungsabbruch geregelt werden? Ein noch offenkundigerer Verstoß gegen die verfassungsgerichtlich entwickelte Verpflichtung zur Minimierung des Risikos der Verletzung von unantastbaren Verfassungswerten[51] ließe sich kaum denken.

(2) Fehlende Fernwirkung bei Verstößen gegen Erhebungsverbote

Die vorgesehene Regelung zum Kernbereichsschutz[52] beschränkt die Unverwertbarkeit der Erkenntnisse, die unter Verstoß gegen die Unantastbarkeit des Kernbereichs erzielt wurden, auf „das Strafverfahren" ein. Dies ist mit der Rechtsprechung des *Bundesverfassungsgerichts* aus der Lauschangriff-Entscheidung unvereinbar.

Das *Bundesverfassungsgericht* statuiert für entsprechende Daten ein absolutes und umfassendes Verwertungsverbot: In der genannten Entscheidung heißt es ausdrücklich, dass *jede Ver-*

---

51 BVerfGE 109, 279 (315).

52 Zu den Verwertungsverboten bei übrigen Verfahrensverstößen siehe unten IV. 2.

wendung solcher im Rahmen der Strafverfolgung erhobener absolut geschützter Daten ausgeschlossen ist[53]. Daraus folgt nicht nur die Unverwertbarkeit der Daten im anlassgebenden Zusammenhang, sondern das umfassende und unbedingte Verbot jeglicher Nutzung dieser Daten. Insbesondere kommen sie nicht als sog. Spurenansätze in Betracht. Ausgeschlossen ist überdies die Verwertung zu gefahrenabwehrenden oder anderweitigen sicherheitsbehördlichen (auch: geheimdienstlichen) Zwecken. Mit anderen Worten: Jede anderweitige Nutzung der Daten stellt unausweichlich einen Verfassungsbruch in Gestalt des vorsätzlichen Antastens eines absolut geschützten Bereichs der Privatsphäre dar.

Der Gesetzgeber sollte – schon um Unsicherheiten in der Rechtsanwendung vorzubeugen – die zitierte Formulierung des *Bundesverfassungsgerichts* übernehmen und nicht versuchen, die Grenze des Zulässigen über das verfassungsgerichtlich definierte Maß hinaus auszudehnen.

(3) Unzureichender prozeduraler Grundrechtsschutz (§ 100a Abs. 4 Satz 5 StPO-E)

§ 100a Abs. 4 Satz 5 StPO-E sieht lediglich in Zweifelsfragen die Pflicht zur unverzüglichen Herbeiführung einer richterlichen Entscheidung vor. Hierin liegt eine unzulässige Beschränkung des verfassungsrechtlich gebotenen prozeduralen Grundrechtsschutzes.

Nach dem Wortlaut der Vorschrift müssen die Strafverfolgungsbehörden erst dann eine richterlichen Entscheidung über die Verwertbarkeit bereits erhobener und gespeicherter Daten herbeiführen, wenn sie selbst Bedenken hinsichtlich des Kernbereichsbezuges haben. Die richterliche Entscheidung kann dann zur Absicherung bisheriger Beweisergebnisse führen, sie kann aber auch umgekehrt die Verwertung für die weitere Ermittlungstätigkeit verbieten. So laufen die Strafverfolgungsbehörden Gefahr, dass gespeicherte Daten, deren unmittelbare Verwertbarkeit aufgrund einer richterlich festgestellten Kernbereichsverletzung ausscheidet, auch als Spurenansatz nicht mehr genutzt werden können. Von daher ist es naheliegend, dass die Herbeiführung einer solchen richterlichen Entscheidung eher selten, zumindest aber möglichst spät vorgenommen wird.

Deshalb hat auch das *Bundesverfassungsgericht* in der Entscheidung zum Lauschangriff deutliche Zweifel anklingen lassen, ob die Entscheidung über die Verwertbarkeit von bereits erlangten Informationen bei den Strafverfolgungsbehörden in den richtigen Händen liegt.

Wegen dieser Gefahr, dass die Strafverfolgungsbehörden den Ermittlungsrichter in Fragen der Verwertbarkeit umgehen, hat das *Bundesverfassungsgericht* in der Entscheidung zum Lauschangriff[54] – ohne dass eine Beschränkung auf eben diese Ermittlungsmethode erkennbar wäre – die Voraussetzungen für eine verfassungsgemäße Regelung statuiert: Bei einer den Kernbereich privater Lebensgestaltung „verletzungsgeneigten" Ermittlungsmethode kann die Verwendung der erhobenen Erkenntnisse nur dann zulässig sein, wenn deren Verwertbarkeit

---

53 BVerfGE 109, 279 (319).

54 BVerfGE 109, 279 (334).

vor der Hauptverhandlung von einer unabhängigen Stelle überprüft worden ist. Am vorliegenden Gesetzentwurf ist somit zu beanstanden, dass die letztliche Verwertbarkeit in der strafgerichtlichen Hauptverhandlung nicht unter den generellen Vorbehalt einer ermittlungsbehörden-unabhängigen Kontrolle gestellt wurde. Die vorliegende Regelung errichtet im Ermittlungsverfahren eine – verfahrensmäßig unzulängliche – „Verwertbarkeitsschwelle" und überlässt die endgültige Verwertbarkeitsentscheidung dem Tatrichter. Eine ausreichende verfahrensrechtliche Sicherung dagegen setzt eine Regelung voraus, die die Strafverfolgungsbehörden verpflichtet, **alle** aus verdeckten Beweiserhebungsmaßnahmen stammenden Erkenntnisse, die der Anklage zugrunde gelegt werden, von einem Ermittlungsrichter auf ihre Verwertbarkeit hin überprüfen zu lassen.

