BUNDESRECHTSANWALTSKAMMER

Stellungnahme

der Bundesrechtsanwaltskammer

zum

Gesetzentwurf der Bundesregierung zum

Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG

BR-Drucks. 275/07

erarbeitet vom

Strafrechtsausschuss
der Bundesrechtsanwaltskammer

Rechtsanwalt Prof. Dr. Dr. Alexander Ignor, Berlin, Vorsitzender
Rechtsanwalt und Notar Dr. Jochen Heidemeier, Stolzenau
Rechtsanwalt Thomas C. Knierim, Mainz (Berichterstatter)
Rechtsanwalt Dr. Daniel Krause, Berlin (Berichterstatter)
Rechtsanwalt Prof. Dr. Holger Matt, Frankfurt am Main
Rechtsanwältin Anke Müller-Jacobsen, Berlin
Rechtsanwalt Dr. Eckhart Müller, München
Rechtsanwalt Prof. Dr. Reinhold Schlothauer, Bremen
Rechtsanwältin Dr. Anne Wehnert, Düsseldorf

Prof. Dr. Matthias Jahn, Erlangen (Berichterstatter)
Vors. RiLG Joachim Rahlf, Augsburg (Berichterstatter)

Rechtsanwalt Frank Johnigk, Bundesrechtsanwaltskammer, Berlin
Rechtsanwältin Mila Otto, LL.M., Bundesrechtsanwaltskammer, Brüssel

August 2007
BRAK-Stellungnahme-Nr. 31/2007

Verteiler:

Bundesministerium der Justiz

Rechtsausschuss des Deutschen Bundestages

Arbeitskreise Recht der Bundestagsfraktionen

Landesjustizminister/Justizsenatoren der Länder

Rechtsanwaltskammern

Bundesverband der Freien Berufe

Bundesnotarkammer

Bundessteuerberaterkammer

Deutscher Steuerberaterverband

Wirtschaftsprüferkammer

Institut der Wirtschaftsprüfer

Deutscher Anwaltverein

Deutscher Notarverein

Deutscher Richterbund

Deutscher Juristinnenbund

Bundesvorstand Neue Richtervereinigung

Redaktionen der NJW, Strafverteidiger, Neue Zeitschrift für Strafrecht, ZAP Verlag

Bundesministerium für Wirtschaft und Technologie

A. Einleitung, Übersicht und Zusammenfassung

I. Einleitung

Der Strafrechtsausschuss der Bundesrechtsanwaltskammer begrüßt das Vorhaben, ein harmonisches Gesamtsystem der heimlichen strafprozessualen Ermittlungsmaßnahmen insbesondere im Bereich der Telekommunikationsüberwachung (TKÜ) zu schaffen, das rechtsstaatlichen Maßstäben im Allgemeinen und den Maßgaben des Bundesverfassungsgerichts im Besonderen entspricht.

Der Gesetzentwurf wird diesem Anspruch in Teilen gerecht. Das gilt insbesondere für die z.T. neu gefassten prozessualen Schranken und Einhegungen heimlicher Ermittlungsmaßnahmen wie den Richtervorbehalt und bestimmte Kennzeichnungs-, Benachrichtigungs- sowie Löschungspflichten hinsichtlich der erhobenen Daten. Der Strafrechtsausschuss hat insoweit nur wenige Änderungsvorschläge.

Der Strafrechtsausschuss befürwortet die Übertragung der Vorgaben des Bundesverfassungsgerichts für den Schutz des Kernbereichs der Persönlichkeit bei der akustischen Wohnraumüberwachung auch auf die TKÜ. Allerdings sieht der Ausschuss den gebotenen Schutz in der vorgesehenen Regelung (§ 100a Abs. 4 StPO-E) nicht ausreichend verwirklicht.

Grundsätzliche Bedenken hat der Strafrechtsausschuss gegen die vorgesehene Neuregelung des Schutzes der Berufsgeheimnisträger. Die Regelungen des § 53b StPO-E bleiben z.T. hinter den verfassungsrechtlichen Anforderungen zurück; die Differenzierung zwischen zwei Gruppen von Berufsgeheimnisträgern ist unangemessen.

Ablehnend steht der Ausschuss ferner der Erweiterung des Katalogs der sog. Anlasstaten für eine TKÜ in § 100a Abs. 2 StPO-E gegenüber sowie den im TKG (§§ 113a, 113b TKG-E) und in der StPO (§ 100g StPO-E) neu vorgesehenen Regelungen über die sog. Vorratsdatenspeicherung und deren Verwendung im Strafverfahren. Das gilt auch, soweit die Regelungen der Umsetzung der EU-Richtlinie 2006/24/EG zur sog. Vorratsdatenspeicherung dienen sollen. Auch die zur Umsetzung der Richtlinie getroffenen Regelungen müssen sich am Maßstab der Verfassung messen lassen.

Generell gibt der Strafrechtsausschuss zu bedenken:

Nach traditionellem Grund- und Menschenrechtsverständnis gehen die natürlichen Freiheitsrechte aller staatlichen Gewalt voraus und werden als solche durch die Verfassung gewährleistet. Demgemäß bedarf jeder Eingriff der staatlichen Gewalt in den Schutzbereich dieser Rechte einer besonderen Rechtfertigung, die sich ihrerseits an den Gewährleistungen der Verfassung messen lassen muss.

Es ist daher missverständlich, wenn es in der Einleitung zum Gesetzentwurf heißt, jede weitere gesetzliche Beschränkung der strafrechtlichen Ermittlungstätigkeit bedürfe mit Blick auf die Gewährleistung einer funktionstüchtigen Strafrechtspflege einer besonderen Legitimation.[1] Ein Verfassungsverständnis, welches den Bedürfnissen einer funktionstüchtigen Strafrechtspflege den prinzipiellen Vorrang vor den Freiheitsrechten des Einzelnen einräumte, kann sich nicht auf die Rechtsprechung des Bundesverfassungsgerichts stützen und würde das dem Grundgesetz immanente Verhältnis von Freiheit und staatlicher Gewalt geradezu umkehren. Nicht die Freiheitsrechte müssen sich gegenüber der Strafrechtspflege rechtfertigen. Vielmehr bedürfen die mit der Strafverfolgungstätigkeit verbundenen Eingriffe in die Freiheitsrechte im Hinblick darauf stets einer besonderen Legitimation. An dieser rechtsstaatlichen Prämisse gilt es auch in Zeiten erhöhter gesellschaftlicher Sicherheitsbedürfnisse festzuhalten.

Angesichts dieser Grundsätze eines rechtsstaatlichen Strafprozessrechts begrüßt es der Strafrechtsausschuss ausdrücklich, dass der Entwurf keine Regelung der sog. Online-Durchsuchung enthält, und rät dringend davon ab, den Entwurf im Verlaufe des Gesetzgebungsverfahrens damit zu befrachten.

Wer Grundrechte einschränken will, muss die Geeignetheit, Erforderlichkeit und Angemessenheit des beabsichtigten Grundrechtseingriffs nachweisen. Heimliche Überwachungsmaßnahmen müssen in einem Rechtsstaat Ausnahmen sein. Soweit danach verdeckte Ermittlungsmaßnahmen im Bereich der Telekommunikation überhaupt in Betracht kommen, sind im Hinblick auf die Rechtsprechung des Bundesverfassungsgerichts (insb. BVerfGE 109, 279 ff.) folgende Grundsätze zu beachten:

- Soweit es um Eingriffe in Art. 13 GG geht, darf die hohe Eingriffsschwelle für eine heimliche akustische Wohnraumüberwachung nicht unterschritten werden.

[1] BR-Drucks. 275/07, S. 43 unter Bezugnahme auf BVerfGE 33, 367, 383. Dort wird indes kein allgemeiner solcher Grundsatz aufgestellt, weil sich die Formulierung nur im Zusammenhang mit einer Erweiterung des gesetzlichen Zeugnisverweigerungsrechtes findet, es also gerade um Erweiterung von Freiheit und nicht um ihre Einschränkung geht.

- Auch bei sonstigen Grundrechtseingriffen müssen der Schutz des Kernbereichs privater Lebensgestaltung und das damit einher gehende Verbot einer umfassenden Ausforschung der Persönlichkeitssphäre durch Beweiserhebungs- und Verwertungsverbote gewährleistet werden.

- Die besondere Stellung der Berufsgeheimnisträger erfordert geeignete Vorkehrungen gegen Aushöhlungen des Geheimnisschutzes.

- Es müssen effektive Regelungen über die Kontrolle der Grundrechtseingriffe, die Benachrichtigung darüber und den Rechtsschutz gegeben sein.

II. Übersicht

Der Strafrechtsausschuss nimmt nachfolgend unter **B.** ausführlich Stellung

- zur Kritik an einzelnen Regelungen des dem Gesetzentwurf vorangehenden Referentenentwurfs, soweit diese nach Auffassung des Ausschusses unbegründet ist (unter B. I.)

- zur vorgesehenen Neuregelung des Schutzes der Berufsgeheimnisträger in § 53b StPO-E (unter B. II.)

- zur vorgesehenen Änderung der Regelungen der TKÜ in § 100a StPO-E (unter B. III.)

- zur vorgesehenen sog. Vorratsdatenspeicherung (§§ 113a, 113b TKG-E) und deren Verwendung zur Strafverfolgung (§ 100g StPO-E) (unter B. IV.)

- zum IMSI-Catcher, § 100i StPO-E (unter B.V.)

- zur vorgesehenen Sichtung von räumlich getrennten Speichermedien in § 110 Abs. 3 StPO-E (unter B. VI.)

- zu den vorgesehenen Neufassungen der strafprozessualen Schranken und Einhegungen heimlicher Ermittlungsmaßnahmen (unter B. VII.)

III. Zusammenfassung der Kritik an einzelnen Regelungen des Gesetzentwurfs

Zur besseren Übersicht fasst der Strafrechtsausschuss seine unter **B.** ausführlich begründete Kritik an einzelnen Regelungen des Entwurfs und darauf gründende Empfehlungen vorweg wie folgt zusammen:

Zu § 53b StPO-E

Die vorgeschlagene Differenzierung zwischen zwei Gruppen von Berufsgeheimnisträgern überzeugt nicht. Der Strafrechtsausschuss befürwortet eine Gleichbehandlung aller Berufsgeheimnisträger nach dem Vorbild des § 100c Abs. 6 StPO.

Die in Absatz 4 vorgesehene Regelung zum Wegfall des Beweiserhebungs- und –verwertungsverbotes in sog. Verstrickungsfällen genügt nicht den verfassungsrechtlichen Anforderungen, die das Bundesverfassungsgericht jüngst in der CICERO-Entscheidung (in Bezug auf Presseangehörige) aufgestellt hat. Wegen der vergleichbaren Schutzbedürftigkeit des Vertrauensverhältnisses auch zu den anderen Berufsgeheimnisträgern sollte die Verdachtsschwelle für alle Berufsgeheimnisträger angehoben und dem Verdachtsgrad des § 138a Abs. 1 StPO („*dringend oder in einem die Eröffnung des Hauptverfahrens rechtfertigenden Grade*“) angepasst werden.

Für Maßnahmen gegenüber Verteidigern sollte überdies geregelt werden, dass vor Anordnung der Maßnahme der Antrag auf Ausschließung des Verteidigers (§ 138c StPO) zu stellen ist.

Ferner darf durch die vorgesehene Regelung des § 53b StPO-E keine Relativierung der zu § 148 StPO entwickelten Grundsätze (hinsichtlich des besonderen Schutzes vor Telekommunikationsüberwachungsmaßnahmen im Verhältnis zwischen Mandant und Verteidiger) erfolgen. Daher ist in § 53b Abs. 5 StPO-E zusätzlich die Vorschrift des § 148 StPO anzuführen.

Zu § 97 Abs. 2 Satz 3 StPO-E

Korrespondierend mit Vorstehendem ist auch in die Regelung des § 97 Abs. 2 Satz 3 StPO bezüglich aller Berufsgeheimnisträger der Verdachtsgrad des § 138a Abs. 1 StPO

(“*dringend oder in einem die Eröffnung des Hauptverfahrens rechtfertigenden Grade*“) aufzunehmen.

Zu § 100a StPO-E

In Anbetracht der Schwere des Grundrechtseingriffs der Telekommunikationsüberwachung ist die Ausweitung des Straftatenkataloges in Abs. 2 namentlich auf Straftaten der mittleren Kriminalität, die nicht typischerweise im Rahmen organisierter Kriminalität, sondern im allgemeinen Wirtschafts- und Sozialleben stattfinden (z.B. Dopingdelikte, Betrugsstraftaten, Korruptionsdelikte, Bankrottstraftaten), unangemessen. Maßnahmen der Telekommunikationsüberwachung rechtfertigen sich nicht schon durch das allgemeine Bedürfnis einer funktionstüchtigen Strafrechtspflege.

Die vorgesehene Neuregelung des Abs. 4 Satz 1 trägt dem verfassungsrechtlich gebotenen Schutz des Kernbereichs privater Lebensgestaltung insoweit nicht ausreichend Rechnung, als sie ein Erhebungsverbot nur dann vorsieht, wenn durch die TKÜ-Maßnahme *„allein“* Erkenntnisse aus diesem Kernbereich erlangt würden. Diese Voraussetzung wird in der Praxis – bei der gebotenen Prognose - kaum jemals anzunehmen sein. Damit droht das Erhebungsverbot leerzulaufen. Vorzugswürdig erscheint ein Erhebungsverbot bereits dann, wenn durch die Maßnahme *„überwiegend“* Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden.

Schließlich sollte die Vorschrift des § 100a StPO in einem neu zu schaffenden Abs. 5 ein generelles Verwertungsverbot für Erkenntnisse aus einer TKÜ-Maßnahme vorsehen, bei der die gesetzlichen Anordnungsvoraussetzungen grob fehlerhaft missachtet wurden, um solchen Grundrechtsverstößen effektiv vorzubeugen.

Zu § 100b StPO-E

Die Vorschrift des § 100b Abs. 2 StPO-E, der die formalen Anordnungsvoraussetzungen einer TKÜ-Maßnahme regelt, sollte um das Erfordernis einer schriftlichen Begründung erweitert werden, auch wenn eine Begründungspflicht bereits aus § 34 StPO resultiert. Die Bedeutung, die der Begründung einer Maßnahme für deren Rechtfertigung zukommt, würde dadurch unterstrichen.

Zu § 100g StPO-E und zu den §§ 113a, 113b TKG-E

Durch Einfügung der §§ 113a, 113b TKG-E und weitere Änderungen des Telekommunikationsgesetzes (TKG) soll für die Anbieter von Telekommunikationsleistungen

eine Pflicht zur Speicherung sämtlicher Verkehrs- und Standortdaten für einen Zeitraum von 6 Monaten geschaffen werden (sog. Vorratsdatenspeicherung). Zugleich soll durch Änderung des § 100g StPO-E eine umfassende Befugnis zur Erhebung solcher Daten zum Zwecke der Strafverfolgung geschaffen werden.

Die vorgesehenen Regelungen gehen weit über die nach geltendem Recht bestehende Pflicht zur Speicherung von Kundendaten (§ 111 TKG) und die strafprozessuale Befugnis zur Erhebung von Verbindungsdaten (§ 100g StPO) hinaus.

Die neu vorgesehen Regelungen über die Pflicht zur Speicherung von Verkehrs- und Standortdaten und die Befugnis zur umfassenden Erhebung solcher Daten für Strafverfolgungszwecke werden den verfassungsrechtlich gebotenen Begrenzungen von Eingriffen in das Grundrecht auf ungestörte Telekommunikation (Art. 10 GG) und das Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) insgesamt nicht gerecht. Bei der Vorratsdatenspeicherung der Verkehrs- und Standortdaten handelt es sich um einen verdachts- und anlassunabhängigen Eingriff in die genannten Grundrechte, der im bisherigen Recht ohne Vorbild ist. Sofern ein solcher Eingriff verfassungsrechtlich überhaupt zulässig sein sollte, was der Strafrechtsausschuss bezweifelt, ist er hinsichtlich des Umfangs der zu speichernden Daten und ihrer Verwendungsmöglichkeiten eng zu begrenzen und rechtlich abzusichern. Für die Erhebung von Verkehrs- und Standortdaten sollte zum Zwecke der Strafverfolgung die gleiche Eingriffsschwelle wie für die Erhebung von Inhaltsdaten gelten.

Zu § 101 Abs. 4 Satz 1 StPO-E

Für die geplanten Ausnahmen von der Benachrichtigungspflicht sollte eine Pflicht der Staatsanwaltschaft zur Begründung für die Ausnahme vorgesehen werden.

Zu § 101 Abs. 7 StPO-E

Durch die neu vorgesehene Regelung soll die Möglichkeit geschaffen werden, von der grundsätzlichen Pflicht zur Benachrichtigung über eine heimliche Ermittlungsmaßnahme dann abzusehen, wenn die Benachrichtigung bereits für insgesamt fünf Jahre zurückgestellt worden ist und sich nach diesen fünf Jahren ergibt, dass die Voraussetzungen für eine Benachrichtigung mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft nicht eintreten werden.