(4) Fehlende Absolutheit der Unverwertbarkeit bei richterlicher Feststellung (§ 100a Abs. 4 Satz 6 StPO-E)

§ 100a Abs. 4 Satz 6 StPO-E erklärt die ermittlungsrichterliche Entscheidung über die Unverwertbarkeit bereits erhobener und gespeicherter Daten nur für das „weitere Verfahren" für verbindlich. Hiergegen sind die oben bereits genannten Zweifel zum fehlenden absoluten und umfassenden Nutzungsverbot zu übertragen: Auch insoweit sollte das Gesetz jegliche Verwendung im Strafverfahren und für alle anderen sicherheitsbehördlichen Belange ausdrücklich ausschließen.

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[55].

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

Der Entwurf knüpft an das in § 53 StPO geregelte Zeugnisverweigerungsrecht und unterscheidet 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

---

[55] Vgl. dazu die Beiträge in *Wolter/Schenke* (Hrsg.), Zeugnisverweigerungsrechte bei (verdeckten) Ermittlungsmaßnahmen, Berlin 2002.

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.

Dasselbe gilt für die Zeugnisverweigerungsrechte aus persönlichen Gründen nach § 52. 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[56]. § 53b Abs. 1 sollte sich daher – unter vollständiger Streichung des Abs. 2 – auf alle in §§ 52, 53 genannte Person beziehen.

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

Keineswegs hinnehmbar 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 er mittels einer vagen Generalklausel die Grenzziehung im einzelnen dem Ermessen der Verwaltung überlässt."[57]

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[58], dass ein Verstoß gegen die gesetzlichen Bestimmungen die Verwendung der erzielten Erkenntnisse in jeder Weise unzulässig macht[59] und dass bei der Berührung von Zeugnisverweigerungsrechten die Freigabe erzielter Erkenntnisse für jede Art der Verwendung durch ein Gericht erfolgen muss.

---

56 BVerfGE 109, 279 (328 ff.).

57 *BVerfG*, NJW 57, 297 ff; BVerwG, NJW 55, 1693.

58 Siehe oben II.

59 Siehe unten IV. 2.

Das zugrundeliegende Regelungskonzept mit der im Einzelfall vorzunehmenden Verhältnismäßigkeitsprüfung erscheint schließlich für die Praxis schwer handhabbar, insbesondere wenn man berücksichtigt – wie auch in der Begründung[60] 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[61], 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 Berufsgeheimnisträger bereits dann, wenn lediglich ein einfacher Anfangsverdacht der Tatbeteiligung gegen den Berufsgeheimnisträger vorliegt. Gem. § 152 Abs. 2 StPO genügen hierfür zureichende tatsächliche Anhaltspunkte. Diese Schwelle des Anfangsverdachts liegt niedrig[62]. 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 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. 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.

---

60 Siehe Begründung Ref-E., S. 78/79.

61 BT-Drs. 16/956; BT-Drs. 16/576 sowie BR-Drs. 650/06.

62 *BVerfG*, wistra 2002, 135 (136).

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[63]. So konstatiert die Untersuchung von Backes und Gusy eine Erosion des Richtervorbehaltes und den „weitgehenden Verzicht der Richter selbst, die ihnen vom Gesetz aufgegebene eigenständige und grundrechtsorientierte Prüfung der staatsanwaltschaftlichen Anträge auf Telefonüberwachung vorzunehmen" [64].

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."[65] Diese Begründung ist nicht nachzuvollziehen. Es besteht kein logischer Zusammenhang zwischen den materiellen Anforderungen 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.

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 Aufweichung 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.

---

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

64 *Backes/Gusy* u.a., StV 2003, 249 (252).

65 Siehe Begründung Ref-E, S. 99.

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

Wie die Studien des MPI und der Universität Bielefeld gezeigt haben[66], 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[67] und generell unzureichender Sicherung der Grundrechte im Rahmen von Ermittlungsmaßnahmen[68].

Das allein erfolgversprechende 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[69]. Solange verdeckt tätige Ermittlungsbehörden darauf hoffen können, gewonnene Erkenntnisse (auch, aber nicht nur personenbezogene Daten) nutzen zu können, werden möglicherweise die Grenzen der Befugnisse weitestmöglich – 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 Recht des Beschuldigten auf ein faires, rechtsstaatliches Verfahren beeinträchtigen, weil die aufgrund von Erhebungs- und Verwertungsverboten nicht erlangten Erkenntnisse nicht nur der Anklage sondern auch der Verteidigung entzogen sind.“[70] 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 Eingriffsmaßnahmen 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 unziemlicher Weise: Nach § 136a Abs. 3 StPO gibt es schon immer ein absolutes Verwertungsverbot, wenn die Freiheit der Willensentschließung und der Willensbetäti-

---

66 Siehe oben Fn. 1 und 2.

67 Jüngst *BVerfG*, NJW 2006, 3411 f.

68 Vgl. statt vieler etwa zur Wohnungsdurchsuchung BVerfGE 103, 142; zur DNA-Analyse BVerfGE 103, 21.

69 So auch schon *Hirsch*, Ausufernde Telefonüberwachung im Strafverfahren, in: Grundrechte-Report 1998, Seite 131 ff. und *Müller-Heidelberg*, Deutschlands Überwachungskultur, in Grundrechte-Report 2004, S. 101 ff.

gung 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.