Der Strafrechtsausschuss lehnt diese Regelung ab, weil sie eine ohnehin kaum vorstellbare Fallgestaltung betrifft und zur Schwächung der nachträglichen Rechtsschutzmöglichkeiten

beiträgt. Stattdessen sollte eine definitive Pflicht zur Benachrichtigung des von einer heimlichen Ermittlungsmaßnahme Betroffenen spätestens nach fünf Jahren eingeführt werden.

Zu § 101 Abs. 9 Satz 1 StPO-E

Die vorgesehene Ausschlussfrist für den nachträglichen Rechtsschutz gegen verdeckte Ermittlungsmaßnahmen ist mit zwei Wochen zu kurz bemessen; sie sollte auf einen Monat erweitert werden.

Zu § 110 Abs. 3 StPO-E

Die Vorschrift soll eine Befugnis dafür schaffen, im Rahmen einer Durchsuchung solche elektronischen Speicher auf beweisrelevante Daten durchzusehen, die von den Räumlichkeiten des Betroffenen getrennt sind, zu denen er aber zugangsberechtigt ist, und diese Daten für die Strafverfolgung ggf. zu speichern.

In Anbetracht der vielfach noch ungeklärten Fragen zur verfassungsrechtlichen Zulässigkeit von Eingriffen in die Netzwerkkommunikation, insbesondere zur Durchsicht von Computern, die miteinander verbunden sind, lehnt der Strafrechtsausschuss die Vorschrift als zu unbestimmt ab. Sie konkretisiert weder Art noch Umfang des Eingriffs und stellt die Durchsicht von Netzwerken oder internetbasierten Datenspeichern Durchsuchungen nach §§ 102 ff. StPO gleich. Richtigerweise sind solche Maßnahmen den für Eingriffen in die Telekommunikation vorgesehenen Bestimmungen der §§ 100a, 100b StPO-E zu unterwerfen.

Zu § 477 Abs. 2 StPO-E

Auch im Falle der Postbeschlagnahme ist die Zweckbindung der dadurch gewonnenen Daten zu gewährleisten.

B. Stellungnahme

I. Befürwortung des Konzepts einer „harmonischen Gesamtregelung“ und Zurückweisung einzelner Kritikpunkte am vorausgehenden Referentenentwurf

Der Strafrechtsausschuss befürwortet das Ziel einer harmonischen Gesamtregelung der strafprozessualen heimlichen Ermittlungsmaßnahmen insbesondere im Bereich der Telekommunikationsüberwachung[2], und sieht die mit dem Gesetzentwurf vorgelegte Umsetzung in weiten, wenn auch nicht allen Teilen als gelungen an.

Die in **§ 100b Abs. 1 Satz 4 StPO-E** vorgesehene **Befristung der richterlichen TKÜ-Anordnung auf zwei Monate** – eine Verkürzung der geltenden Frist von drei Monaten - entspricht dem im Grundsatz der Verhältnismäßigkeit enthaltenen Prinzip der Erforderlichkeit. Soweit dagegen vorgebracht wird[3], die Änderung der Anordnungsdauer erscheine nicht geboten, weil von den Strafverfolgungsbehörden Überwachungsmaßnahmen ohnehin beendet würden, wenn entweder das Ziel der Ermittlungen erreicht ist oder aber die Zielerreichung aussichtslos erscheint, so mag dies in vielen Fällen zutreffen. Dieser Einwand berücksichtigt aber nicht die in der Entwurfsbegründung angesprochenen Ermittlungsroutinen bei TKÜ-Anordnungen. Das Abschalten von Telefonüberwachungsmaßnahmen dürfte nicht immer nur rechtliche, sondern oftmals rein praktische Gründe haben (Ressourcenprobleme, Verlagerung von Ermittlungsschwerpunkten auch innerhalb von Fachkommissariaten). Jedenfalls wird durch Verkürzung der Anordnungsfristen die Stellung des Ermittlungsrichters gestärkt.[4]

Der in **§ 100b Abs. 1 Satz 6 StPO-E** vorgesehene **Übergang der ermittlungsrichterlichen Kontrolle auf das im Rechtszug übergeordnete Gericht nach Ablauf von sechs Monaten** bedeutet eine Intensivierung der richterlichen Kontrolle, die im Hinblick auf die mit dem Zeitablauf einhergehende Vertiefung des Grundrechtseingriffs geboten ist. Die

---

2 S. dazu bereits *Zypries*, RuP 2006, 5 (6) sowie BT-Drucks. 14/7008, S. 6.

3 Stellungnahme des Deutschen Richterbundes zum RefE vom Januar 2007, S. 3.

4 Siehe dazu *Strafrechtsausschuss der Bundesrechtsanwaltskammer*, Thesen zum Richtervorbehalt (RS-Nr. 96/2004). Kritisch zum status quo ermittlungsrichterlicher Kontrolle auch BVerfG (3. Kammer des 2. Senats), NJW 2005, 275 (276); Jahn NStZ 2007, 255 (259 m.w.N.). S. auch BT-Drucks. 16/1421 v. 10.05.2006, S. 4 (unter 3.).

Regelung könnte zudem der nicht seltenen Praxis bloß formelhafter Begründungen von Entscheidungen[5] entgegenwirken.

Der Strafrechtsausschuss begrüßt es des weiteren, dass der Gesetzentwurf wie auch schon der Referentenentwurf **keine Regelung der sog. heimlichen Online-Durchsuchung** vorsieht.

Die Besonderheit der Online-Durchsuchung besteht darin, dass die davon betroffenen Computer nicht im Rahmen einer „offenen" Wohnungsdurchsuchung durch Ermittlungsbeamte und ggf. hinzuziehende weitere Personen (vgl. §§ 105 Abs. 2, 106 Abs. 1 StPO), sondern mittels eines heimlichen Online-Zugriffs durchsucht werden. Dieser Zugriff erfolgt bspw. unter Zuhilfenahme technischer Vorrichtungen (sog. Trojaner- oder Backdoor-Programme), sobald der zu durchsuchende PC mit dem Internet verbunden ist. Auf diesem Weg können dort gespeicherte und möglicherweise verfahrensrelevante Daten und E-Mails eingesehen und zur Beweissicherung heruntergeladen werden, ohne dass der Verdächtige hiervon erfährt.

Bekanntlich hat nicht nur der Ermittlungsrichter des BGH[6], sondern auch der 3. Strafsenat[7] entschieden, dass die Praxis der sog. verdeckten Online-Durchsuchung im geltenden Recht keine Grundlage findet. Insbesondere können weder die Durchsuchungsvorschriften der §§ 102 ff. StPO noch § 100a StPO hierfür als Rechtsgrundlage herangezogen werden.

Der Regierungsentwurf sieht zwar mit § 110 Abs. 3 StPO-E die Durchsicht elektronischer Datenträger vor. Ausdrücklich soll durch die Vorschrift aber nicht der heimliche Online-Zugriff auf zugangsgeschützte Datenbestände im Sinne eines so genannten *„staatlichen Hackings"* erlaubt werden[8].

Die Online-Durchsuchung stellt eine heimliche Maßnahme dar, die eine denkbar weite Überwachung und Durchleuchtung der Kommunikation wie auch der Privatsphäre des Betroffenen bedeutet. Heimliche Ermittlungsmethoden zur Strafverfolgung müssen in einem Rechtsstaat die Ausnahme bleiben. Schon aus diesem Grunde darf eine Gesetzgebung in diesem Bereich kein Schnellschuss sein. Außerdem sind dabei auch künftige technische Entwicklungen zu bedenken.

---

5 *Kühne,* in: Löwe/Rosenberg, 26. Aufl. (2006), Einl. F Rn. 206.

6 BGH (Ermittlungsrichter), Beschl. v. 25.11.2006 – 1 BGs 184/06 und Beschl. v. v. 28.11.2006 – 1 BGs 186/2006, m. Anm. *Jahn/Kudlich*, JR 2007, 57. A.A. noch BGH (Ermittlungsrichter), Beschl. v. 21.2.2006 – 3 BGs 31/06 m. abl. Anm. *Beulke*/*Meininghaus*, StV 2007, 63 sowie *Hoffmann*, NStZ 2005, 121 (123).

7 Beschl. v. 31.1.2007 – StB 18/06.

8 BR-Drucks. 275/07, S. 146.

Fraglos ist durch einen solchen schwerwiegenden Eingriff in die Privatsphäre des Einzelnen das Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) berührt. Ferner ist das Grundrecht auf Unverletzlichkeit der Wohnung (Art. 13 Abs. 1 GG) zumindest dann betroffen, wenn auf Computer und andere Datenträger zugegriffen werden soll, die sich in einer Wohnung oder in einem Betriebs- oder Geschäftsraum befinden[9]. Inhaltlich können solche heimlichen Online-Überwachungen den unantastbaren Kernbereich der Persönlichkeitssphäre verletzen. Das Gewicht des Grundrechtseingriffs wächst mit der zunehmenden Vernetzung der Bürger und ist derzeit in seinen Auswirkungen noch wenig abschätzbar. Soweit der Schutzbereich von Art. 13 GG betroffen ist, würde eine gesetzliche Regelung zwingend eine Änderung des Grundgesetzes voraussetzen, weil die bestehenden Schranken des Grundrechtes auf Unverletzlichkeit der Wohnung repressive heimliche Onlinezugriffe nicht zulassen.

Im Übrigen muss derjenige, der Grundrechte einschränken will, die Geeignetheit, Erforderlichkeit und Angemessenheit des beabsichtigten Grundrechtseingriffs nachweisen. Diese Voraussetzungen sind für verdeckte Online-Überwachungen bislang nicht hinreichend dargetan. Aus diesem Grunde sind auch die Empfehlungen der Ausschüsse des Bundesrates[10] in der Stellungnahme des Bundesrates[11] zu Recht nicht aufgegriffen worden, weil sie die Unverzichtbarkeit des Ermittlungsinstruments der Online-Durchsuchung nur behauptet, aber nicht beleget hatten.

II. Zur vorgesehenen Neuregelung des § 53b StPO-E

1. Inhalt und Zweck der Neuregelung

Ausgehend von der Kernbereichsrechtsprechung des Bundesverfassungsgerichts verfolgt der Gesetzentwurf den Ansatz, dem besonderen Schutz des Vertrauensverhältnisses des Bürgers zu den in § 53 StPO genannten Berufsgeheimnisträgern durch eine allgemeine, „vor die Klammer“ gezogene Regelung Rechnung zu tragen. Durch die neue Vorschrift des § 53b StPO-E wird nach der Entwurfsbegründung ein *„harmonisiertes System zur Berücksichtigung*

---

9 Ebenso *Harrendorf*, StraFo 2007, 149, 151 f. *Bär,* MMR 2007, 175 (176) und *Jahn/Kudlich*, JR 2007, 57. Zum selben Ergebnis führt die von *Rux,* JZ 2007, 285 (292 ff.) für die Eingriffsmaßnahme der Online-Durchsuchung vorgeschlagene Analogie zu Art. 13 Abs. 1 GG. A.A. *Beulke*/*Meininghaus*, StV 2007, 63 (65).

10 BR-Drucks. 275/1/07 Nr. 25, S. 17 ff. Der dort vorgeschlagene Rückgriff auf den Katalog des § 100a StPO stünde in Widerspruch zu dem beschriebenen Anwendungsbereich, der im wesentlichen Falle der organisierten Kriminalität und des Terrorismus beschreibt. Das Erfordernis einer Änderung des Art. 13 GG wurde überhaupt nicht angesprochen.

11 BR-Drucks. 275/07 v. 8.6.2007.

der von den Zeugnisverweigerungsrechten der Berufsgeheimnisträger (§§ 53, 53a StPO) geschützten Interessen ein(geführt)"[12].

Der Ansatz des Entwurfes, für Eingriffe, durch die die zeugnisverweigerungsberechtigten Berufsgeheimnisträger (§ 53 StPO) betroffen sein können, eine allgemeine, für sämtliche Ermittlungsmaßnahmen der StPO geltende Regelung zu schaffen, ist ausdrücklich zu begrüßen. Hierdurch wird ein unbefriedigender Rechtszustand behoben und dem Postulat des EGMR[13] Rechnung getragen, der im Hinblick auf Art. 8 Abs. 1 MRK zwar nicht den Ausschluss ganzer Berufsgruppen von der Überwachung verlangt, wohl aber konkrete Anforderungen an entsprechende nationale Regelungen gestellt hat. Solche fehlten in Deutschland bisher; lediglich § 100h Abs. 2 StPO sieht bislang eine spezielle Regelung für Berufsgeheimnisträger bei der Anordnung zur Auskunftserteilung über Telekommunikationsverbindungen vor.

Zu begrüßen ist ferner der Ansatz des Entwurfes, wonach § 53b StPO-E schon dann Anwendung findet, wenn das Kommunikationsverhältnis zu einem Berufsgeheimnisträger von der Maßnahme (lediglich) mitbetroffen sein kann, also nicht erst dann, wenn die Maßnahme gezielt auf dieses Kommunikationsverhältnis gerichtet ist.[14] Dadurch wird nicht nur der Bedeutung der geschützten Kommunikationsverhältnisse Rechnung getragen, sondern auch etwaigen Umgehungsrisiken entgegen gewirkt.

Der Ansatz des Entwurfes, den Schutz der Kommunikationsverhältnisse zu Berufsgeheimnisträgern strukturell über die Verankerung eines Beweiserhebungsverbotes kombiniert mit einem Beweisverwertungsverbot (§ 53b Abs. 1 Satz 1 und 2 StPO-E) zu gewährleisten, ist im Ausgangspunkt sachgerecht. Er entspricht der in § 100c Abs. 6 StPO getroffenen Regelung.

2. Kritik

Gleichwohl bestehen gegen den Entwurf in verschiedener Hinsicht gewichtige Bedenken. Diese richten sich zuvorderst gegen die Differenzierung zwischen Seelsorgern, Verteidigern und Parlamentsabgeordneten (§ 53 Abs. 1 Satz 1 Nr. 1, 2 und 4 StPO), bei denen ein Beweiserhebungsverbot bestehen soll, und den anderen Berufsgeheimnisträgern, bei denen (lediglich) besondere Anforderungen an die Anordnung kombiniert mit einem Beweisverwertungsverbot bestehen sollen. Diese differenzierende Regelung schafft hinsichtlich der Intensität des Schutzes vor staatlichen Eingriffen eine sachlich nicht

12 BR-Drucks. 275/07, S. 74.
13 StV 1998, 683 m. Anm. *Kühne*.
14 BR-Drucks. 275/07 S. 76.

gerechtfertigte und demzufolge nicht hinnehmbare „Zweiklassengesellschaft“ innerhalb der Berufsgeheimnisträger. Bedenken bestehen ferner insoweit, als die Regelung zum Fortfall des Schutzes vor staatlichen Eingriffen in Verstrickungskonstellationen (§ 53b Abs. 4 StPO) der jüngsten Rechtsprechung des Bundesverfassungsgerichts („CICERO“)[15] nicht gerecht wird und anzupassen ist. Aus diesem Grund ist auch die vorgeschlagene Änderung des § 97 Absatz 2 Satz 3 StPO-E nicht ausreichend und ebenfalls anzupassen.

a) Unsachgemäße Differenzierung zwischen zwei Gruppen von Berufsgeheimnisträgern (§ 53b Abs. 1 und 2 StPO-E)

Dem Entwurf ist nachdrücklich entgegenzutreten, soweit er zwischen einzelnen Berufsgruppen in § 53b Abs. 1 und 2 StPO-E differenziert.

Schon bei Einführung der Regelungen zum sog. großen Lauschangriff in §§ 100c und 100d StPO hat sich eine zunächst erwogene Differenzierung zwischen Geistlichen, Strafverteidigern und Abgeordneten einerseits und den anderen Berufsgeheimnisträgen andererseits zu Recht nicht durchsetzen können. Auf Empfehlung des Vermittlungsausschusses wurde die Beweisverbotsregelung des (früheren) § 100d Abs. 3 StPO (heute § 100c Abs. 6 StPO) auf alle Berufsgeheimnisträger erstreckt.[16] Die seinerzeit gegen eine Differenzierung sprechenden Erwägungen gelten unverändert fort. Der Gesetzgeber sollte deshalb auch bei § 53b StPO-E von einer Differenzierung absehen und die Regelung des § 53b Abs. 1 StPO-E auf alle Berufsgeheimnisträger (§ 53 Absatz 1 StPO) erstrecken.

Soweit sich die Entwurfsbegründung auf die Entscheidung des Bundesverfassungsgerichts zur Wohnraumüberwachung bezieht, vermag dies die Differenzierung nicht zu tragen. Das Bundesverfassungsgericht hat in seiner Entscheidung anders als die Entwurfsbegründung andeutet – keineswegs nur die seelsorgerischen Gespräche und die Kommunikation mit dem Verteidiger dem Kernbereich privater Lebensgestaltung zugeordnet, sondern vielmehr ausgeführt, dass auch Gespräche mit dem Arzt im Einzelfall dem Kernbereich privater Lebensgestaltung zuzuordnen sein können.[17] Andere Berufsgruppen hat das Bundesverfassungsgericht in diesem Zusammenhang gar nicht angesprochen, sich also hinsichtlich der Zuordnung nicht geäußert. Eine positive Differenzierung lässt sich daraus

---

15 NJW 2007, 1117.

16 Zustimmung des Bundestages BT-Plenarprot. der 222. Sitzung S. 20294 ff., des Bundesrates BR-Plenarprot. der 722. Sitzung S. 53 ff.; Gesetzesbeschluss BR-Drucks. 214/98.