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 (Verkehrsdatener-

---

[70] Begründung Ref-E., S. 53

hebung), ebenso bei der diesem Bereich zumindest nahe liegende 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[71]. 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.

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.

---

[71] BVerfGE 109, 279 (366)

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 vorgeschlagen 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 bereichspezifischen 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, be-

legt die MPI-Studie[72], 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[73]. 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.

Die in den Absätzen 5 und 6 zur Diskussion gestellten weiteren Angaben, die im Falle der akustischen Wohnraumüberwachung in § 100e Abs. 2 Nr. 9-11 StPO bereits geltendes Recht sind, sind für eine sachgerechte Erfolgskontrolle unverzichtbar. Es kann nicht Aufgabe von Gutachtern – etwa der MPI-Studie – 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 in Nr. 5 und 6 genannten Angaben zur Verfügung stehen. Dass in der Begründung angeführte Gegen-Argument des zusätzlichen Aufwandes[74] überzeugt jedenfalls nicht.

---

72 Siehe oben Fn. 1.

73 A.a.O., S. 444.

74 Begründung Ref-E., S. 105, 2. Anstrich.

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[75]. 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[76]. 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 03. 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[77]. Die Bundesregierung erklärte ihrerseits, dieser Forderung folgen zu wollen.

---

75 Ratsdokument 8958/04.

76 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.

77 BT-Drs. 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-Drs. 15/3773, BT-Drs. 15/4748; BT-Drs. 15/4597; BT-Drs. 16/128; BT-Drs. 16/237; BT-Drs. 16/545, BT-Drs. 16/690, BT-Drs. 16/1622; BR-Drs. 275/02; BR-Drs. 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 Speicherungsdauer 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[78]. 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[79].

---

[78] *EuGH*, Urteil vom 5. Oktober 2000, Rs. C-376/98, Deutschland/EP und Rat („Tabakwerbeverbotsrichtlinie"), Slg. 2000, I-8419, Rn. 86.

[79] *Streinz*, Europarecht, 7. Aufl., Heidelberg 2005, S. 361.

Ziel und der Inhalt der Vorratsdatenspeicherungsrichtlinie betreffen aber in erster Linie die Vorsorge zur Strafverfolgung[80]. Die Angleichung nationaler Rechtsvorschriften zwecks Verbesserung des Binnenmarktes kann bei der Vorratsdatenspeicherung, wenn überhaupt, lediglich als sekundärer Zweck bezeichnet werden[81]. 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[82]. 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 gestützte Richtlinie mangels Rechtsgrundlage für nichtig[83].

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[84]. 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 Op-

---

80 Vgl. Art. 1 Abs. 1 sowie Erwägungsgründe Nr. 7 und 21 RL2006/24/EG.

81 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.

82 EuGH, Rs. C-301/06.

83 EuGH, Urteil vom 30. Mai 2006, Rs. C 317/04 und C-318/04, EP/Rat = NJW 2006, S. 2029f.

84 Vgl. *EuG*H, Rs. 136/79, „National Panasonic“, Slg. 1980, S. 2033; EuGH, Rs. 46/87 und 227/88, “Hoechst”, Slg. 1989, 2859f.

position 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 Umsetzungsgesetz dann wieder zurückzunehmen wäre, ist erheblich. Eine u.U. verzögerte Umsetzung ist deshalb unter dem Gesichtspunkt der Verhältnismäßigkeit hinzunehmen“[85]. Die Bundesregierung wird außerdem aufgefordert, während der EU-Ratspräsidentschaft auf die Rücknahme der Richtlinie zur Vorratsdatenspeicherung hinzuwirken bzw. 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[86]. 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 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[87]. Da den zugreifenden Strafverfolgungsbehörden keine Schranken bei der Auswertung dieser Daten auferlegt sind, wird die Erstellung von Kommunikations- und Bewegungsprofilen aller 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 Datenschutzrechts (Datensparsamkeit, Zweckbindungsgebot, hohe Anforderungen bei der

---

85 BT-Drs. 16/1622, S. 6.

86 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, §§ 8 Abs. 8 und 9 Abs. 4 BVerfSchG, § 10 Abs. 3 MADG, § 8 Abs. 3a BNDG, §§ 3, 5 und 8 G10.

Anwendung des Verhältnismäßigkeitsgrundsatzes) und schränkt das Grundrecht auf Fernmeldegeheimnis und auf informationelle Selbstbestimmung unverhältnismäßig ein. Insbesondere mit der vorgesehenen Verwendung der gespeicherten Daten für die Verfolgung mittelschwerer und mittels Telekommunikationseinrichtungen begangener Straftaten (vgl. § 100g Abs. 1 StPO-E) 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[88]. „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“[89].

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[90].

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[91]. 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 Kommunikationsge-

---

87 Vgl. Pressemitteilung des BMJ vom 8. November 2006.

88 BVerfGE 67, 157 (172).

89 *BVerfG*, NJW 2006, 976 (978). Vgl. auch BVerfGE 107, 299 (320); 113, 348 (365).