17 BVerfGE 109, 279, 322 f.

nicht herleiten. Entsprechendes gilt für die vom Entwurf in Bezug genommene Regelung des § 100h Absatz 2 StPO. Diese Bestimmung war stets wegen der unterschiedlichen Behandlung der Berufsgeheimnisträger umstritten und wird als willkürlich angesehen.[18] Überdies liegen zu der Vorschrift, die die eng umgrenzte Materie der Auskunft über Telekommunikationsverbindungen regelt, keine Erkenntnisse über deren praktische Handhabung vor. Eine Rechtsprechung hat sich dazu noch nicht herausgebildet. Um so weniger erscheint es sachgerecht, die vorgesehene allgemeine Regelung an diese umstrittene – und überdies noch nicht bewährte – Spezialregelung anzulehnen, zumal diese Eingriffe weit geringerer Intensität regelt.

Der Entwurf vermag auch deshalb nicht zu überzeugen, weil die Durchbrechung der bei § 97 Absatz 1 StPO und § 100c Abs. 6 StPO bestehenden Gleichbehandlung der Berufsgeheimnisträger nicht begründet wird; sie ist auch nicht begründbar. Selbst wenn die Erwägungen der Entwurfsbegründung zum unterschiedlichen Kernbereichsbezug bei den verschiedenen Berufsgruppen zuträfen (vgl. dazu aber noch sogleich), so werden sie gleichwohl im Hinblick auf Beschlagnahme und Wohnraumüberwachung gleich behandelt. Einbußen für eine effektive Strafverfolgung haben sich hieraus nicht ergeben und werden – soweit ersichtlich – auch nirgendwo behauptet. Bei dieser Sachlage ist eine Durchbrechung der Gleichbehandlung, die der Entwurf vorsieht, in besonderer Weise begründungsbedürftig. Diese Begründung bleibt der Entwurf schuldig.

Zu den einzelnen in § 53b Absatz 2 StPO-E in Bezug genommenen Berufsgruppen ist im Übrigen auf folgendes hinzuweisen: Auch außerhalb des Verteidigungsverhältnisses besteht die vom BVerfG herausgehobene Bedeutung der unkontrollierten Berufsausübung des Rechtsanwaltes.[19] Bei Rechtsanwälten und Ärzten berücksichtigt der Entwurf nicht ausreichend, dass das Eindringen in das Mandats- bzw. Arzt-Patienten-Verhältnis regelmäßig eine Vielzahl von Unbeteiligten berührt. Auch wenn die mit Rechtsanwälten und Ärzten geführte Kommunikation nicht in jedem Einzelfall dem Kernbereich privater Lebensgestaltung zuzuordnen sein mag, so gilt doch andererseits, dass ein solcher Kernbereichs-Bezug in vielen Fällen gegeben ist. Dies gilt insbesondere vor dem Hintergrund, dass viele der in § 53 Abs. 1 Nr. 1 bis 3b StPO genannten Berufsgeheimnisträger mittlerweile auch quasi-seelsorgerische Aufgaben erfüllen und ihnen hierbei unmittelbar kernbereichs-relevante Informationen anvertraut werden. Bei Psychologen, Psychotherapeuten, Ärzten aber auch bei Rechtsanwälten (z.B. Familienrecht) liegt dies auf der Hand. Hinzu tritt der Umstand, dass eine Vielzahl Unbeteiligter in ihren jeweils geschützten Vertrauensverhältnissen von Eingriffen

---

18 *Meyer-Goßner*, StPO § 100h, Rn. 9 m.N.

19 BVerfG Beschl. v. 30.04.2007 – 2 BvR 2151/06 – Rz. 22 (El Masri).

betroffen sein können. Die Differenzierung des Entwurfes erweist sich hiernach als nicht sachgerecht.

Diese Erwägungen werden auch nicht dadurch aufgefangen, dass § 53b Abs. 2 StPO-E besondere Anforderungen an die Verhältnismäßigkeitsprüfung bei Anordnung der Maßnahme gegenüber den in § 53 Absatz 1 Satz 1 Nr. 3 bis 3b, 5 StPO genannten Berufsgeheimnisträgern formuliert und verlangt, das öffentliche Interesse an der von den Berufsgeheimnisträgern wahrgenommenen Aufgabe und das Interesses an der Geheimhaltung der diesen anvertrauten oder bekannt gewordenen Tatsachen besonders zu berücksichtigen. Hierbei handelt es sich nicht um die Verankerung zusätzlicher Abwägungskriterien, sondern lediglich um eine Hervorhebung ohnehin bei der Abwägung zu berücksichtigender Interessen. Eine Anhebung der Eingriffsschwelle bewirkt die die Abwägung konkretisierende Regelung in § 53b Abs. 2 Satz 1 StPO-E daher nicht.

Überdies ist zu berücksichtigen, dass die bei der Anordnung nach § 53b Abs. 2 Satz 1 StPO-E vorzunehmende Abwägung notwendigerweise abstrakt bleiben muss und daher in der Gefahr steht, in der Praxis eher schematisch vorgenommen zu werden. Der Entwurf unternimmt es, die von der Rechtsprechung für Beweisverwertungsverbote entwickelte Abwägungslehre in § 53b Abs. 2 Satz 1 StPO-E auf die Prüfung der Unzulässigkeit der Beweiserhebung zu übertragen. Ob dieser Ansatz im Ergebnis tatsächlich einen Schutz vor unverhältnismäßigen Anordnungen zu bieten vermag, ist bereits vom Ansatz her zweifelhaft. Während sich die von der Rechtsprechung des Bundesgerichtshofes entwickelte Abwägungslehre mit dem Eingreifen eines Verwertungsverbotes nach erfolgten Verfahrensverstößen befasst und die Abwägung des Gewichtes des Verfahrensverstoßes für die Rechtsgüter des Betroffenen gegenüber den Interessen einer funktionstüchtigen Strafrechtspflege anhand des konkreten Einzelfalls erfolgt, ist die in § 53b Abs. 2 StPO-E vorgesehene Abwägung prognostischer und damit notwendigerweise allgemeiner Natur. Dies zeigt sich auch an den im Entwurf genannten abwägungsrelevanten Aspekten, die sich allgemein auf das öffentliche Interesse an den wahrgenommenen Aufgaben der Berufsträger und das (allgemeine) Interesse an der Geheimhaltung der diesen anvertrauten oder bekannt gewordenen Tatsachen beziehen. Es ist zu besorgen, dass die gesetzliche Formulierung in ihrer (notwendigerweise) abstrakten Formulierung der Abwägungskriterien keinen besonderen Schutz gegen unverhältnismäßige Eingriffe bietet. Das damit drohende Absinken der Eingriffsschwelle ist nicht hinnehmbar.

Die vorgesehene Regelung erscheint im übrigen kaum praktikabel und führt mit ihren komplizierten hintereinander geschalteten Verhältnismäßigkeitsprüfungen bei der Anordnung der

Maßnahme und bei der Verwertung gewonnener Erkenntnisse zu unvorhersehbaren Einzelfallentscheidungen. Der Bürger, der einen Arzt, Rechtsanwalt, Wirtschaftsprüfer etc. aufsucht und um Rat, Behandlung oder Begleitung bittet, vermag im vorhinein nicht abzuschätzen, welchen Schutz sein Kommunikationsverhältnis vor staatlichen Eingriffen genießt, weil dies von einer Abwägung im Einzelfall abhängen soll. Das ist namentlich für den Bürger nicht hinnehmbar, der von Ermittlungsmaßnahmen als unbeteiligter Dritter betroffen wäre.

Dabei ist zu bedenken, dass Beweise, die durch Maßnahmen gegenüber nichtbeschuldigten Berufsgeheimnisträgern gewonnen worden sind, in der Praxis so gut wie keine Rolle spielen. Deshalb sollte, für alle Berufsgeheimnisträger das in § 53b Abs. 1 StPO-E geregelte Beweiserhebungsverbot verankert werden. Solche Erkenntnisse, die aus dem Eindringen in ihre Kommunikationsverhältnisse gewonnen worden sind, sind einem strikten Verwertungsverbot zu unterstellen. Das entspricht auch der Wertung des § 203 StGB, der alle Berufsgeheimnisträger und die diesen anvertrauten bzw. bekannt gewordenen Geheimnisse erfasst. Nennenswerte Beeinträchtigungen des Interesses an einer effektiven Strafverfolgung dürften damit nicht verbunden sein.

b) Gebotene Anhebung der Eingriffsvoraussetzungen in sog. Verstrickungsfällen (§§ 53b Abs. 4 , 97 Abs. 2 Satz 3 StPO-E)

Zu begrüßen die im Entwurf vorgesehene Anhebung der Voraussetzungen für die Unanwendbarkeit der das Kommunikationsverhältnis schützenden Regelungen in Fällen des Verdachts der Beteiligung etc. Entfällt das Beschlagnahmeprivileg des § 97 Abs. 1 StPO nach geltendem Recht (§ 97 Abs. 2 Satz 3 StPO, entsprechend § 100c Abs. 6 Satz 3 StPO) bereits dann, wenn gegen den Berufsgeheimnisträger allein der Verdacht der Beteiligung etc. besteht, sieht § 53b Abs. 4 StPO-E (und die entsprechend angepassten § 97 Abs. 2 Satz 3 StPO-E, § 100c Abs. 6 Satz 3 StPO-E) vor, dass gegen den Berufsgeheimnisträger aufgrund dieses Verdachts ein Ermittlungsverfahren eingeleitet sein muss.

Die Verankerung dieser „Schwelle“ für Eingriffe in die geschützten Vertrauensverhältnisse trägt deren Schutzbedürfnis jedoch nicht in ausreichender Weise Rechnung. Denn bei ihr handelt es sich der Sache nach nicht um eine Anhebung des Verdachtsgrades, sondern vielmehr (nur) um ein zu dem bisher erforderlichen einfachen Verdacht hinzutretendes Erfordernis einer Verfahrenshandlung (Einleitung eines Ermittlungsverfahrens gegen den

Berufsgeheimnisträger), die ihrerseits keinen gesteigerten Verdachtsgrad voraussetzt und über die – einer Überprüfung weitgehend entzogen – allein die Staatsanwaltschaft disponiert.

Das Bundesverfassungsgericht hat zum besonderen Schutz der Medienangehörigen jüngst hervorgehoben, dass es eines gesteigerten Verdachts gegen Medienangehörige bedürfe, um Eingriffe in deren geschützte Sphäre in sog. Verstrickungsfällen rechtfertigen zu können. Dabei hat es herausgestellt, dass es nicht hinnehmbar sei, jedweden Verdacht für die Anordnung einer Durchsuchung oder Beschlagnahme bei einem Journalisten ausreichen zu lassen. Denn sonst hätte die Staatsanwaltschaft es in ihrer Hand, durch die Entscheidung zur Einleitung des Ermittlungsverfahrens den besonderen grundrechtlichen Schutz der Medienangehörigen zum Wegfall zu bringen, selbst wenn die Anhaltspunkte für eine Beihilfe schwach sind.[20] Dies gilt in derselben Weise für alle Berufsgeheimnisträger. Auch bei ihnen würde die Möglichkeit, aufgrund eines unzureichenden Verdachts Ermittlungsmaßnahmen durchzuführen, zu dem nicht von der Hand zu weisenden Risiko führen, dass die Staatsanwaltschaft ein Ermittlungsverfahren mit dem ausschließlichen oder überwiegenden Ziel einleitete, auf diese Weise in die geschützte Sphäre des Berufsgeheimnisträges zur Erlangung von Erkenntnissen einzudringen.[21]

Daher vermag ausschließlich eine Anhebung des Verdachtsgrades einen effektiven Schutz der geschützten Sphäre der Berufsgeheimnisträger in Verstrickungskonstellationen zu gewährleisten. Dabei hat die Anhebung der Verdachtsschwelle insbesondere auch dem Umstand Rechnung zu tragen, dass Ermittlungsmaßnahmen gegenüber Berufsgeheimnisträgern stets eine Vielzahl unbeteiligter Dritter in deren geschützten Kommunikationsverhältnissen zu dem Berufsgeheimnisträger berühren und beeinträchtigen. Zu verlangen ist daher die Übernahme des im geltenden Recht in § 138a Abs. 1 StPO verankerten Verdachtsgrades in § 53b Abs. 4 StPO-E. Ermittlungsmaßnahmen gegen einen Berufsgeheimnisträger sind hiernach nur zulässig, wenn dieser *„dringend oder in einem die Eröffnung des Hauptverfahrens rechtfertigenden Grade“* der Teilnahme, oder einer Begünstigung, Strafvereitelung oder Hehlerei verdächtig ist.

Entschieden abgelehnt wird die Empfehlung des Bundesrats,[22] in den Katalog der Verstrickungstaten auch die Geldwäsche aufzunehmen, weil die Konturenlosigkeit des

---

20 BVerfG, Urteil des Ersten Senats vom 27.2.2007 - 1 BvR 538/06, 1 BvR 2045/06 – „CICERO“, Rn. 62, NJW 2007, 1117, 1120.

21 So betreffend Journalisten BVerfG, a.a.O.

22 BR-Drucks. 275/07 (Beschluss), Nr. 1.

Tatbestandes und seine Problematik in Bezug auf Rechtsanwälte und Strafverteidiger nur neue Einfallstore für die Überwachung der Anwaltstätigkeit öffnen würde.

c) Sonderfall: Maßnahmen gegenüber Verteidigern (§ 148 StPO)

Die Verankerung des Beweiserhebungs- und Verwertungsverbots im Hinblick auf Verteidiger in § 53b Abs. 1 StPO-E entspricht im Ansatz dem geltenden Recht, wonach das Verteidigungsverhältnis umfassenden Schutz vor Eingriffen genießt (§ 148 StPO).[23]

Bedenken bestehen gegen den Entwurf jedoch insoweit, als die Einführung einer auch Verteidiger erfassenden allgemeinen, „vor die Klammer gezogenen" Vorschrift (§ 53b StPO) die Frage des Verhältnisses zu § 148 StPO aufwirft und ungeklärt lässt. Nach § 148 StPO darf der Verkehr des Beschuldigten mit seinem Verteidiger nicht behindert werden, er muss insbesondere frei von jeder Überwachung sein. Aus § 148 StPO hat die Rechtsprechung Grundsätze zum Schutz des Verteidigungsverhältnisses hergeleitet, die in verschiedener Hinsicht über den Schutz der Vertrauensverhältnisse des Bürgers zu anderen Berufsgeheimnisträgern hinausgehen.[24] Der Entwurf enthält keine Regelung dazu, dass diese aus dem Rechtsstaatsprinzip hergeleiteten Grundsätze auch durch die Einführung des dem Kernbereichsgedanken verpflichteten § 53b StPO-E nicht tangiert werden und unangetastet bleiben. Diese Unklarheit führt auch zu bedeutsamen praktischen Konsequenzen:

Der Entwurf lässt die gefestigte Rechtsprechung des Bundesgerichtshofes zu § 100a StPO unberücksichtigt, wonach die Überwachung des Fernmeldeverkehrs eines Verteidigers nur zulässig ist, wenn dieser selbst als Täter oder Teilnehmer einer Katalogtat verdächtig ist.[25] Indem § 53b Abs. 1 i.V.m. Abs. 4 StPO-E einen nicht straftat-spezifizierten Beteiligungsverdacht für Ermittlungsmaßnahmen gegen einen Verteidiger als allgemeine Regelung ausreichen lässt, führt er in den praktisch bedeutsamen Fällen der Telefonüberwachung (§ 100a StPO) zu einer nicht hinnehmbaren Ausweitung der Eingriffsbefugnis. Schon die Neuregelung des § 100h Abs. 2 StPO, an die sich § 53b Abs. 4 StPO-E anlehnt, hatte insoweit zurecht zu kritischen Anmerkungen Anlass gegeben.[26] Der Gesetzgeber ist gehalten, die zu § 100a StPO gefestigte Rechtsprechung zu Überwachung des Fernmeldeverkehrs des Verteidigers gesetzlich festzuschreiben und die Zulässigkeit

---

23 Näher LR-*Schäfer*, § 100a Rn. 75 zur Telefonüberwachung.
24 Näher LR-*Schäfer*, a.a.O.
25 BGHSt 33, 347 m. Anm. *Welp* NStZ 1986, 289.
26 LR-*Schäfer*, a.a.O.

solcher Maßnahmen auf Fälle zu beschränken, bei denen der dringende oder hinreichende Verdacht der Täterschaft oder Beteiligung an einer Katalogtat i.S.d. § 100a StPO vorliegt.

Eine allgemeine, den zu § 148 StPO entwickelten Grundsätzen Rechnung tragende Regelung könnte darin bestehen, § 148 StPO in § 53b Abs. 5 StPO-E aufzunehmen, woraus im Gesetz deutlich würde, dass die zu § 148 StPO entwickelten Grundsätze von § 53b StPO-E unberührt bleiben.