90 BVerfGE 100, 313 (359).

91 BVerfGE 107, 299 (313).

heimnis mit der gesetzlich angeordneten Verpflichtung der Anbieter öffentlicher Telekommunikationsdienste, fast alle anfallenden Verbindungsdaten für 6 Monate zu speichern (vgl. § 110a Abs. 2 TKG-E). Die Tatsache, dass die Erhebung und Speicherung der Daten durch die Telekommunikationsunternehmen erfolgt, 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[92]. 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 (§ 110b Abs. 1 TKG-E). Aufgrund der in den §§ 100g, 100a StPO-E vorgesehenen Normen können sich dann 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[93]. 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 späterer Strafverfolgung sicherstellen[94].

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

---

92 Vgl. BVerfGE 107, 299 (313).

93 Vgl. BVerfGE 113, 348 (365).

94 Vgl. Begründung Ref-E., S. 147.

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 allen Benutzerinnen und Benutzern elektronischer Telekommunikationsmittel unterstellt, sie könnten in der Zukunft zum Objekt staatlicher Strafverfolgung werden. Dieser generelle Verdacht 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 bestimmbaren Zwecken wäre damit unvereinbar“[95]. Das Bundesverfassungsgericht hat ausdrücklich festgestellt, dass das Grundgesetz eine „globale und pauschale Überwachung“ zu Zwecken der Auslandsaufklärung nicht zulässt[96]. Es leuchtet wenig ein, warum dies bei der Strafverfolgungsvorsorge anders sein soll. Die allgemeine Zweckbestimmung des Gesetzentwurfs, die Speicherung der Verbindungsdaten diene der Strafverfolgung, genügt vor diesem Hintergrund nicht den verfassungsrechtlichen Anforderungen[97].

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 Kommunikationsmittel – wie Internetcafés, Straßentelefonzellen, Mailkonten außerhalb der EU und den USA oder vorausbezahlte international einsetzbare SIM-Karten – zurückgrei-

95 BVerfGE 100, 313 (360).
96 BVerfGE 100, 313 (376).
97 BVerfGE 107, 299 (321).

fen[98]. Darüber hinaus muss auch die Möglichkeit berücksichtigt werden, Anonymisierungsdienste einzusetzen. Beide 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, die eigentliche „Zielgruppe" der Maßnahme wird sich ihr entziehen. Wenn die vorhandenen Verbindungsdaten keiner Person eindeutig zugeordnet werden können, dann ist ihre Verwertbarkeit bei einer strafrechtlichen Ermittlung 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[99].

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[100].

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 milderes Mittel zur Verfügung, durch das die Ziele des Gesetzgebers weitgehend zu erreichen wären[101]. 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 einen Zugriff auf in der Vergangenheit angefallene Daten ist das

---

98 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.

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

100 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).

101 Zum sogenannten „Quick-freeze-Verfahren" vgl. *Büllingen*, DuD 2005, S. 349 (350).

„Data Preservation"-Verfahren nutzlos und nicht im gleichen Maße förderlich wie die generelle Vorratsdatenspeicherung[102].

Trotzdem ist zu bemerken, dass erhebliche Zweifel an der Notwendigkeit der Speicherungsdauer von sechs Monaten bestehen. Erfahrungsgemäß betreffen die Zugriffe der berechtigten Behörden in ähnlichen Konstellationen fast ausschließlich die ersten drei Monate der Speicherung[103]. 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 Speicherungsvorgang – 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"[104].

Die Regelungen des Gesetzentwurfes stehen damit im Gegensatz zu wichtigen verfassungsrechtlichen Grundsätzen des Datenschutzes[105]. 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

---

[102] In diesem Sinne auch die Begründung zum Gesetzentwurf, S. 67: „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".

[103] Vgl. dazu *Westphal*, EuZW 2006, S. 555 (558).

[104] *Humanistische Union*, Stellungnahme vom 12.12.2005, S. 6.

[105] BVerfGE, 65, 1 (44, 46).

„kein belangloses Datum“[106] 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“[107]. Dass dies durch den vorgestellten Gesetzentwurf geschieht, ist nicht ersichtlich.

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

In § 110a Abs. 1 Satz 1 TKG-E wird der Kreis der zur Speicherung Verpflichteten festgelegt. Danach sind zur Speicherung diejenigen verpflichtet, die Telekommunikationsdienste für die Öffentlichkeit erbringen oder an der Erbringung solcher Dienste mitwirken. Gespeichert werden müssen nur Verkehrsdaten, die vom jeweiligen Dienstanbieter bei der Nutzung seines Dienstes erzeugt oder verarbeitet werden. Die Pflicht besteht auch dann, wenn ein Anbieter Telekommunikationsdienste erbringt, ohne eine eigene Telekommunikationsanlage zu betreiben (§ 110a 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 einem „Mitwirken“ bei der Erbringung eines Telekommunikationsdienstes ausgegangen werden kann oder ab welcher Stufe 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 oder daran mitwirkt und dementsprechend Normadressat des §100g StPO wäre[108]. Vergleichbare Streitfälle werden mit dem Gesetzentwurf nicht beseitigt, sondern eher noch verstärkt.

Ähnlich problematisch ist der maßgebliche Bezug der Adressaten auf die „Öffentlichkeit“ im Sinne des § 110a Abs. 1 S. 1 TKG-E. Leider trägt auch die Begründung nicht zur Klärung des Adressatenkreises bei: Demnach bestünde für „den nicht öffentlichen Bereich (z.B. unternehmensinterne Netze, Nebenstellenanlagen oder E-Mail-Server von Universitäten ausschließlich für dort immatrikulierte Studierende oder Bedienstete sowie die Telematikinfrastruktur im Gesundheitswesen)“[109] keine Speicherungspflicht. Auch die

---

106 BVerfGE, 65, 1 (45).

107 BVerfGE 2 BvR 1345/03 („IMSI-Catcher“), Rn. 84.

108 Vgl. *Fraenkel/Hammer*, DuD 2006, S. 499f.

109 Begründung Ref.-E., S. 1146.

Begriffsbestimmungen des § 3 TKG helfen nicht bei der Auslegung des Tatbestands „Öffentlichkeit“, weil dort keine Definitionen von „Öffentlichkeit“ oder „öffentlichen Telekommunikationsnetzen“ enthalten sind. Eine gesetzliche Klärung des Begriffs der „Öffentlichkeit“ erscheint aus Gründen der Rechtssicherheit dringend geboten.

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[110]. Welche anderen Leistungen noch unter dem Begriff des „Verarbeitens“ in Zusammenhang mit der Vorratsdatenspeicherung zu subsumieren wären, ist offen. Ähnliches gilt für das Merkmal des „Mitwirkens“: Die im Schrifttum verbreitete Ansicht, dass als „Mitwirkende“ alle zu behandeln sind, die an einer Nachrichtenübermittlung in irgendeiner Form beteiligt sind, trägt zu einer effektiven Rechtsanwendung kaum bei[111].

Zu bemerken ist außerdem, dass die geplante Regelung keine Begrenzung der Speicherungspflicht auf solche Betreiber vorsieht, die Telekommunikationsdienste geschäftsmäßig erbringen oder daran mitwirken. Dabei 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) Quasi-Verbot der Anonymisierungsdienste

Das Gesetz regelt auch den Status derjenigen, die so genannte Anonymisierungsdienste betreiben und anbieten. 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[112]. Bezüglich dieser Anonymisierungsdienste wird in der Begründung zum Gesetzesentwurf ausgeführt: „Einen Telekommunikationsdienst für die Öffentlichkeit im Sinne des § 110a Abs. 1 TKG-E erbringt auch, wer einen Anonymisierungsdienst betreibt und hierbei die Ausgangskennung des Telekommunikationsnutzers durch eine andere ersetzt“[113]. Wenn aber die Anbieter von Internetanonymisierungsdiensten die entsprechenden in § 110a

---

110 Begründung Ref.-E., S. 147.

111 Vgl. *Säcker* in: ders. (Hrsg.), Berliner Kommentar zum Telekommunikationsgesetz, Frankfurt am Main 2006, § 3, Rn. 9.

112 Vgl. *Spindler/ Schmitz/Geis*, TDG-Kommentar, München 2004, S. 292f.

113 Begründung Ref.-E., S. 146.

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. Der Gesetzentwurf läuft praktisch auf ein Verbot der Anonymisierungsdienste hinaus.

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.[114] Insoweit geht die Verpflichtung zur Vorratsdatenspeicherung für die Anbieter solcher Dienste über die Anforderungen der Richtlinie hinaus. Zudem widerspricht der Entwurf der geltenden Rechtslage, wonach die Anbieter von Telediensten verpflichtet sind, den Nutzern die Inanspruchnahme sowie die Bezahlung von Telediensten anonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist (vgl. § 4 Abs. 6 TDDSG).

dd) Katalog der zu speichernden Daten (§ 110a 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 (§ 110a 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[115]. 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 jeweiligen Dienstes (bei vorausbezahlten Diensten wie beispielsweise Prepaid-SIM-Karten oder Flatrate-Tarifen für den Internetzugang) (§ 110a Abs. 2 Nr. 4 d) TKG-E); die Pflicht zur Speicherung erfolgloser Anrufsversuche (Art. 3 Abs. 2 RL, § 110a Abs. 5 TKG-E)[116]; die Erhebung von Daten in Echtzeit (§ 100g Abs. 1 S. 3 StPO-E); die Angaben über die Hauptstrahlrichtung der Funkantennen beim Mobilfunk (§ 110a Abs. 6 TKG-E); das praktische Verbot von anonymen E-Mail-Konten (111 TKG-E)[117]. Bei all diesen Da-

---

[114] Die Zuordnung der Anonymisierungsdienste zu den Telediensten ist dadurch begründet, dass bei ihnen die Umschreibung der IP-Adressen auf der Anwendungsebene, nicht auf der Ebene des Transportprotokolls stattfindet.

[115] Vgl. BT-Drs. 16/545, S. 4.

[116] 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 absichtlich einen Kommunikationsvorgang ablehnt und z. B. nicht ans Telefon geht. Dass dies das Risiko stark erhöht, in unbegründeten Verdacht zu geraten, liegt auf der Hand.

[117] § 111 Abs. 1 S. 3 TKG-E verpflichtet die Anbieter von E-Mail-Diensten zur Erfassung von Daten wie Name, Anschrift, Geburtsdatum und Kennung des elektronischen Postfachs. Dies bedeutet, dass die anonyme Eröffnung eines E-Mail-Kontos bei einem deutschen Anbieter künftig nicht mehr möglich wäre. Es ist allerdings fraglich, ob die anonyme Bereitstellung von Telekommunikationsdiensten nach der Vorratsspeicherungsrichtlinie generell verboten werden soll. Einerseits sollen die aufgelisteten Daten gespeichert werden, nur soweit sie im Zuge der Bereitstellung von Kommunikationsdiensten erzeugt und verarbeitet werden

ten 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 (§ 110a Abs. 2 Nr. 1 TKG-E) wird die bisherige, umstrittene „Zielwahlsuche“ (§ 100g Abs. 2 StPO) entbehrlich. Für jedes Benutzerkonto werden künftig nicht nur alle ausgehenden, sondern auch alle ankommenden Verbindungen gespeichert. Die doppelte Speicherung aller Verbindungsdaten bei Sender und Empfänger zeigt einmal mehr, wie umfassend die künftige Vorratsdatenspeicherung von Verkehrsdaten ist und mit welcher Intensität sie in die Grundrechte eingreift[118].