Des weitere bestehen gegen den Entwurf insoweit Bedenken, als die in § 53b Abs. 4 StPO-E getroffene Regelung zur Unanwendbarkeit von § 53b Abs. 1 StPO-E in Verstrickungsfällen die Regelung des § 138a StPO unberücksichtigt lässt. Es entspräche der dort getroffene Wertentscheidung des Gesetzgebers, die Schutzwirkungen des § 53b Abs. 1 StPO für Verteidiger erst dann in Wegfall geraten zu lassen, wenn der Verteidiger gemäß § 138a StPO ausgeschlossen worden ist.

d) Verwertungsverbot, Löschungsgebot und gerichtliche Entscheidung (§ 53b Abs. 1 Sätze 2-4 StPO-E)

Ebenso wie bei § 100a Absatz 4 Satz 2 StPO-E ist auch das Beweisverwertungsverbot des § 53b Absatz 1 Satz 2 StPO für das Gesamtkonzept der Neuregelung **unverzichtbar**. Auf die Ausführungen zu § 100a Absatz 4 Satz 2 StPO-E wird verwiesen. Allein ein umfassendes Beweisverwertungsverbot ist geeignet, das Beweiserhebungsverbot des § 53b Absatz 1 StPO-E abzusichern.

Das das Beweiserhebungs- und –verwertungsverbot flankierende Gebot der unverzüglichen Löschung (§ 53b Abs. 1 Satz 3 und 4 StPO-E) ist sachgerecht. Wie bei § 100a Absatz 4 StPO-E ist auch hier eine Klarstellung geboten, dass die erhobenen Daten zum frühestmöglichen Zeitpunkt **ohne schuldhaftes Zögern**, jedenfalls aber spätestens bis zum Abschluss der Ermittlungen (§ 169a StPO) zu löschen sind.

III. Zur Neuregelung der Überwachung der Telekommunikation in § 100a ff. StPO-E

1. Zur Neuregelung der Eingriffsvoraussetzungen in § 100a Abs. 1 und 2 StPO-E

a) Zweck der Neuregelung des § 100a Abs. 1 StPO-E und der Erweiterung des Straftatenkatalogs in § 100a Abs. 2 StPO-E

Die Neustrukturierung des bisherigen § 100a Abs. 1 StPO soll dem Bedürfnis nach rechtsstaatlicher Eingriffsbegrenzung Rechnung tragen. Hierbei bildet der Straftatenkatalog des Abs. 2 das Kernstück und den Bezugspunkt für die neu geschaffenen unbestimmten Rechtsbegriffe des Abs. 1 (*„schwere Straftat …, die …auch im Einzelfall schwer wiegt“*). Zur Neuregelung des Straftatenkatalogs führt die Entwurfsbegründung die Untersuchung von *Albrecht/Dorsch/Krüpe* (2003) an, in der 501 Verfahren aus dem Jahr 1998 auf die Effizienz der Telekommunikationsüberwachung (TKÜ) hin untersucht worden sind. Die TKÜ sei ein wichtiges, erfolgreiches und letztlich unverzichtbares Mittel zur Aufklärung schwerer Kriminalität.[27]

b) Kritik an der Neuregelung des § 100a Abs. 1 StPO-E

Die Neuregelung des § 100a Abs. 1 verdeutlicht, dass zwangsläufig auch unverdächtige Dritte wie z.B. Familienangehörige, andere soziale Bezugspersonen, Arbeitgeber, Abgeordnete, Justizangehörige und auch Unternehmen, sofern sie (auch unwissentlich) irgendeinen Bezug zum Verdächtigen einer Katalogtat haben, von einer Telekommunikationsüberwachung betroffen sein können.

Eine heimliche Ermittlungsmaßnahme, die derart intensiv in die Rechte von Bürgern eingreift, muss nicht nur von schützenden Formen wie dem Richtervorbehalt, ggf. einer Datenmissbrauchsaufsicht[28] und einer (späteren) Benachrichtigungspflicht begleitet werden. Zudem muss die Anlasstat von solchem Gewicht sein, dass der Eingriff angemessen ist.

Der insoweit neu geschaffene Begriff der **„schweren Straftat“** in Absatz 1 Nr. 1 nimmt sowohl auf den Begriff der *„besonders schweren Straftat“* in Art. 13 Abs. 3 S. 1 GG als auch auf die für andere heimliche Ermittlungsmaßnahmen vorausgesetzte Anlasstat *„von erheblicher Bedeutung“* Bezug. Unter den Begriff der *„besonders schweren Straftat“* fallen alle Straftaten mit Höchststrafen von mehr als fünf Jahren Freiheitsstrafe.[29] Eine *„Straftat*

---

[27] BR-Drucks. 275/07, S. 45 f.; dabei reklamiert der Entwurf eine umfassende Berücksichtigung der Entscheidungen des BVerfG, vgl. BVerfGE 107, 299, 322; 109, 279, 346; BVerfG, 1 BvR 668/04, Absatz-Nr. 154, NJW 2005, 2603, 2610 f.

[28] So kennt die Republik Österreich beispielsweise die Kontrolle durch einen unabhängigen Rechtschutzbeauftragten (§§ 149n, 149o ÖStPO).

[29] BVerfGE 109, 279, 347 f.

von erheblicher Bedeutung“ liegt demgegenüber vor, wenn sie mindestens der mittleren Kriminalität zuzurechnen ist, den Rechtsfrieden empfindlich stört und aufgrund ihrer Begehungsform geeignet ist, das Gefühl der Rechtssicherheit bei den Bürgern nachhaltig zu beeinträchtigen.[30] Mit dem neuen Begriff will der Gesetzentwurf auch Straftaten mit einer Höchststrafe von mehr als einem Jahr Freiheitsstrafe erfassen, wenn ein bedeutendes Rechtsgut geschützt wird oder ein besonderes öffentliches Interesse an der Strafverfolgung besteht. Mit dieser Regelung sollen die bisher weitgehend auf *„besonders schwere Straftaten“* (im Wesentlichen organisierte Kriminalität und terroristische Aktivitäten) beschränkten Telefonüberwachungen auf eine Vielzahl weiterer Straftaten ausgeweitet werden.

Dieser Ausweitung des Katalogs setzt der Entwurf in Abs. 1 Nr. 2 als Korrektiv das Erfordernis entgegen, dass die Tat ***„auch im Einzelfall schwer wiegt“***.[31] Allerdings enthält der Gesetzentwurf kein Kriterium dafür, wann das der Fall ist. Die Anordnungsvoraussetzungen sind insoweit ähnlich **unbestimmt** wie diejenigen des § 33a NdsSOG, der vom Bundesverfassungsgericht für nichtig erklärt worden ist. Ungeachtet dessen weist der Entwurf darauf hin, dass es denkbar sei, auch in minder schweren Fällen zunächst eine im Einzelfall schwerwiegende Tat anzunehmen und eine TKÜ anzuordnen, und zwar selbst dann, wenn zunächst ein weder der Tat noch der Teilnahme Verdächtiger ermittelt werden kann. Damit kann auch bei minder schweren Straftaten eine Vielzahl von (unbeteiligten) Personen von der Maßnahme betroffen sein.

Die qualifizierte Subsidiaritätsklausel in **Absatz 1 Nr. 3** des § 100a StPO-E soll sicherstellen, dass die Verhältnismäßigkeitsprüfung im Einzelfall den Anforderungen des Bundesverfassungsgerichts genügt. Angesichts der unbestimmten Weite der Eingriffsvoraussetzungen bestehen Zweifel, dass hierdurch ein wirksames Korrektiv geschaffen wird. Erfahrungsgemäß neigen die Ermittlungsbehörden allzu schnell zu der Annahme, dass eine Aufklärung der Straftat ohne TKÜ nicht möglich ist.

c) Kritik an der Ausweitung des Straftatenkatalogs in § 100a Abs. 2 StPO-E

(1) Die Neuregelung des § 100a Abs. 1 bezeichnet unter Nr. 1 StPO-E die in Abs. 2 katalogartig aufgelisteten Taten als *„schwere Straftaten“*. Tatsächlich ist der Katalog um

---

30 BVerfGE 109, 279, 344.

31 BR-Drucks. 275/07, S. 87 unter Hinweis auf die Entscheidungen des BVerfG in BVerfGE 107, 299, 322 (zu § 100g StPO), in BVerfGE 109, 279, 346 (zu § 100c StPO) und in 1 BvR 668/04, Absatz-Nr. 154, NJW 2005, 2603, 2611 (zum im Nds. SOG verwendeten Begriff der Straftat von erheblicher Bedeutung).

viele Straftaten erweitert worden, die den **Bereichen der mittleren und leichten Kriminalität** zuzurechnen sind, wie ein Blick auf die jeweiligen Strafrahmen zeigt.

Folgende neue Straftaten wurden u.a. in den Katalog aufgenommen:

Neue Straftaten	**Strafrahmen**
Abgeordnetenbestechung gem. § 108e StGB	Geldstrafe oder Freiheitsstrafe bis 5 Jahre
Einfache Fälschung von Zahlungskarten mit Garantiefunktion gem. § 152a Abs. 3 und § 152b Abs. 1 bis 4 StGB	Freiheitsstrafe von 1-10 Jahre
Verbreitung, Erwerb kinderpornographischer Schriften gem. § 184b Abs. 1 und 2 StGB	Freiheitsstrafe von 3 Monaten bis 5 Jahre
Menschenhandel, Förderung des Menschenhandels gem. §§ 232 Abs. 1 und 2, 233 Abs. 1 und 2, 233a StGB	Freiheitsstrafe von 3/6 Monaten bis 5/10 Jahre
Räuberischer Diebstahl gem. § 252 StGB	1 Jahr bis 15 Jahre
Betrug und Computerbetrug im besonders schweren Fall, §§ 263 Abs. 3 Satz 2, Abs. 5, 263a Abs. 2 StGB Gleichgelagert sind besonders schwere Fälle von Subventionsbetrug und Urkundenfälschung	Freiheitsstrafe von 6 Monaten/1 Jahr bis 5/10 Jahre
Bankrott gem. §§ 283a, 283 StGB	Freiheitsstrafe von 6 Monaten bis 10 Jahre
Ausschreibungsabsprachen (Submissionsbetrug) § 298 StGB	Geldstrafe oder Freiheitsstrafe bis 5 Jahre
Bestechung im geschäftlichen Verkehr	Freiheitsstrafe von 3 Monaten bis 5 Jahre

Neue Straftaten	Strafrahmen
gem. §§ 299, 300 Satz 2 StGB	
Bestechlichkeit und Bestechung gem. §§ 332 und 334 StGB	Freiheitsstrafe von 6 Monaten bis 5 Jahre
Bandenmäßige Steuerhinterziehung und Schmuggel, §§ 370 Abs. 3 Satz 2 Nr. 5, 373 AO sowie banden- und gewerbsmäßige Steuerhehlerei, § 374 Abs. 2 AO	Freiheitsstrafe von 3/6 Monaten bis 5/10 Jahre

Gem. § 100a Abs. 1 Nr. 1 sollen auch die **Handlungen zur Vorbereitung** von *„schweren Straftaten“* eine TKÜ-Maßnahme rechtfertigen können, wenn sie selbst eine Straftat darstellen, ohne dass sie im Straftatenkatalog des Abs. 2 im einzelnen aufgeführt werden. Hiervon werden bspw. bei der Geld- und Wertzeichenfälschung Vorbereitungshandlungen i.S.d. § 149 Abs. 1 StGB erfasst, bei der Scheckkartenfälschung Vorbereitungshandlungen nach § 152a Abs. 5 StGB sowie das Sich-Verschaffen von Automatenprogrammen nach § 263a Abs. 3 StGB.

(2) **Besonders problematisch** erscheinen dem Ausschuss

- die Beibehaltung der inzwischen zu einfachen Vergehenstatbeständen herabgestuften Straftaten nach § 34 Abs. 1 bis 3 AWG ;
- die Einbeziehung zahlreicher Korruptionsdelikte (§§ 108e, 298, 299, 300a, 332, 334 StGB) , die typischerweise im Wirtschaftsleben und nicht im Bereich organisierter Kriminalität begangen werden; eine Begründung für die Aufnahme des § 298 StGB in den Katalog fehlt;
- die Einbeziehung von Betrugs- und Bankrottdelikten nach §§ 263, 264, 283a StGB, für die das Gleiche gilt.

Auch der Straftatbestand der Geldwäsche (§ 100a Abs. 2 Nr. 1 m StPO-E) gehört nicht in einen Katalog schwerer Straftaten. Zum einen ist der Strafrahmen des Grundtatbestandes der Geldwäsche (3 Monate bis 5 Jahre) eher niedrig, verglichen mit den anderen Katalogtaten, die bis auf einige Ausnahmen Verbrechenstatbestände sind. Zum anderen kann es im frühen Stadium eines Ermittlungsverfahrens (in dem die Anordnung erfolgt) schwierig sein zu beurteilen, ob es schon um Handlungen geht, die sich auf Vermögenswerte aus abgeschlossenen strafbaren Vortaten beziehen oder noch um Handlungen zur Verwirklichung der Vortat. Das Betäubungsmittelstrafrecht und das Steuerstrafrecht kennen insoweit eine Vielzahl problematischer Fallgestaltungen. Im Betäubungsmittelstrafrecht stellt die Geldwäsche anerkanntermaßen eine straflose Nachtat zu den Tatbestandsvarianten z.B. des Handeltreibens oder der Einfuhr dar. Der Straftatbestand der Geldwäsche kommt hier erst dann zur Anwendung, wenn sich die Beteiligung an der Vortat nicht beweisen lässt oder diese, etwa mangels Verschuldens, nicht strafbar ist.[32] Mittels des Verdachts der Geldwäsche könnten TKÜ-Anordnungen in Fällen getroffen werden, die – wie z.B. der Grundtatbestand des § 29 Abs. 1 Satz 1 BtMG - eine Überwachungsanordnung nicht rechtfertigten, weil sie selbst keine Anlasstat darstellen. Gleiches gilt für die gewerbsmäßige Steuerhinterziehung, die keine Katalogtat darstellt, aber nunmehr Vortat der Geldwäsche nach § 261 StGB werden soll.[33] Damit wird praktisch die „normale“ Steuerhinterziehung in die TKÜ einbezogen, weil sie regelmäßig über mehrere Veranlagungsjahre erfolgt und damit Anlass zum Verdacht von Gewerbsmäßigkeit bietet.

(3) Unabhängig von der Kritik an der vorgesehen Ausweitung des Anlasstatenkatalogs in § 100a Abs. 2 StPO-E hält der Strafrechtsausschuss das Regelungsmodell eines solchen Kataloges gegenüber anderen Regelungsmodellen grundsätzlich für vorzugswürdig.

Das gilt zunächst für den Vorschlag[34] einer Flexibilisierung des Anlasstatenkatalogs in Anlehnung an das Vorbild des § 261 Abs. 1 Satz 2 Nr. 1 StGB. Der Deliktskatalog des § 100a StPO war zwar bislang schon nicht konsistent[35] und wäre es mit den vorgesehenen Neuregelungen noch weniger. Dennoch vermag eine Lösung, die allein oder doch vornehmlich nach der Deliktsschwere differenziert und auf einen Katalog verzichtet, nicht zu überzeugen. Der Gesetzgeber ist gehalten, sich bei jeder potentiellen

---

32 Vgl. *Weber*, BtMG, 2. Auf. 2003, Rn. 532 vor §§ 29 ff.
33 Art. 4 des Entwurfs; Begründung dazu BR-Drucks. 275/07, S. 178.
34 Stellungnahme des Deutschen Richterbundes zum RefE vom Januar 2007, S. 2.
35 *Schäfer*, in: Löwe/Rosenberg, 25. Aufl. (2003), § 100a Rn. 39; *Neuhaus*, FS Rieß, 374 (385); *Kudlich*, JR 2003, 453 (454).

Anlasstat nach § 100a StPO die hohe Bedeutung des Telekommunikationsgrundrechts vor Augen zu führen.[36] Diesem Zweck wird ein ausdifferenzierter Anlasstatenkatalog eher gerecht.

Gleiches gilt für das Modell einer Kombination von abstrakt-generellen und konkret-individuellen Kriterien in § 100a Abs. 2 StPO, wie es sich im Entwurf von Bündnis 90/Die Grünen findet.[37] Nach § 100a Abs. 2 dieses Entwurfs sollen (Nr. 1) überwachungsfähig alle Verbrechen sowie vorsätzliche Vergehen sein, die mit Freiheitsstrafe von mindestens einem Jahr bedroht sind (gemeint sind besonders schwere Fälle eines Vergehenstatbestandes), sowie (Nr. 2) Vergehen, die im Höchstmaß mit Freiheitsstrafe von mindestens fünf Jahren bedroht sind und bei denen „auf Grund der äußeren Umstände" im Falle einer Verurteilung eine Freiheitsstrafe von mindestens einem Jahr zu erwarten ist. Dieser Ansatz dürfte sein Ziel einer restriktiveren Überwachungspraxis – wenn überhaupt – nur um den Preis größerer Rechtsunsicherheit erreichen. Bereits die Definition in § 100a Abs. 2 Nr. 2 dürfte den Kreis der überwachungsfähigen Delikte um Straftaten wie Diebstahl, Unterschlagung anvertrauter Sachen, Begünstigung, Strafvereitelung und Hehlerei erweitern. Der Gesetzgeber ist durch das Rechtsstaatsprinzip zudem verpflichtet, ein Mindestmaß an Vorhersehbarkeit bei der Rechtsanwendung auch im Recht der repressiv-polizeilichen Telekommunikationsüberwachung zu gewährleisten[38]. Ungeklärt bleibt bei diesem Regelungsmechanismus aber, ob der Ermittlungsrichter in einem unter Umständen sehr frühen Stadium des Ermittlungsverfahrens und ohne Kenntnis der Person des Beschuldigten überhaupt zuverlässig die Prognose abgeben kann, die zu erwartende Verurteilung führe zu einer Freiheitsstrafe von mindestens einem Jahr.