Nach § 110a 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[119]. 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[120]. Damit würde das eingeschaltete Mobiltelefon „zu einer Art ungewolltem Peilsender“[121], der die Bewegung seines Nutzers meldet. Somit wird auch die aus verfassungsrechtlicher Sicht äußerst bedenkliche Ermittlungsmethode des sogenannten „stillen SMS“ de facto legalisiert[122].

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

---

(Art. 3 Abs. 2 RL 2006/24/EG). Vgl. aber andererseits die Regelungen von Art. 5 Abs. 1 a) 2. iii) RL 2006/24/EG, wonach die Anschrift und der Name des Teilnehmers bzw. registrierten Benutzers zu speichern sind und Art. 5 Abs. 1 e) 2. vi) RL 2006/24/EG, wonach „im Falle vorbezahlter anonymer Dienste Datum und Uhrzeit der ersten Aktivierung des Dienstes und die Kennung des Standorts (Sell-ID), an dem der Dienst aktiviert wurde“ zu speichern sind. In Deutschland besteht seit 2004 eine Identifizierungspflicht auch beim Erwerb von Prepaid-SIM-Karten (vgl. § 111 TKG). Was passiert aber, wenn bei der privaten Bereitstellung von Diensten (etwa: WLAN-Zugang) einige der geforderten Verbindungsdaten gerätebedingt nicht für die erforderliche Dauer gespeichert werden können?

118 Die Ausführungen in der Begründung des Gesetzentwurfs, wonach die Zielwahlsuche lediglich „entfällt“ (Begründung Ref.-E., S. 116), sind hier irreführend.

119 Um eine genauere Ermittlung des Standortes eines Mobiltelefons zu ermöglichen, verpflichtet § 110a Abs. 6 TKG-E die Anbieter zur Angabe der geografischen Lage der jeweiligen Funkzelle sowie der Hauptstrahlrichtung der Funkantennen.

120 Begründung Ref.-E., S. 112.

121 Zöller, CILIP 85 (3/2006), S. 21 (26).

122 Begründung Ref.-E., S. 112.

Kommunikation geben[123]. 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[124]. Zum anderen können auf Grund einer umfangreichen Sammlung von Verkehrs-, Standort- und Bestandsdaten Kommunikationsinhalte durchaus nachgebildet werden. Nach § 110a 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 Nutzerin / der Nutzer in Anspruch genommen hat – die Verbindungsdaten damit Rückschlüsse auf die Inhalte der Verbindung zulassen[125].

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[126]. Indem Verkehrsdaten in digitalisierter, standardisierter Form erfasst werden, bestehen für sie ungleich mehr Möglichkeiten ihrer (automatisierten) Auswertung und Verarbeitung als bei Inhaltsdaten[127]. 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 einzustufen, weil es sich dabei „nur" um Verkehrsdaten handele, in ihrer Pauschalität irreführend[128].

Nach alledem ist festzuhalten, dass die Pflicht zur Speicherung und Aufbewahrung der in § 110a Abs. 2 bis 5 TKG-E aufgelisteten Daten zu einer sehr umfangreichen Sammlung von

---

123 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.

124 Vgl. www.heise.de/ct/hintergrund/meldung/69995.

125 Vgl. www.heise.de/newsticker/meldung/83054.

126 BVerfGE 65, 1 (45).

127 *Breyer*, Die systematische Aufzeichnung und Vorhaltung von Telekommunikations-Verkehrsdaten für staatliche Zwecke in Deutschland, Berlin 2005, S. 212.

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 verstoßen daher gegen den Verhältnismäßigkeitsgrundsatz.

ee) Missbrauchsgefahr durch Private

Die massenhafte Speicherung von Verkehrs- und Standortdaten erhöht das Risiko eines Datenmissbrauchs[129]. 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 § 110b Abs. 3 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 Telekommunikationsdienstanbieter. Für die Benutzerinnen und Benutzer der Dienste bleibt das Risiko eines unberechtigten Zugriffs durch die Mitarbeiter der Telekommunikationsunternehmen bestehen[130]. Die Tatsache, dass die Speicherung automatisch, also ohne jede Kenntnisnahme durch Personen erfolgen soll, kann dieses Risiko nicht mindern[131]. 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 solcher Daten an andere Unternehmen. Die sogenannte „Telefonüberwachungsaffäre", die im letzten Jahr in Italien für Schlagzeilen sorgte, ist ein weiteres markantes Beispiel solche 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

---

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

129 Vgl. *ULD Schleswig-Holstein*, Stellungnahme vom 04.10.2006, S. 4.

130 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.

131 Die entsprechende Bemerkung in der Begründung zum Gesetzesentwurf steht in einem gewissen Widerspruch zur Verpflichtung zu Sicherungsmaßnahmen in § 110b Abs. 3 S. 2 TKG-E. Vgl. Begründung Ref.-E., S. 69.

vorgesehen nutzen würden[132]. Auf diese Weise könnte die Vorratsdatenspeicherung zu kontraproduktiven Effekten bei der Verbrechensbekämpfung führen, weil sie das Begehen bestimmter Straftaten erleichtern würde[133]. Ein wirksames präventives Datenschutzmanagement erscheint daher im behandelten Zusammenhang zwingend geboten. Der Gesetzesentwurf enthält allerdings keine Vorkehrungen, die dieses gewährleisten können[134].

e) Zwischenergebnis für die erste Stufe

Die durch das Umsetzungsgesetz vorgesehene Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten stellt wegen der Erfassung umfangreicher Telekommunikationsdaten einer Vielzahl von Personen ohne jeglichen Verdacht generell 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 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.