2. Zur Neuregelung des Kernbereichsschutzes in § 100a Abs. 4 und 5 StPO-E

a) Unzureichende Regelung des vorgesehenen Beweiserhebungsverbots in § 100a Abs. 4 Satz 1 StPO

Der Strafrechtsausschuss begrüßt die beabsichtigte Übertragung der Vorgaben des Bundesverfassungsgerichts für den Schutz des Kernbereichs privater Lebensgestaltung bei

---

36 Siehe – im Zusammenhang der Frage der Geltung des Art. 19 Abs. 1 Satz 2 GG im Strafprozessrecht – BVerfGE 35, 185 (189) zu § 112a Abs. 1 Nr. 2 StPO.

37 Vgl. den TKÜ-Entwurf der Fraktion Bündnis 90/DIE GRÜNEN, BT-Drucks. 16/3827 v. 13.12.2006. Ähnlich *Stellungnahme des AK Vorratsdatenspeicherung* zum RefE vom 19.1.2007, S. 14 f. (vier Jahre Freiheitsstrafe zu erwarten).

38 Vgl. *Löffelmann*, ZStW 118 (2006), 358 (362 f.); *Gusy*, in: Folgerungen aus dem Urteil des BVerfG zur akustischen Wohnraumüberwachung, (Hrsg.) *Scharr* (2004), 35 (54).

der akustischen Wohnraumüberwachung[39] auf die TKÜ.[40] Wenngleich der Eingriff in die Telekommunikation hinter Maßnahmen der akustischen Wohnraumüberwachung an Intensität regelmäßig zurückbleibt und der Bürger zur höchstpersönlichen Kommunikation nicht in gleicher Weise auf Telekommunikation angewiesen ist wie auf das Refugium seiner Wohnung, fordert die nach Art. 1 Abs. 1 GG und 19 Abs. 2 GG garantierte Unantastbarkeit der Menschenwürde auch im Bereich der Telekommunikationsüberwachung Vorkehrungen zum Schutz individueller Entfaltung im Kernbereich privater Lebensgestaltung,[41] denn Inhalte aus dem Bereich der absolut geschützten Privatsphäre können ebenso am Telefon wie in der Wohnung besprochen werden.

Allerdings verwirklicht die vorgesehene Regelung nach Auffassung des Ausschusses den gebotenen Schutz nicht hinreichend .

Gemäß § 100a Abs. 4 Satz 1 StPO-E hat die Anordnung der Telekommunikationsüberwachung zu unterbleiben, wenn tatsächliche Anhaltpunkte für die Annahme vorliegen, dass durch die Maßnahme allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden. Die Regelung will dem zwingenden Kernbereichsschutz mithin bereits durch ein **Beweiserhebungsverbot** Rechnung tragen. Dies überzeugt im Ansatz. Ein bloßes Beweisverwertungsverbot für Erkenntnisse aus dem Kernbereich höchstpersönlicher Lebensgestaltung würde selbst mit Rücksicht auf die unterschiedlichen Schutzbereiche und Schutzrichtungen von Art. 10 GG einerseits und Art. 13 GG andererseits den Anforderungen des Bundesverfassungsgerichts nicht gerecht werden. Der Kernbereichsschutz muss von Verfassungs wegen **präventiv** wirken und sicherstellen, dass bereits die Erhebung kernbereichsrelevanter Daten weitgehend ausgeschlossen ist[42]. Dies kann ein reines Verwertungsverbot nicht leisten.

Der vorgeschlagene **§ 100a Abs. 4 Satz 1 StPO-E** gewährleistet den notwendigen Schutz des unantastbaren privaten Lebensbereiches jedoch nicht ausreichend, weil die Vorschrift ein Erhebungsverbot nur dann vorsieht, wenn durch die Maßnahme ***„allein“*** Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden.[43] Das Wort „allein“ sollte durch ***„überwiegend“*** ersetzt werden; denn es fragt sich, wann eine ermittlungsrichterliche

---

39 BVerfGE 109, 279 (313 f.). Vgl. auch schon BVerfGE 6, 32 (41); 27, 1 (6); 32, 373 (379); 34, 238 (245); 80, 367 (373).

40 So auch *Löffelmann*, ZIS 2006, 87 (98); *Jahn*, JuS 2006, 946.

41 BVerfGE 113, 348 (391); *Weißer*, GA 2006. 148 (167); *Baldus*, in: Folgerungen aus dem Urteil des BVerfG zur akustischen Wohnraumüberwachung, (Hrsg.) *Scharr* (2004), 9 (15 ff.); krit. *Löffelmann*, AnwBl. 2006, 598 (601); *ders.*, ZStW 118 (2006), 358 (377 ff., 385).

42 Vgl. BVerfGE 109, 279 (318 ff.). A.A. für die präventive Telekommunikationsüberwachung *Gusy*, Nds.VBl. 2006, 65 (69); zweifelnd für den repressiven Bereich noch ders., in: Folgerungen aus dem Urteil des BVerfG zur akustischen Wohnraumüberwachung, (Hrsg.) *Scharr* (2004), 35 (52).

43 So auch *Wolter*, GA 2007, 183, 196.

Prognose dahingehend zu erwarten ist, dass *„allein“* Erkenntnisse aus dem privaten Kernbereich erlangt werden.

Bei Dienst- bzw. Geschäftsanschlüssen werden kaum jemals tatsächliche Anhaltspunkte für die Annahme *ausschließlich* kernbereichsrelevanter Kommunikation vorliegen, zumal (zu Recht) keine Umfeldermittlungen wie bei der akustischen Wohnraumüberwachung vorgesehen sind. Aber auch bei einem ausschließlich „privat“ genutzten Telefonanschluss ist nicht von vornherein anzunehmen, dieser werde einzig und allein zur Führung kernbereichsrelevanter Gespräche verwendet.

Gespräche mit „engsten Vertrauten“[44] werden zwar in der Regel dem höchstpersönlichen Bereich zuzuordnen sein. Doch auch Gesprächen mit diesen Personen kann ein Sozialbezug innewohnen, so dass nach der verfassungsgerichtlichen Rechtsprechung der Kernbereichsschutz entfällt,[45] weil auch in einem intimen Gespräch Informationen über die Anlasstat auftauchen können. Deshalb dürften selbst Gespräch zwischen „Kernbereichspartnern“ abgehört und aufgezeichnet werden, weil die Prognose, dass ausschließlich (allein) kernbereichsspezifische Äußerungen zu erwarten seien, in der Praxis kaum je zu begründen sein wird. In der jetzigen Form handelt es sich bei § 100a Abs. 4 Satz 1 StPO-E daher um ein **Beweiserhebungsverbot ohne Anwendungsbereich.**[46]

Das gilt um so mehr, als ein Abhören in Echtzeit schon wegen des unvertretbaren personellen Aufwandes in der Praxis kaum durchgeführt wird. Daher lässt sich ein wirksamer Kernbereichsschutz nur in der Weise realisieren, dass der Begriff *„allein“* durch ***„überwiegend“*** ersetzt wird. Dies würde bspw. bei der Anwahl der Telefonnummern engster Familienangehöriger trotz des nicht auszuschließenden Sozialbezugs des Gesprächsinhalts die für ein Erhebungsverbot erforderliche *Prognose* der Kernbereichsrelevanz rechtfertigen.

Ob die im präventiv-polizeilichen Bereich bereits praktizierte Richterbandlösung[47]**,** also die Auswertung aufgezeichneter Gespräche allein durch den Ermittlungsrichter (oder von ihm besonders verpflichtete Personen) einen tragfähigen Kompromiss darstellen kann, sollte im weiteren parlamentarischen Verfahren entschieden werden.

---

44 Siehe hierzu *Weißer*, GA 2006, 148 (162 ff.); *G. Haas*, NJW 2004, 3082 (3083).

45 Zutr. *Löffelmann*, ZIS 2006, 87 (91); *Kutscha*, NJW 2005, 20 (22); *Gusy*, in: Folgerungen aus dem Urteil des BVerfG zur akustischen Wohnraumüberwachung, (Hrsg.) *Scharr* (2004), 35 (51).

46 Bezeichnenderweise verzichtet die Entwurfsbegründung, die sonst erfreulich reich an praktischen Beispielen ist, hier auch auf jegliche Exemplifizierung.

47 Vgl. dazu *Löffelmann*, AnwBl. 2006, 598 (601); *ders.*, ZIS 2006, 87 (90) und zu § 29 Abs. 4, 8 POG Rhl.-Pf. *Perne*, DVBl. 2006, 1486 (1489). Zu entsprechenden Forderungen - Durchsicht *nur* durch den Ermittlungsrichter - in den „Tagebuchfällen“ vgl. *Wolter*, StV 1990, 175 (177); *Amelung* NJW 1990, 1753 (1759 f.).

b) Zum Beweisverwertungsverbot des § 100a Abs. 4 Satz 2 StPO-E

Das Beweisverwertungsverbot ist für das Gesamtkonzept der Neuregelung unverzichtbar. Es entspricht den vom Bundesverfassungsgericht aufgestellten Vorgaben[48] und der gefestigten fachgerichtlichen Rechtsprechung[49].

c) Erfordernis einer zeitlichen Präzisierung des vorgesehenen Löschungsgebots in § 100a Abs. 4 Satz 3 StPO-E

Die Regelung entspricht der Forderung des BVerfG, dass Kommunikationsinhalte des höchstpersönlichen Bereichs unverzüglich gelöscht werden müssen, wenn es ausnahmsweise zu ihrer Erhebung gekommen ist. Sie ist eine notwendige Konsequenz des Erhebungsverbotes.

Der Begriff der **Unverzüglichkeit** in § 100a Abs. 4 Satz 3 StPO-E ist in der Rechtsprechung zur akustischen Wohnraumüberwachung[50] nicht eindeutig geklärt und wird auch in der Entwurfsbegründung nicht präzisiert. Dies könnte dazu führen, die Löschung erst nach Beendigung des Verfahrens vorzunehmen. Daher muss klargestellt werden, dass die Löschung **ohne schuldhaftes Zögern**, spätestens aber zum **Abschluss der Ermittlungen** (§ 169a StPO) zu erfolgen hat. Vor der Löschung sind jedoch dem von der Maßnahme betroffenen Beschuldigten und seinem Verteidiger Gelegenheit zur Kenntnisnahme sowie rechtliches Gehör zu gewähren. Den Beschuldigten **entlastende Äußerungen** aus dem Kernbereich dürfen keinesfalls ohne sein rechtliches Gehör „ungehört“ vernichtet werden. Der Persönlichkeitsschutz Dritter – etwa bei Gesprächen zwischen abgehörten mutmaßlichen, aber nicht beschuldigten Nachrichtenmittlern nach § 100a Abs. 3 StPO – bedarf dabei noch einer sorgfältigen Abwägung, die das Interesse des Beschuldigten an einer Entlastung vom Tatvorwurf mit dem Interesse der nicht verdächtigten mutmaßlichen Nachrichtenmittler am Erhalt ihrer Intimsphäre in Einklang bringt.

---

48 S. oben Fn. 36.

49 BGHSt 14, 358 ff.; 19, 325 ff.; 34, 397 (399 ff.); 36, 167 (173 ff.); 44, 46 (48); BGHR StPO § 261 Verwertungsverbot 8, 11; BGH, NStZ 2000, 383.

50 Vgl. BVerfGE 113, 348 (392).

d) Erfordernis eines Beweisverwertungsverbots für Erkenntnisse auf Grund grob fehlerhafter gerichtlicher Anordnungen von TKÜ-Maßnahmen (Vorschlag eines neu einzuführenden § 100a Abs. 5 StPO)

Im Hinblick auf die Ergebnisse rechtstatsächlicher Untersuchungen gerichtlicher Entscheidungen zur Telefonüberwachung[51] ist es rechtsstaatlich geboten, ein **Verwertungsverbot** für Erkenntnisse auf Grund **grob fehlerhafter gerichtlicher Anordnungen** von TKÜ-Maßnahmen einzuführen. Dies würde besser als bisher sicherstellen, dass das Gericht einen Überwachungsantrag sorgfältig prüft und begründet und der Staatsanwalt vor Vollzug einer gerichtlichen Anordnung diese nochmals überprüft.

Als grob fehlerhaft muss man zumindest ansehen[52]

- das Fehlen einer Begründung entgegen § 34 StPO,
- das Fehlen einer Bestimmung über Art, Umfang und Dauer einer Maßnahme entsprechend § 100b Abs. 2 Nr. 3 StPO-E (im Tenor oder in der Begründung),
- das Fehlen von einzelfallbezogenen Ausführungen zu den Anordnungsvoraussetzungen des § 100a Abs. 1 Nr. 1 – 3 StPO-E.

Ein solches Verwertungsverbot könnte als **§ 100a Absatz 5 StPO-E** den vorgelegten Entwurfsregelungen angeschlossen werden. Der Gesetzestext könnte lauten:

„Erkenntnisse aus dem Vollzug grob fehlerhafter gerichtlicher Anordnungen zur Überwachung und Aufzeichnung der Telekommunikation dürfen im Strafverfahren nicht verwertet werden. Gleiches gilt für Erkenntnisse aus dem Vollzug grob fehlerhafter staatsanwaltschaftlicher Anordnungen auf Grund von Gefahr im Verzug (§ 100b Absatz 1),auch wenn sie gerichtlich bestätigt wurden.“

Der Vorschrift des **§ 100g StPO-E** müsste eine gleichartige Bestimmung als Absatz 5 angefügt werden.

---

51 *Albrecht/Dorsch/Krüpe*, Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmethoden, 2003, *Backes/Gusy* u. a., Wirksamkeitsbedingungen von Richtervorbehalten bei Telefonüberwachungen, 2002.

52 Siehe dazu bereits *Strafrechtsausschuss der Bundesrechtsanwaltskammer*, Thesen zum Richtervorbehalt (RS-Nr. 96/2004), These 6.

3. Zur Neuregelung des § 100b Abs. 1 Satz 3 StPO-E

Zu bedauern ist die Neuregelung des § 100b Abs. 1 Satz 3 StPO-E, wonach die Daten aufgrund einer von der Staatsanwaltschaft wegen Gefahr im Verzug getroffenen Anordnung, die nicht richterlich bestätigt wird, verwertet werden dürfen, wenn Gefahr im Verzug tatsächlich bestand. Der Referentenentwurf hatte dem gegenüber ein uneingeschränktes Beweisverwertungsverbot für den Fall vorgesehen, dass die aufgrund (vermeintlicher) Gefahr im Verzug getroffene staatsanwaltschaftliche Anordnung nicht binnen drei Werktagen vom Ermittlungsrichter bestätigt wird. Dadurch wäre die gerichtliche Kontrolle zeitlich vorverlagert worden. Dies hätte dem auf effektiven Grundrechtsschutz im Ermittlungsverfahren bedachten Konzept besser entsprochen und ist auch wegen der Sachnähe des Ermittlungsrichters vorzugswürdig. Seine Stellung im Ermittlungsverfahren würde dadurch gestärkt.[53]

[53] Siehe dazu *Strafrechtsausschuss der Bundesrechtsanwaltskammer*, Thesen zum Richtervorbehalt (RS-Nr. 96/2004). Kritisch zum status quo ermittlungsrichterlicher Kontrolle auch BVerfG (*3. Kammer des 2. Senats*), NJW 2005, 275 (276); *Lilie*, ZStW 111 (1999), 807 (814); *Schünemann*, ZStW 114 (2002), 1 (20); *Heghmanns*, GA 2003, 433 (440). S. auch BT-Drucks. 16/1421 v. 10.5.2006, S. 4 (unter 3.).

IV. Zur vorgesehenen sog. Vorratsdatenspeicherung (§§ 113a, 113b TKG-E) und deren Verwendung zur Strafverfolgung (§ 100g StPO-E)

Durch Einfügung der §§113a, 113b TKG-E und weitere Änderungen des Telekommunikationsgesetzes (TKG) soll für die Anbieter von Telekommunikationsdienstleistungen eine Pflicht zur Speicherung sämtlicher Verkehrs- und Standortdaten für einen Zeitraum von 6 Monaten geschaffen werden (sog. Vorratsdatenspeicherung). Zugleich soll durch Änderung des § 100g StPO-E eine umfassende Befugnis zur Erhebung solcher Daten für die Strafverfolgung geschaffen werden.

Der Strafrechtsausschuss lehnt die vorgesehenen Regelungen ab, weil sie den verfassungsrechtlich gebotenen Begrenzungen von Eingriffen in das Grundrecht auf ungestörte Telekommunikation (Art. 10 GG) und in das Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) insgesamt nicht gerecht werden.