---

[132] Vgl. für entsprechende Beispiele *Breyer*, Die systematische Aufzeichnung und Vorhaltung von Telekommunikations-Verkehrsdaten für staatliche Zwecke in Deutschland, Berlin 2005, S. 231.

[133] 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 Telekommunikationsdienstanbieter zum Schutz des Fernmeldegeheimnisses verpflichtet sind). Mit dem vorgelegten Gesetzesentwurf wird aber dieser Schutzpflicht keinesfalls Genüge getan.

[134] So auch das *ULD Schleswig-Holstein*, Stellungnahme vom 04.10.2006, S. 4.

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[135].

a) 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 festgelegt, was unter „schwere Straftaten" zu verstehen ist[136]. Auch zur Frage, ob die Daten für weitere Zwecke verwendet werden dürfen, verhält sich die Richtlinie nicht. Den EU-Mitgliedsstaaten stehen daher erhebliche 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 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. Zu bemerken ist außerdem, dass in der entsprechenden Norm des § 110b Abs. 1 TKG-E lediglich von „Verfolgung von Straftaten" die Rede ist.

Dabei ist zunächst fraglich, was unter „Straftat von erheblicher Bedeutung" zu verstehen ist, was im Zusammenhang mit dem Bestimmtheitserfordernis im Rahmen des Art. 10 Abs. 1 GG von besonderer Bedeutung ist. 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. Bezüglich der Tatbestandsvoraussetzung der „Straftat von erheblicher Bedeutung" in § 100g Abs. 1 Nr. 1 StPO-E erscheint es zweifelhaft, ob diese hinreichend bestimmt ist[137]. Die Begründung zum Gesetzesentwurf

---

135 Vgl. BVerfGE 100, 313 (376); 107, 299 (320); 113, 348 (282).

136 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.

137 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

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[138]. 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 geboten, die betreffenden Straftaten in einem enger verfassten abschließenden Katalog aufzulisten[139]. Der Gesetzesentwurf geht auch in diesem Punkt über die europarechtlichen Vorgaben hinaus (Art. 1 Abs. 1 Richtlinie 2006/24/EG).

Es ist außerdem fragwürdig, ob der generelle Verweis auf den 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, dass die Subsidiaritätsklausel des § 100g Abs. 1 S. 2 StPO-E nur die Kategorie der mittels Telekommunikation 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 wäre und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht.

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 über die Vorgaben der Richtlinie hinaus (vgl. Art. 1 Abs. 1 RL). Dies widerspricht dem vom Bundesverfassungsgericht entwickelten Grundsatz der möglichst grundrechtsschonenden Umsetzung von EG-Richtlinien[140].

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.

b) Unzureichende Differenzierung bezüglich der Kontaktpersonen (Nachrichtenmittler)

2006, S. 159f. Das Bundesverfassungsgericht hat allerdings den Begriff im Hinblick auf § 110g StPO als hinreichend bestimmt angesehen (BVerfGE 107, 299, 322).

138 Begründung Ref.-E., S. 84.

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

140 Vgl. *BVerfG*, NJW 2005, S. 2289 („Europäisches Haftbefehlsgesetz").

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.

Auch diese Regelung erscheint angesichts der Intensität des Grundrechtseingriffs, den sie herbeiführt, nicht ausreichend bestimmt. Es fehlt ein handhabbarer Maßstab für die Prüfung, beim Vorliegen welcher konkreter Tatsachen eine Unterstützung des Beschuldigten durch eine Drittperson mittels Kommunikationsmittel anzunehmen ist. Eine restriktive Auslegung könnte das Bestimmtheitsdefizit nicht beseitigen.

c) Die zugriffsberechtigten Behörden

Die Vorratsdatenspeicherungsrichtlinie eröffnet den Mitgliedsstaaten breite Ermessensspielräume, was die Bestimmung der zugriffsberechtigten Behörden und der Zugriffsvoraussetzungen und -verfahren betrifft (vgl. Art. 11 RL 2006/24/EG i.V.m. Art. 15 Abs. 1 der Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG).

Der Gesetzentwurf sieht dementsprechend grundlegende Änderungen bezüglich 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[141]. *So würde es Ihnen künftig ermöglicht, selbst und in Echtzeit Verkehrsdaten sowie Standortdaten zu erheben und zu verwerten*. Die Auskunftsverpflichtung der Dienstanbieter bleibt davon unberührt[142]. Dies ist ein tiefgehender Eingriff in das Grundrecht auf vertrauliche Telekommunikation, für dessen Rechtfertigung keine Gründe ersichtlich sind.