Die nachfolgende Begründung erläutert zunächst die vorgesehenen Regelungen. Hierbei wird deutlich, dass die vorgesehene Pflicht zur Speicherung von Verkehrs- und Standortdaten weit über die bestehende Pflicht zur Speicherung von Kundendaten (§ 111 TKG) hinausgeht und – ohne jeden Verdacht oder sonstigen Anlass - ein umfassendes „Bewegungsbild“ eines Menschen über den Zeitraum eines halben Jahres schafft. Das ist bereits für sich genommen ein intensiver Eingriff in die genannten Grundrechte, der im geltenden Recht ohne Vorbild ist. Zudem ist eine Beschränkung der Verwendung für die Strafverfolgung nicht gesichert. Mit Blick auf die einschlägige Rechtsprechung des Bundesverfassungsgerichts bezweifelt der Strafrechtsausschuss die Verfassungsmäßigkeit eines solchen Eingriffs.

Sofern eine verdachts- und anlassunabhängige Vorratsdatenspeicherung überhaupt verfassungsgemäß ist, wäre für die Erhebung solcher Daten zur Strafverfolgung die gleiche Schwelle wie für die Erhebung von Inhaltsdaten zu fordern.

1. Zu den vorgesehen Änderungen des Telekommunikationsgesetzes (TKG)

a) Inhalt und Tragweite der sog. Vorratsdatenspeicherung (§§ 113a, 113b TKG-E)

Nach Art. 2 RegE sollen durch (erneute)[54] Änderung der §§ 96, 97, 110-112, 115, 149 und Einfügung der §§ 113a, 113b TKG-E die TK-Anbieter für Zwecke der Strafverfolgung[55] zu einer Vorratsspeicherung der in § 96 TKG bezeichneten Verkehrsdaten für die Dauer von mindestens sechs Monaten verpflichtet werden. Außerdem wird für Zwecke der in § 112 Abs. 2 TKG aufgeführten Behörden[56] das bereits bestehende automatisierte Abrufverfahren in Bezug auf Personen- und Anschlussdaten um die Gerätedaten von Mobiltelefonen, E-Mail –Adressen sowie die Daten ihrer Inhaber und Provider erweitert[57].

Vor allem mit der sog. Vorratsdatenspeicherung greift der Gesetzentwurf tief in die Betriebsführung aller Unternehmen ein, die Telekommunikationsdienste erbringen oder daran mitwirken, das sind sämtliche Anbieter von Festnetz- und Mobiltelefonie sowie von Internetdienstleistungen. Auch andere öffentliche Daten- und Providerdienste[58] einschließlich solcher von E-Mail-Dienstleistungen sind davon betroffen. Zur Begründung für diese Gesetzesänderung verweist der RegE insbesondere auf die Richtlinie 2006/24/EG.

Durch die Pflicht zur sog. Vorratsdatenspeicherung wird im Zusammenwirken mit der bereits bestehenden Pflicht zur dauerhaften Speicherung aller Bestandsdaten sowie der anlassbezogenen Speicherpflicht zur Überwachung ein vollständiges **„Bewegungsbild" eines TK-Kunden** geschaffen. Nach den nach §§ 113a, 113b TKG-E zu speichernden Verbindungs-, Übertragungsprotokoll- und Standortdaten beim TK-Anbieter zu Zwecken der Strafverfolgung wird eine Tatsachengrundlage im Regelungsbereich der bisherigen §§ 100g und 100i StPO geschaffen. Die Datenspeicherung aller bei einem Verbindungsaufbau in Anspruch genommenen TK-Daten (außer Inhaltsdaten, § 113a Abs. 8 TKG-E) wenigstens auf eine Zeit von sechs Monaten[59] erlaubt weit über die bislang erreichbaren gegenwartsbezogenen Bestandsinformationen hinaus eine Rekonstruktion der Vergangenheit. Ein solcher Datenbestand ermöglicht die Rückverfolgung der Datenentstehung, -verarbeitung, -speicherung und –abrechnung auf wenigstens sechs

---

55 Ausdrücklich § 113a Abs. 1 Satz 1 TKG-E; eine vergleichbar allgemeine Zwecksetzung findet sich in § 100 Abs. 3 TKG (Datenspeicherung zur Aufdeckung von Leistungserschleichungen und sonstigen rechtswidrigen Inanspruchnamen), § 110 TKG (technische Umsetzung von Überwachungsmaßnahmen) und §§ 111, 112, 113 TKG (Abrufverfahren für Strafverfolgung, Gefahrenabwehr und Verfassungsschutz).

56 Z.B. Polizei-, Justiz- und Verfassungsschutzbehörden sowie die BAFin.

57 Siehe §§ 111 Abs. 1 - 5, 112 Abs. 1 , 115 Abs. 2, 149 Abs. 1 Nrn. 29-30a TKG-E.

58 Vgl. dazu die Stellungnahme der Bundesrechtsanwaltskammer vom Januar 2007 an das BVerfG in der Sache 2 BvR 902/06; Strafrechtsausschuss – RS-Nr. 56/2007.

59 Hinzu kommt ein weiterer Monat, wenn der TK-Anbieter die Zeit für die Löschungsverpflichtung nach § 113a Abs. 11 TKG-E ausnutzt.

Monate. Der Eingriff ist nach der bestehenden Rechtslage nur vergleichbar mit der langfristigen und vollständigen Speicherung von Mautdaten oder den Daten aus Kameraüberwachungen auf öffentlichen Plätzen oder in öffentlichen Einrichtungen, wobei diese Speicherungen nicht einmal personenbezogen erfolgen.

Mit einer solchen anlassunabhängigen Speicherpflicht kann zum einen eine wirksame Grundlage für Ermittlungen gegen den **TK-Anbieter** geschaffen werden. Vorstellbar sind beispielsweise Ermittlungen wegen Abrechnungsbetruges, wegen strafbarer Wettbewerbs- und Kartellverstöße, wegen Unterstützen oder Unterhalten von illegalen Websites wie auch wegen der Nutzung von Internet- und Telefondiensten für Straftaten, wie sie in der jüngsten Vergangenheit von Staatsanwaltschaften im Bundesgebiet geführt worden sind.

In gleicher Weise ermöglicht dieser umfassende Datenbestand Ermittlungen gegen **jeden einzelnen TK-Kunden** für jegliche strafrechtliche und strafprozessuale Zwecksetzung. Damit mögen eine Vielzahl von Deliktsbereichen der terroristischen und der organisierten Kriminalität erfasst werden, es sind aber auch Aufklärungshilfen für die sog. Cyber-Kriminalität, Internet-Pornographie, Stalking, Computersabotage, Phishing, Hacking oder andere Delikte der mittleren und – in Einzelfällen auch – der Bagatellkriminalität zu erwarten. Die Ausweitung des Angebotsspektrums mittels Telekommunikation ist ungebrochen und dürfte auch in Zukunft viele Novationen hervorbringen, die insbesondere von Jugendlichen und Heranwachsenden gerne genutzt werden. Ein umfassend gespeicherter Datenbestand lässt eine Umfeldrecherche zu, die eine unüberschaubare Vielzahl sozialer oder familiärer Kontakte einbezieht, für die Berührungspunkte mit einer etwaigen strafrechtlichen Betätigung zumindest zweifelhaft sind.

Die Datenspeicherung und Auskunftserteilung soll völlig **von der Kenntnis des TK-Kunden gelöst** werden. Der private Nutzer der Telekommunikation darf nicht über Abfragen im automatisierten Verfahren oder bei manuellen Auskunftsersuchen unterrichtet werden (§ 113 Abs. 1 S. 4 TKG, § 113b Satz 2 TKG-E).

b) Erweiterung der Speicherungsverpflichtungen in § 111 TKG-E

Für **Auskunftsersuchen der Sicherheitsbehörden** (§ 111 TKG-E) soll die bisher schon bei jedem TK-Anbieter eingerichtete Kundendatenbank mit Informationen über jeden Anschlussinhaber, Telefonnummern, Anschrift und Geburtsdatum um Gerätedaten eines Mobiltelefons, E-Mail-Adressen sowie deren Inhaber und Provider erweitert werden. Damit würden sämtliche verkauften Mobiltelefone, deren Karten- und Gerätekennung wie auch alle elektronischen Postfächer, die von Telekommunikationsdienstleistern eingerichtet und

verwaltet werden, in einer automatisch abrufbaren Datenbank registriert sein. Für ausländische Mobilfunkbetreiber wird das die zusätzliche Frage aufwerfen, ob sie den Meldepflichten jedenfalls für deutsche Anschlusskunden genügen müssen. Die Regulierungsbehörde darf diese Daten jederzeit ohne Nachricht an den TK-Anbieter **automatisch abrufen** (§ 112 TKG-E). Indem auch der Abruf von Daten mittels einer „Ähnlichenfunktion“ ermöglicht werden soll, wird die Ausweitung der automatischen Auskunft über Dritte, die nicht von dem eigentlichen Vorgehen betroffen sind, ermöglicht. Benachrichtigungs- oder Löschungspflichten sind nicht vorgesehen.

Die gesetzlichen Regelungen zu **manuellen Auskunftsersuchen** in § 113 TKG bleiben unberührt, so dass die einzelfallbezogenen Auskunftsersuchen zu Zwecken der Strafverfolgung, der Gefahrenabwehr und des Verfassungsschutzes bzw. des MAD in vollem Umfang aufrechterhalten werden.

c) Verwendungsmöglichkeit der sog. Vorratsdaten (§ 113b TKG-E)

Sämtliche nach den §§ 95, 96, 113a, 111, 112 TKG-E gespeicherten Daten dürfen auf Anfrage der Ermittlungsbehörden für Zwecke der Strafverfolgung, der Abwehr erheblicher Gefahren und zur Aufgabenerfüllung der Geheimdienste unverzüglich übermittelt werden (§ 113b S. 1 TKG-E). Die Anfragebefugnis und das zu beachtende Verfahren darüber ergeben sich nicht aus dem TKG, sondern aus den Neuregelungen der StPO (§§ 100g, 100i StPO) sowie einigen Bundesgesetzen über das BKA, den Zollfahndungsdienst, die BAFin (WpHG) und den Verfassungsschutzgesetzen bzw. dem MAD-/BND-Gesetzen.

Eine sonstige Datenverwendung ist untersagt (§ 113b S. 1 letzter Halbsatz TKG-E). Über die Datenübermittlung muss nach dem TKG-E **keine Dokumentation** geführt werden. Der abgefragte Datenbestand muss **nicht aufbewahrt** werden. Jegliche Datenverwendung bei dem Datenempfänger regelt das jeweilige Ermächtigungsgesetz, wobei er – sofern er nicht aus anderen Gründen dem TKG unterliegt – die kunden- und datenschützenden Regelungen des TKG nicht anwenden muss.

2. Überblick über die einschlägige Rechtsprechung des Bundesverfassungsgerichts

Eine staatliche Vorratsdatenspeicherung ohne konkreten Anlaß für eine erst nachträglich konkretisierte Zwecksetzung greift in die Grundrechte auf ungestörte, staatlich nicht

überwachte Telekommunikation (Art. 10 Abs. 1 GG) und auf informationelle Selbstbestimmung des Grundrechtsträgers (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) ein. Das BVerfG hat das in einem Fall der Datenspeicherung auf einem Mobiltelefon, den Abruf dieser Daten und deren Verwendung im Strafverfahren mit Beschluss vom 12.03.2003 so entschieden: *„Insofern genügt es verfassungsrechtlichen Anforderungen nicht, dass die Erfassung der Verbindungsdaten allgemein der Strafverfolgung dient. Vorausgesetzt sind vielmehr eine Straftat von erheblicher Bedeutung, ein konkreter Tatverdacht und eine hinreichend sichere Tatsachenbasis“*.[60]

Mit Urteil vom 12.04.2005 hat das BVerfG die Verfassungsbeschwerde gegen den Einsatz von GPS in einem strafrechtlichen Fall auf der Grundlage des § 100c Abs. 1 Nr. 1b StPO zurückgewiesen. Auch wenn er die Ermächtigungsgrundlage als ausreichend erachtete, hat der 2. Senat betont, dass es sich jeweils nur um eine Einzelmaßnahme handeln darf, dass die Staatsanwaltschaften durch Information und Dokumentation aller Maßnahmen ein Übermaß der staatlichen Eingriffe zu vermeiden haben und dass sicherzustellen ist, dass der Eingriff auf den notwendigen Mindestumfang begrenzt wird.[61]

Für die präventive polizeiliche Telefonüberwachung „als Vorsorge für die zukünftige Strafverfolgung“ hat der 1. Senat des BVerfG mit Urteil vom 27.07.2005 eine präventiv-polizeiliche Regelung für Vorratsdatenspeicherung nach § 33a des damaligen NdsSOG für nichtig erklärt. Dem Landesgesetzgeber stand nach der Erkenntnis des BVerfG keine Gesetzgebungsbefugnis zu. Darüber hinaus hat der Senat für etwaige bundesgesetzliche Regelungen Vorgaben gemacht, an denen sich auch der jetzige Entwurf [62] orientieren muss: [63]

.

- Die anlassunabhängige Vorratsdatenspeicherung fällt in den Schutzbereich des Art. 10 Abs. 1 GG, weil sich staatliche Stellen ohne Zustimmung der Beteiligten Kenntnis vom Inhalt und den Umständen des fernmeldetechnisch vermittelten Kommunikationsvorgangs verschaffen können.[64] Nicht nur die Speicherung an sich,

---

60 BVerfG zur Handy-Überwachung, 1 BvR 330/96 vom 12.3.2003, NJW 2003, 1787 (1791), = BVerfGE 107, 299, Abs. 75, 78.

61 BVerfG, 2 BvR 581/01, Urteil vom 12.4.2005, Abs. 62-64, BVerfGE 112, 304, 320.

62 Der Entwurf erwähnt die Entscheidung sowohl in der allgemeinen Begründung, S. 44/45, als auch in der Begründung zu § 100a StPO-E, S. 85.

63 BVerfG, 1 BvR 668/04, Urteil vom 27.7.2005, NJW 2005, 2603 ff., Abs. 81; vgl. auch BVerfGE 100, 313 <358>; 106, 28 <37>; 107, 299 <313>; 110, 33 <52 f.>

64 BVerfG a.a.O. Abs. 82; vgl. BVerfGE 100, 313 <366>; 107, 299 <313>

sondern auch die Datenverarbeitung für unterschiedliche Zwecke als dem ursprünglichen Erhebungszweck stellt einen Eingriff in das Grundrecht dar.[65]

- Die Eingriffsnormen müssen bestimmt sein und einen gesetzlich klar normierten Umfang der Datenspeicherung, Datenübermittlung, Datenverarbeitung und Datenverwendung haben. Die Kriterien, die für die Gefahrenabwehr (eine konkrete Gefahrenlage) oder die Strafverfolgung (bereits verwirklichte Straftaten) entwickelt worden sind, genügen nicht für eine Vorfeldspeicherung.[66] Den spezifischen Bestimmtheitsanforderungen genügt ein Gesetz, das die Vorsorge für die Verfolgung künftiger Straftaten oder die Verhütung vor Straftaten beabsichtigt, nur, wenn der Eingriff sich auf mögliche auffällige Verhaltensumstände bezieht. Die Norm muss handlungsbegrenzende Tatbestandselemente enthalten, die einen Standard an Vorhersehbarkeit und Kontrollierbarkeit vergleichbar dem schaffen, der für die Aufgaben der Gefahrenabwehr und der Strafverfolgung geboten ist.[67] Dem genügten jedenfalls die Eingriffsschwellen „Straftaten von erheblicher Bedeutung“ oder die „Unerlässlichkeit“ der Maßnahme nicht.

- Es muss ein angemessener Ausgleich für den heimlichen Eingriff und die damit verbundene Wehrlosigkeit des Einzelnen geschaffen werden. Der Richtervorbehalt ist dazu grundsätzlich geeignet, er kompensiert aber nicht unverzichtbare Bestimmtheitsdefizite.