Bei der Bewertung der geplanten Regelungen über den staatlichen Zugriff auf die vorrätig gespeicherten Daten ist weiterhin von Bedeutung, ob den Nachrichtendiensten dieser Zugriff erlaubt wird. Nach der geltenden Rechtslage dürfen nicht nur die Strafverfolgungsbehörden, sondern auch die Nachrichtendienste sowie die Verfassungsschutzämter auf bestimmte Verkehrsdaten zugreifen[143]. Nach der Begründung zum Gesetzesentwurf soll eine Übermittlung der aufgrund des § 110a TKG-E gespeicherten Vorratsdaten für andere Zwecke als zur Verfolgung von Straftaten gemäß § 110b Abs. 1 S. 1 TKG-E nicht zulässig sein. Damit sei – so

---

141 Begründung Ref.-E., S. 109.

142 § 100g Abs. 2 S. 1 StPO-E i.V.m. § 100b Abs. 3 StPO-E

143 vgl. § 100g StPO, § 3 Nr. 3 TKG, §§ 112, 113 TKG, § 8 Abs. 8 BVerfSchG, § 8 Abs. 3a BNDG, § 10 Abs. 3 MADG

die Begründung – „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[144]. Dies wird auch durch die Vorschrift des § 110b Abs. 1 S. 3 TKG-E betont. Das darin enthaltene umfassende Übermittlungsverbot ist positiv zu bewerten[145]. Wäre es beispielsweise auch den Nachrichtendiensten erlaubt, auf alle vorrätig gespeicherten Daten zuzugreifen, wäre dies wegen der diesbezüglichen geringen Rechtsschutzmöglichkeiten der Betroffenen mit dem Grundgesetz nicht vereinbar.

Bedenken bestehen aber hinsichtlich des staatlichen Zugriffs auf die dynamischen IP-Adressen im Internetbereich. 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 Auskunftsersuchen bezüglich statischer IP-Adressen einschlägig, weil diese Adressen als Bestandsdaten im Sinne von § 3 Nr. 3 TKG anzusehen sind[146]. Dementsprechend dürfen derzeit Auskunftsersuchen bezüglich dynamischen IP-Adressen nach Maßgabe der §§ 100g und 100h StPO angeordnet werden. Die relevante Rechtsprechung ist allerdings uneinheitlich[147]. Eine gesetzliche Klarstellung erscheint daher notwendig. Richtigerweise stellen die dynamischen IP-Adressen aber Verkehrsdaten dar, u.a. weil sie in keinem unmittelbaren Zusammenhang mit dem jeweiligen Vertragsverhältnis stehen.

d) Zu niedrige Eingriffsschwelle

Für den Zugriff auf die von den Telekommunikationsanbietern gespeicherten Daten ist lediglich ein Anfangsverdacht vorgesehen (§ 100g Abs. 1 S. 1 StPO-E). Die Praxis hat gezeigt, 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 unan-

---

144 Begründung Ref.-E., S. 151.

145 *Zu bemerken ist gleichwohl, dass in der Praxis die Trennung zwischen den allein aufgrund der Speicherungsverpflichtung nach § 110a TKG-E gespeicherten Daten und den übrigen Daten schwer sein wird (vgl. § 110b Abs. 1 S. 3 TKG-E). Auch diesbezüglich sind also Unsicherheiten bei der Rechtsanwendung nicht ausgeschlossen*.

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

gemessen. Zweifelhaft ist außerdem, ob das damit einhergehende Ausmaß der vorgesehenen Zugriffsbefugnisse in einem angemessenen Verhältnis zu ihrem tatsächlichen Nutzen steht[148].

e) Zwischenergebnis für die zweite Stufe

Die Zugriffsmöglichkeiten auf Vorratsdaten bei der Verfolgung mittelschwerer und aller mittels Telekommunikationsmitteln begangener Straftaten ist unverhältnismäßig und geht über die Vorgaben der Vorratsdatenspeicherungsrichtlinie hinaus. Dies wird noch dadurch verstärkt, dass für die Verwendung von Vorratsdaten bereits ein Anfangsverdacht reicht und die Differenzierung bezüglich der Kontaktpersonen (Nachrichtenmittler) unzureichend ist.

2. Verstoß gegen Art. 12 Abs. 1 GG

Mit der Verpflichtung der Telekommunikationsunternehmen zur Speicherung der in § 110a 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[149]. 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 § 110a Abs. 6 TKG-E enthaltene Verpflichtung der Telekommunikationsunternehmen, Angaben zu ihrer Netzplanung zu machen, das praktische Verbot von Anonymisierungsdiensten sowie die Pflicht zur Erhebung von Kundendaten und Kundenidentifizierung bei Eröffnung eines E-Mail-Accounts (§ 111 TKG-E) dar. Auch dies beeinträchtigt die Unternehmensfreiheit der Telekommunikationsunternehmen, die zu befürchten haben, dass viele Kunden deswegen verloren gehen.

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

---

147 Vgl. einerseits *LG Bonn*, DuD 2004, S. 628 und andererseits *LG Hamburg*, MMR 2005, S. 711, LG Stuttgart, NJW 2005, S. 614.

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

149 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).

gung vorsieht[150]. Dabei ist zu berücksichtigen, dass der Deutsche Bundestag die Bundesregierung ausdrücklich aufgefordert hat, zeitnah einen Gesetzesentwurf für eine angemessene Entschädigung der Telekommunikationsunternehmen für die Inanspruchnahme im Rahmen der Erfüllung hoheitlicher Ermittlungsmaßnahmen im Bereich der Telekommunikation vorzulegen[151]. Ob dies mit der geplanten Änderung des JVEG in ausreichendem Maße geschehen wird, bleibt abzuwarten[152]. 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[153].

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.

---

150 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).

151 Vgl. BT-Drs. 16/545, S. 4.

152 Vgl. dazu Begründung Ref.-E., S. 73.

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