- Um dem Grundsatz der Verhältnismäßigkeit genügen zu können, muss eine gesetzliche Regelung einen angemessenen Ausgleich zwischen dem Allgemein- und dem Individualinteresse herstellen. Dabei spielt die Anzahl der betroffenen Bürger, die Auswahl der Grundrechtsträger, die Gestaltung der Einschreitschwellen und die Intensität der Beeinträchtigungen eine Rolle.[68] Das BVerfG urteilte: *„…Im Bereich der Telekommunikationsüberwachung ist von Bedeutung, ob die Betroffenen als Personen anonym bleiben, welche Informationen erfasst werden können und welche Nachteile den Grundrechtsträgern aufgrund der Überwachungsmaßnahme drohen oder von ihnen nicht ohne Grund befürchtet werden. Auf Seiten der mit dem Eingriff verfolgten Zwecke ist das Gewicht der Ziele und Belange maßgeblich, denen die Telekommunikationsüberwachung dient. Es hängt unter anderem davon ab, wie bedeutsam die Rechtsgüter sind, die mit Hilfe der Maßnahme geschützt werden*

65 BVerfG a.a.O., Abs. 83 zu den Verwendungsmöglichkeiten nach §§ 38 ff. NdsSOG.
66 BVerfG a.a.O., Abs. 120
67 BVerfG a.a.O., Abs. 121; vgl. BVerfGE 110, 33/56.
68 BVerfG a.a.O., Abs. 136.

sollen, und wie wahrscheinlich der Eintritt einer Rechtsgutverletzung ist (vgl. BVerfGE 100, 313 <375 f.>).“

- Eingriffe zu Zwecken der Strafverfolgung und der Gefahrenabwehr müssen die betroffenen Rechtsgüter abwägen. Allerdings muss stets gewährleistet bleiben, dass Annahmen und Schlussfolgerungen einen konkret umrissenen Ausgangspunkt im Tatsächlichen haben. Bei einem geringen Gewicht des gefährdeten Rechtsguts steigen die Anforderungen an die Prognosesicherheit sowohl hinsichtlich des Grads der Gefährdung als auch hinsichtlich ihrer Intensität.[69] Der Senat entschied: *„…Knüpft das Gesetz nicht einmal an Planungs- oder sonstige Vorbereitungshandlungen an - wie in der früheren Regelung des § 39 Abs. 2 AWG oder jetzt in § 23a Abs. 2 und 3 ZFdG -, sondern begnügt es sich mit nicht näher eingegrenzten Tatsachen, die die Annahme einer künftigen Straftat rechtfertigen, steigen die Anforderungen an das Gewicht des Schutzguts und die Gefährlichkeit der erwarteten Verletzungshandlung weiter. Der schwere Eingriff in das Telekommunikationsgeheimnis kann bei einer derart weiten und offenen Umschreibung der Voraussetzungen der Vorsorge für die Verfolgung und der Verhütung künftiger Straftaten nur dann als angemessen bewertet werden, wenn der zu schützende Gemeinwohlbelang allgemein sowie im konkreten Fall überragend wichtig ist.“*[70]

- Schließlich muss ein Ausgleich durch eine notwendige Benachrichtigung des Betroffenen geschaffen werden. Eine lange Zurückstellung der Benachrichtigung führt zu einer Gefährdung des effektiven Rechtsschutzes und damit zur Intensivierung des Eingriffs. Schließlich sind angemessene Regelungen zum Schutz des absoluten Kernbereichs privater Lebensgestaltung vorzusehen.[71]

In der Folgezeit hat das Bundesverfassungsgericht diese Anforderungen bestätigt. In der Entscheidung vom 04.04.2006 hat es eine anlassunabhängige Rasterfahndung für verfassungswidrig erklärt und „das außerhalb statistischer Zwecke bestehende strikte Verbot der Sammlung personenbezogener Daten auf Vorrat“ ausgesprochen.[72]

Im Falle des IMSI-Catchers sieht das BVerfG die Eingriffsschwelle des § 100i StPO gerade noch als verfassungsgemäß an .[73] Die dort noch maßgebliche Überlegung war, dass die

---

69 BVerfG a.a.O., Abs. 149.
70 BVerfG a.a.O., Abs. 150.
71 BVerfG a.a.O., Abs. 157-159.
72 BVerfG, 1 BvR 518/02 vom 4.4.2006, NJW 2006, 1939 (1943), Abs. 105.
73 Beschluss vom 22.08.2006, 2 BvR 1345/03

Gerätedaten nicht mehr der Kommunikation zwischen Menschen zuzuordnen sind, sondern ausschließlich gerätebezogene Funkdaten enthalten (Abs. 57). Da in den Neuregelungen aber eine Kombination aller Daten vorgesehen ist, mithin Bestands- und Gerätedaten, die ohne vorherige richterliche Erlaubnis oder zur Eigensicherung abgefragt werden können mit solchen Daten, die als Vorratsdaten zu speichern sind, kombiniert werden können, wird das erneut die Frage der Eingriffstiefe und der Verhältnismäßigkeit aufwerfen.

Bei dem Bundesverfassungsgericht ist derzeit noch eine Verfassungsbeschwerde[74] gegen die bereits bestehenden Vorschriften des Telekommunikationsgesetzes (§§ 95 Abs. 3, 111-113 TKG), die eine Bevorratung von personenbezogenen Daten zum automatisierten Abruf vorsehen, anhängig. Eine Entscheidung steht noch aus.

Des weiteren ist eine Rechtsbeschwerde der Republik Irland gegen die EU-Richtlinie zur Vorratsdatenspeicherung anhängig. Am 30.05.2006 hatte der Europäische Gerichtshof EG-Rechtsakte für nichtig erklärt, welche die Übermittlung von Fluggastdaten in die USA genehmigten.[75] Zur Begründung führte der Gerichtshof an, es handele sich um „eine Datenverarbeitung, die nicht für die Erbringung einer Dienstleistung erforderlich ist, sondern zum Schutz der öffentlichen Sicherheit und zu Strafverfolgungszwecken als erforderlich angesehen wird.“[76] Für den Bereich der öffentlichen Sicherheit und der Strafverfolgung sei die Europäische Gemeinschaft nicht zuständig. Dies gelte auch dann, wenn eine Harmonisierung unterschiedlicher Regelungen in den Mitgliedsstaaten angestrebt werde. Die zum RefE vorgelegten Stellungnahmen weisen auf Zweifel an der Rechtmäßigkeit der RL hin.[77]

3. Kritik an den vorgesehenen Änderungen des TKG

Die verdachtslose systematische Protokollierung des Kommunikationsverhaltens jedes Bürgers für Zwecke der Strafverfolgung ist bereits ein Eingriff in das Fernmeldegeheimnis, der den vom Bundesverfassungsgericht aufgestellten Anforderungen genügen muss. Durch die Vorratsdatenspeicherung bleiben die Verkehrsdaten nicht auf den flüchtigen, vorübergehenden Zweck begrenzt, sondern sie verselbständigen sich zu einem begehrten Zugriffsobjekt, besonders wenn es um die Herstellung von Bewegungsbildern, Kommunikationskontakten oder Kommunikationsnetzen der TK-Nutzer geht. Weit über die

---

74 BVerfG, 1 BvR 1299/05.
75 EuGH, Urteil vom 30.5.2006, Az. C-317/04 und C-318/04.
76 EuGH, Urteil vom 30.5.2006, Az. C-317/04 und C-318/04 Abs. 57.
77 Vgl. auch *Gauben*, DRiZ 2007, 33 ff.

Strafverfolgung, die Gefahrenabwehr und den Verfassungsschutz hinaus weckt ein solcher Datenbestand **Begehrlichkeiten**, sei es zur Forschung und Entwicklung, sei es zur Konsumforschung und -förderung einschließlich der Produktvermarktung über Telefon und Internet.

Aus den gespeicherten Daten über das Kommunikations- und Bewegungsverhalten lassen sich **sensible Informationen** über das Privat- und Intimleben ablesen. Erfahrungsgemäß kommt es immer wieder zur unbefugten Offenlegung vertraulicher Daten durch Mitarbeiter des speichernden Unternehmens, Mitarbeiter der Eingriffsbehörden oder Unbefugte („Hacker"). Die Offenlegung der Kommunikationsdaten etwa von Prominenten kann schwerwiegende Folgen nach sich ziehen und auch für kriminelle Handlungen wie Erpressung oder politische Zwecke genutzt werden. Eine Vorratsdatenspeicherung beeinträchtigt ferner berufliche Aktivitäten (z.B. in den Bereichen Medizin, Recht, Kirche, Journalismus) ebenso wie politische und unternehmerische Aktivitäten, die Vertraulichkeit voraussetzen. Wenn jeder Kontakt etwa zu Berufsgeheimnisträgern, Journalisten oder Abgeordneten nachvollzogen werden kann, werden Menschen, die ein Bekanntwerden ihres Kontakts vermeiden möchten, eine Kontaktaufnahme unterlassen. Bei befürchteten Repressalien, bestimmten Krankheiten oder strafrechtlichen Vorwürfen wollen die Betroffenen ein Bekanntwerden oft um jeden Preis vermeiden. Selbst wenn sie sich trotz der Vorratsdatenspeicherung nicht von einer Kontaktaufnahme abschrecken lassen, höhlt die Datenspeicherung das Arzt- und Anwaltsgeheimnis sowie den Quellenschutz von Journalisten aus. Die Vorratsdatenspeicherung führt zu Kommunikationsstörungen und Verhaltensanpassungen. Sie steht damit dem Grundrecht des Einzelnen, sich frei von Beobachtung durch staatliche oder quasi-staatliche Stellen zu entfalten, entgegen.

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

Mit der Aufspaltung der Speicherpflichten in einem fortgeschriebenen TKG und die Zugriffsrechte darauf in den strafprozessualen und bundespolizeilichen Regelungen wird

eine Vorlage für landespolizeiliche Zugriffsrechte für die Gefahrenabwehr und den Verfassungsschutz geschaffen. Die Normwirkung der vorgesehenen Änderungen des TKG und der StPO erfüllen dabei nicht die Anforderungen an die Urteile des BVerfG vom 27.07.2005 und vom 02.03.2006.

- Die Speicherpflicht „zu Zwecken der Strafverfolgung“ ist **unbestimmt**. Da schon die Speicherpflicht einen Eingriff in das Fernmeldegeheimnis darstellt, wäre im TKG unter den gleichen Voraussetzungen wie in der StPO oder den Polizeigesetzen eine hinreichend bestimmte, anlassbezogene, klare und kontrollierbare Regelung zu schaffen, die zu einer differenzierten langfristigen Speicherung von Teilnehmerdaten führt. Gerade der Zugriff auf solche Daten für die Aufklärung mittlerer und punktuell sogar einfacher Kriminalität bedarf der Begrenzung gegenüber dem Kernbereich privater Lebensgestaltung. Dem verfassungsrechtlichen Verhältnismäßigkeitsgebot ist nicht ausreichend Rechnung getragen.

- Schon die Datenspeicherung bei gewerblichen, nichtstaatlichen Einrichtungen für staatliche Zwecke müsste durch eine unabhängige, regelmäßige und effektive justizielle Aufsicht überwacht werden. Dann erfordert erst recht der Umgang (Verarbeitung, Speicherung, Übertragung, Löschung) solcher Daten auf Justizeinrichtungen eine solche Datenkontrolle. Weder die im Dezember 2006 neu in das TKG aufgenommenen Datenschutzvorschriften zugunsten der Kunden noch die Schutznormen des BDSG stellen eine solche Aufsicht sicher, da sie nicht auf die Beachtung der neuen Abfragemöglichkeiten und der Verwendungsbeschränkungen der Ermittlungsbehörden ausgerichtet sind.

- Es muss ein effektiver Ausgleich für die bei der Datenübermittlung fehlende Benachrichtigung geschaffen werden, um eine nachträgliche Kontrolle des Betroffenen zu ermöglichen.

Fazit: Die neu vorgesehenen Regelungen über die Pflicht zur Speicherung von Verkehrs- und Standortdaten werden – insbesondere im Zusammenhang mit der vorgesehenen Befugnis zur umfassenden Erhebung solcher Daten für die Strafverfolgung und andere Zwecke – den verfassungsrechtlich gebotenen Begrenzungen von Eingriffen in das Grundrecht aus ungestörte Telekommunikation (Art. 10 GG) und das Grundrecht auf informationelle Selbstbestimmung (Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 GG) insgesamt nicht gerecht und vom Strafrechtsausschuss daher abgelehnt.

4. Zur vorgesehenen Änderung des § 100g Abs. 1 StPO-E

Der Entwurf setzt die Eingriffsschwelle für die Erhebung von Verkehrsdaten (§ 100g StPO-E) im Verhältnis zur Erhebung von Inhaltsdaten (§ 100a StPO-E) niedriger an. Während für die Inhaltsdatenerhebung der Verdacht schwerer Straftaten erforderlich ist, (die dann in § 100a Abs. 2 StPO-E enumerativ aufgezählt sind), soll für die Verkehrsdatenerhebung eine „Straftat von auch im Einzelfall erheblicher Bedeutung, *insbesondere* eine in § 100a Abs. 2 bezeichnete Straftat“ ausreichen, also auch eine in § 100a Abs. 2 StPO-E unerwähnte Nichtkatalogtat, wenn sie nur im konkreten Einzelfall „erhebliche Bedeutung“ hat. Das ist einerseits begrüßenswert, weil nicht mehr wie bisher missverständlich auf den abstrakten Schweregrad einer Straftat abgestellt wird, sondern auf den konkret-individuellen Schweregrad und somit ein Gleichklang mit der Telekommunikationsüberwachung nach § 100a Abs. 1 Nr. 2 StPO-E („wenn die Tat auch im Einzelfall schwer wiegt“) hergestellt wird. Während § 100a Abs. 1 Nr. 1 StPO-E jedoch *kumulativ* den konkret-individuellen Schweregrad der abstrakten Katalogtat fordert, verzichtet § 100g StPO-E bei der Verkehrsdatenerhebung auf eine solche Kumulation und lässt Alternativität ausreichen, so dass auch Nichtkatalogtaten bei individueller Schwere die Verkehrsdatenerhebung ermöglichen. Misslich ist dabei die unterschiedliche Wortwahl des Gemeinten („Tat auch im Einzelfall schwer wiegt“ in § 100a Abs. 1 Nr. 2 StPO-E gegenüber „Straftat von auch im Einzelfall erheblicher Bedeutung“ in § 100g Abs. 1 Nr. 1 StPO-E). Unverständlich ist auch, dass nur bei Straftaten *mittels* Telekommunikation eine Subsidiaritätsklausel vorgesehen ist, wonach die Maßnahme voraussetzt, dass die Erforschung des Sachverhaltes auf andere Weise aussichtslos wäre, nicht aber bei allen anderen Straftaten. Gerade bei Straftaten, die mittels Telekommunikation begangen werden, ist typischerweise die Erforschung des Sachverhalts auf andere Weise aussichtslos, so dass die Subsidiaritätsklausel ins Leere läuft. Abgesehen von Fällen des Stalkings per Telefon ist bei den meisten Delikten, die *mittels* Telekommunikation begangen werden, eine anderweitige Erforschung des Sachverhalts als mildere Maßnahme kaum denkbar. Die Verbreitung von Kinderpornographie mittels Internet kann regelmäßig *allein* durch Verkehrsdatenüberwachung ermittelt werden, so dass die Subsidiaritätsklausel immer ins Leere läuft. Ihre gute Berechtigung hat sie vor allem bei Delikten, die möglicherweise auch mittels Telekommunikation begangen werden oder durch Telekommunikationsüberwachung nachgewiesen werden können. Dort hat die Subsidiaritätsklausel ihren berechtigten Platz.

Offenbar geht er von einer höheren Schutzwürdigkeit der Inhaltsdaten im Verhältnis zu den Verkehrsdaten aus. Diese Ansicht ist aber unzutreffend. In die Vertraulichkeit der Telekommunikation darf nur ausnahmsweise zur Abwehr schwerer Gefahren und zur Verfolgung schwerer Straftaten eingegriffen werden. Dies gilt für Kommunikationsinhalte, Kommunikationsumstände und Kommunikationsbeteiligte in gleicher Weise; denn die technische Differenzierung in Inhalts-, Verkehrs- und Bestandsdaten ist ohne Bedeutung für Nutzbarkeit und Verwendungsmöglichkeiten solcher Daten. Gerade die jeweiligen Nutzungs- und Verwendungsmöglichkeiten bestimmen nach der Rechtsprechung des Bundesverfassungsgerichts die Schutzwürdigkeit von Daten[78].

Der staatliche Zugriff auf die näheren Umstände der Telekommunikation – insbesondere bei der vorgesehenen weitreichenden Speicherung der gesamten Kommunikationsumstände - kann mindestens so schwerwiegend wie der Zugriff auf Telekommunikationsinhalte sein. Das ergibt sich schon daraus, dass die Verarbeitungs- und Verwendungsmöglichkeiten von Verkehrsdaten höher sind als die von Inhaltsdaten. Verkehrsdaten können automatisch analysiert, mit anderen Datenbeständen verknüpft und auf bestimmte Suchmuster hin durchkämmt sowie nach im Einzelfall subjektiv auswählbaren Kriterien geordnet und ausgewertet werden. Diese Möglichkeiten bestehen bei Inhaltsdaten so nicht.

Das Bundesverfassungsgericht hat dazu ausgeführt: „Immer mehr Lebensbereiche werden von modernen Kommunikationsmitteln gestaltet. Damit erhöht sich nicht nur die Menge der anfallenden Verbindungsdaten, sondern auch deren Aussagegehalt. Sie lassen in zunehmendem Maße Rückschlüsse auf Art und Intensität von Beziehungen, auf Interessen, Gewohnheiten und Neigungen und nicht zuletzt auch auf den jeweiligen Kommunikationsinhalt zu und vermitteln – je nach Art und Umfang der angefallenen Daten – Erkenntnisse, die an die Qualität eines Persönlichkeitsprofils heranreichen können“.[79]

Ein Grundsatz, wonach Verkehrsdaten typischerweise weniger schutzbedürftig seien als Inhaltsdaten, lässt sich somit nicht aufstellen; ein unterschiedliches Schutzniveau für Inhaltsdaten einerseits und Verkehrsdaten andererseits ist nicht gerechtfertigt. Der Zugriff auf Informationen über die Kommunikation und die Kommunizierenden (Verkehrsdaten, Bestandsdaten) muss deshalb den gleichen Voraussetzungen unterliegen wie der Zugriff auf die Inhalte der Kommunikation.

---

78 BVerfG (Volkszählung) vom 15.12.1983, 1 BvR 209/83 u. a., BVerfGE 65, 1 (45).

79 BVerfG (TKÜ), 2 BvR 2099/04 vom 2.3.2006, BVerfGE 115, 166, Abschnitt 91.

5. Zur vorgesehenen Regelung des § 100g Abs. 3 StPO-E (Datenträger mit Verbindungsdaten)

a) Nach dem klarstellenden Hinweis in § 100g Abs. 3 StPO-E sollen Datenträger, auf denen Verbindungsdaten gespeichert sind, nach den §§ 94 ff. StPO beschlagnahmefähig sein, wenn sie sich außerhalb des Zugriffsbereiches eines TK-Anbieters befinden.[80]

b) Die Sicherstellung und Beschlagnahme von Datenträgern ist nach traditioneller Auffassung eine Maßnahme der §§ 94 ff. StPO. Die vom Entwurf eingefügte „Klarstellung“ für Datenträger mit Verbindungsdaten bedeutet daher nicht ein „Mehr“ an Rechtsschutz für den Betroffenen, sondern eine Ausweitung der Zugriffsmöglichkeiten auf jegliche Art von **Speichermedien** und jeglichen Verfügungsberechtigten über Verbindungsdaten ohne die Schutzmechanismen der Neuregelungen, wie bspw. die Beweiserhebungs- und –verwertungsverbote, die Datenverwendungsregelungen und Benachrichtigungspflichten beachten zu müssen. Dass solche Regelungen erforderlich sind, hat das BVerfG in den Entscheidungen vom 02.03.2006 – 2 BvR 2099/04 – und vom 05.02.2004 – 2 BvR 1621/03 – anerkannt. Telekommunikationsverbindungsdaten unterliegen auch dann dem grundrechtlichen Schutz aus Art. 13 Abs. 1 und Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG (informationelle Selbstbestimmung), wenn sie am Endgerät angekommen sind und dort wahrnehmbar gemacht werden können.[81] Da die „Klarstellung“ den Ermittlungszugriffen auf Telefonzentralen, Telefonanlagen, Firmenserver, Netzwerkserver und sonstiger, dem TKG nicht unterworfener Sammelstellen von Verbindungsdaten den Weg bahnen soll, hat die Regelung erhebliche praktische Bedeutung. Auch der Zugriff auf solche Daten geschieht nämlich „heimlich“ aus der Sicht des Betroffenen. Daher müssen Regelungen geschaffen werden, die die Datenerhebung- und –verwendung einschränken sowie eine Benachrichtigung sicherstellen.

---

80 BR-Drucks. 275/07, S. 52 als Konsequenz aus den Entscheidungen des BVerfG vom 4.2.2005, -2 BvR 308/04- NJW 2005, 1637 ff. und vom 2.3.2006, -2 BvR 2099/04.

81 Vgl. dazu ausführlich die Stellungnahmen des Strafrechtsausschusses vom Juni 2005, RS 24/2005 unter Hinweis auf die Entscheidungen BVerfG Beschl. v. 3.3.2004 – 1 BvF 3/92, NJW 2004, 2213; Beschl. v. 5.2.2005, 2 BvR 308/04, wistra 2005, 219; Beschl. v. 14.12.2004 – 2 BvR 1451/04, NJW 2005, 1855. Außerdem hatten Strafrechtsausschuss und Verfassungsrechtsausschuss der BRAK im (noch laufenden) Verfahren des BVerfG, 2 BvR 902/06 (E-Mail-Beschlagnahme), RS 56/2007, darauf hingewiesen, dass die ohne gesetzliche Grundlage vorgenommenen Eingriffe nicht den Anforderungen der Art. 13 Abs. 1, 2 Abs. 1 GG entsprechen (dazu auch sogleich zu § 110 Abs. 3 StPO-E).

V. IMSI-Catcher, § 100i StPO-E

Eine erhebliche Erweiterung der heimlichen Überwachungsmöglichkeiten enthält § 100i StPO-E. Der Einsatz des IMSI-Catchers soll nicht mehr wie im geltenden Recht beschränkt sein auf die Ermittlung von Gerätenummern oder Handy-Standorten *zur Vorbereitung einer Telekommunikationsüberwachung* nach § 100a StPO oder *Festnahme des Beschuldigten*, sondern *generell zur Erforschung des Sachverhalts* zulässig sein, sofern der Verdacht einer Katalogtat nach § 100a Abs. 2 StPO-E oder einer *anderen Straftat von auch im Einzelfall erheblicher Bedeutung* vorliegt.

Damit sollen auch bei außerhalb des Katalogs noch § 100a Abs. 2 StPO-E liegenden anderen Straftaten von (auch im Einzelfall) erheblicher Bedeutung Bewegungsprofile ermöglicht werden[82] sowie Vorbereitungen einer Verkehrsdatenerhebung nach § 100g StPO-E ermöglicht werden,[83] die nach geltendem Recht unzulässig sind.[84]

Anders als das geltende Recht und noch der Referentenentwurf verzichtet § 100i StPO-E in der Fassung des Regierungsentwurfs zudem ohne jede Begründung auf die Subsidiaritätsklauseln des geltenden § 100i Abs. 2 und 3 StPO, wonach die Ermittlung von Standort und Geräte- bzw. Kartennummer des Mobilfunkendgerätes voraussetzt, dass die Durchführung der Überwachungsmaßnahme oder die Ermittlung des Aufenthaltsorts des Beschuldigten ohne IMSI-Catcher nicht möglich oder wesentlich erschwert wäre. Kenntnis der Gerätenummern oder des Standorts des Handys müssen nur noch *erforderlich zur Erforschung des Sachverhalts* oder zur Ermittlung des Aufenthaltsorts des Beschuldigten sein. Bei der heutigen Verbreitung von Mobilfunkgeräten wird diese Erforderlichkeit stets gegeben sein.

Bewegungsprofile sind jedoch Eingriffe in die grundgesetzlich geschützte informationelle Selbstbestimmung und dürfen daher nur als Ultima ratio erhoben werden, wenn andere Ermittlungsmaßnahmen aussichtslos wären.

Gleiches gilt für den Einsatz des IMSI-Catchers zur Vorbereitung einer Verkehrsdatenerhebung nach § 100g StPO. Bei mittels Telekommunikation begangener Straftaten sieht § 100g Abs. 1 Satz 2 StPO-E zu Recht vor, dass Verkehrsdaten (Geräte- und Kartennummern, Standort, Anrufer- und Angerufenennummern, Beginn und Ende der Telekommunikation) nur erhoben werden dürfen, wenn die Erforschung des Sachverhaltes oder des Aufenthaltsorts des Beschuldigten auf andere Weise aussichtslos wäre und die

---

82 BR-Drucks. 275/07, S. 127: „Unterstützung einer Observationsmaßnahme“.
83 BR-Drucks. 275/07, S. 127.
84 LR-*Schäfer*, § 100i Rn. 8; *Hilger*, GA 2002, 557.

Erhebung der Verkehrsdaten überdies verhältnismäßig ist. Dann kann bei ebenfalls heimlicher Vorbereitung einer solchen Verkehrsdatenerhebung keine geringere Eingriffsschwelle gelten.

VI. Zur vorgesehenen Neuregelung des § 110 Abs. 3 StPO (Sichtung von räumlich getrennten Speichermedien)

Der Entwurf will durch eine Änderung des § 110 Abs. 3 StPO-E erreichen, dass die Computerdaten, die bei einer Durchsuchung nicht auf dem Heimcomputer, sondern auf anderen, über eine Datenleitung verbundenen Computern auffindbar sind, von jeder Ermittlungsperson durchgesehen werden können, ohne dass es eigenständiger richterlicher Anordnungen bedarf.[85] Das Übereinkommen des Europarates verpflichte den Gesetzgeber, den Zugriff auf räumlich entfernte Datenträger „in Echtzeit“ zu ermöglichen. Auch wenn es sich dabei um Telekommunikationsvorgänge handele, könne eine Beschränkung auf einen bestimmten Straftatenkatalog den internationalen Vereinbarungen nicht entnommen werden.

Gemeint sind mit dieser Regelung alle Computer, die in ein Netzwerk eingebunden sind, also wohl fast alle geschäftlich und viele (bei steigenden Zahlen) privat genutzten Computeranlagen.

Die Vorschrift hätte zur Folge, dass den Ermittlungspersonen nahezu jeder national und international individuelle Zugang des Betroffenen zu einem Datenbestand (BSPW für Bankdaten, Börsendaten, Telekommunikationsabrechnungen, Chatrooms etc.) ohne richterliche Anordnung unabhängig von den Begrenzungen der §§ 100a ff. StPO erlaubt wäre. Das wird dem Schutz der Grundrechte aus Art. 13 Abs. 1, Art. 12 Abs. 1, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG nicht gerecht.

In der Strafverfolgungspraxis ergeben sich Probleme des Geheimnisschutzes und der Beachtung ausländischer Geheimnisschutz- und Strafvorschriften, die nicht bereits während der Durchsuchung geklärt werden können. Zwei Beispiele sollen an dieser Stelle genannt werden.

---

[85] BR-Drucks. 275/07, S. 54 ff. als Konsequenz aus Art. 16 I, 32 der Übereinkommens des Europarates vom 23.11.2001 über die Bekämpfung der Computerkriminalität mit dem Hinweis, im geltenden Recht sei der Zugriff auf räumlich entfernte Daten (auch im Ausland) nicht geregelt.

(1) Eine inländische Niederlassung einer Bank unterhält eine Netzwerkverbindung zur schweizerischen Muttergesellschaft. Alle Konten für Kunden werden bei dieser Muttergesellschaft geführt, die Daten können nur online von den Beratern der inländischen Niederlassung abgefragt werden. Die Durchsuchung der Steuerfahndung vor ort im Inland will auf Daten zugreifen, die durch ein in der Schweiz auch strafrechtlich geschütztes Bankgeheimnis gesichert sind. Damit können Rechtshilfevorschriften umgangen werden.

(2) Ein Privatmann ruft die für ihn bestimmten E-Mails aus einer Internet-Mailbox ab.[86] Soll der Ermittler nunmehr den Zugang auf diese Mail-Box und die dort gespeicherten Inhalte fremder Kommunikation unter Umgehung aller Schutzmechanismen der §§ 100a ff. StPO-E über eine Telekommunikationsleitung gestattet werden? Darf der Beschuldigte das Passwort zurückhalten? Dürfen auf Kosten des Beschuldigten derartige Internetrecherchen („Google-Suche“) auf dem Heimcomputer angestellt werden, wenn das der Ermittlungsperson zweckmäßig erscheint?

Die Beispiele zeigen, dass durch **§ 110 Abs. 3 StPO-E** die **Probleme vermehrt** statt gelöst werden. Die Eingrenzung durch die Umschreibung „für die Untersuchung von Bedeutung“ ist unbestimmt und lässt wahllose Eingriffe zu. Die Speicheranweisung wird zu einer einschränkungslosen Sofortsicherung aller erreichbaren Daten führen, weil der Inhaber des „Datenträgers“ nicht unverzüglich ausfindig gemacht werden kann. Beschränkende Verwendungsregelungen sind nicht vorgesehen. Die Speicheranweisung bedeutet eine Datenverselbständigung während der Gesamtdauer des Verfahrens, d.h. einen jahrelangen Eingriff. Die Vorschrift wird daher abgelehnt**.**

VII. Zu den vorgesehenen strafprozessualen Schranken und Einhegungen heimlicher Ermittlungsmaßnahmen

Der Gesetzentwurf verfolgt das Ziel, die heimlichen strafprozessualen Ermittlungsmaßnahmen durch schützende Formen wie den Richtervorbehalt, Kennzeichnungspflichten, Gewährleistungen der Zweckbindung, Anforderungen an die Aktenführung, Benachrichtigungspflichten und Rechtsschutzmöglichkeiten rechtlich

[86] Konstellation vergleichbar der Verfassungsbeschwerde B., vgl. BRAK-Stellungnahme vom Januar 2007 an das BVerfG im Verfahren 2 BvR 902/06 (E-Mail-Beschlagnahme), RS 56/2007.

einzuhegen. Dies ist, von einigen Regelungen abgesehen, auf die im Folgenden hingewiesen wird, weitgehend gelungen.

1. Richtervorbehalt

Folgende Richtervorbehalte sind geltendes bzw. geplantes Recht:

Maßnahme	**Richtervorbehalt**
Überwachung und Aufzeichnung der Telekommunikation (§ 100a)	Ermittlungsrichter (§ 100b). Nach 6 Monaten außerhalb des § 169 entscheidet das LG (§ 100b Abs. 1 Satz 6 StPO-E).
Akustische Wohnraumüberwachung (§ 100c)	Landgericht (§ 100d, § 74a Abs. 4 GVG)
Akustische Überwachung außerhalb von Wohnungen (§ 100f)	Ermittlungsrichter (§ 100b, § 100f Abs. 4)
Erhebung von Verkehrsdaten (§ 100g)	Ermittlungsrichter (§ 100b, § 100g Abs. 2)
Besondere technische Maßnahmen = Observationen (§ 100h)	Nein, außer bei längerfristiger Observation, dann: Ermittlungsrichter, § 163f StPO
IMSI-Catcher (§ 100i)	Ermittlungsrichter (§ 100b, § 100i Abs. 3)

Die Anordnung verdeckter strafprozessualer Ermittlungsmaßnamen und die Prüfung der Anordnungsvoraussetzungen für verdeckte Maßnahmen hat der Entwurf weitgehend unter (einen neu gefassten) Richtervorbehalt gestellt. Er will damit die rechtsstaatliche Kontrolle[87] dieser Ermittlungsmaßnahmen, die schwerwiegende Eingriffe in die Grundrechtspositionen von Betroffenen darstellen, stärken[88].

---

87 Dies hatten *Albrecht/Dorsch/Krüpe*, Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmethoden, 2003, S. 467, gefordert.

88 So ausdrücklich die Begründung zum Entwurf BT-Drucks. 275/07, S. 46.

Nach der Rechtsprechung des Bundesverfassungsgericht ist der Richtervorbehalt ein zentrales Instrument, das die Grundrechte der Bürger in besonders schwerwiegenden Eingriffssituationen wirksam schützen soll.[89] Da verdeckte strafprozessuale Ermittlungsmaßnamen ohne vorherige Anhörung des Betroffenen angeordnet und ohne sein Wissen durchgeführt werden sollen, soll die Einschaltung eines unabhängigen Richters „als Sachwalter der Rechte der Betroffenen“[90] auch für eine angemessene Berücksichtigung der Interessen des Betroffenen sorgen.[91] Durch die Einschaltung des Ermittlungsrichters will der Gesetzgeber erreichen, dass dieser als neutrale Instanz die Belange der von der Maßnahme betroffenen Personen eigenständig prüft und dass der durch die Maßnahme erfolgende Grundrechtseingriff *„messbar und kontrollierbar“* [92] bleibt.

Der Ausschuss begrüßt daher, dass die Anordnung verdeckter strafprozessualer Ermittlungsmaßnamen und die Prüfung der Anordnungsvoraussetzungen für verdeckte Maßnahmen weitgehend unter Richtervorbehalt gestellt wird. Damit wird die rechtsstaatliche Kontrolle dieser Ermittlungsmaßnahmen, die schwerwiegende Eingriffe in die Grundrechtspositionen von Betroffenen darstellen, ermöglicht.

2. Konzentrationsmaxime

Nach der Begründung des Entwurfs soll die neu gefasste Regelung in § 162 StPO-E über die Konzentration der örtlichen Zuständigkeit des Ermittlungsrichters am Sitz der Staatsanwaltschaft eine Stärkung der mit dem Richtervorbehalt bezweckten rechtsstaatlichen Kontrolle bewirken[93] und zugleich eine Spezialisierung in der ermittlungsrichterlichen Tätigkeit fördern[94]. Damit werden Verbesserungsvorschläge umgesetzt, die auch in den beiden rechtstatsächlichen Untersuchungen zur richterlichen Kontrolle der Telefonüberwachung enthalten waren.[95]

Eine weitergehende Konzentration – etwa auf die Staatsschutzkammer des Landgerichts am Sitz der ermittlungsführenden StA (§ 100d, § 74a Abs. 4 GVG) – zu fordern, erscheint

---

89 BVerfG, 2 BvR 1473/01 vom 22.1.2002, Absatz-Nr. 12 f.; vgl. auch BVerfGE 57, 346 (355 f.); 76, 83 (91); 103, 142 (150 f.) ; *Amelung*, NStZ 2001, S. 337 (338); krit. *Rabe von Kühlewein*, Der Richtervorbehalt im Polizei- und Strafprozessrecht, 2001, S. 88 ff.; BVerfG, 2 BvR 1845/00 vom 3.12.2002, Absatz-Nr. 11.

90 So die Begründung BR-Drucks. 275/07, S. 151.

91 BVerfG, 2 BvR 1473/01 vom 22.1.2002, Absatz-Nr. 12.

92 Vgl. BVerfGE 20, 162 (224); 42, 212 (220); 103, 142 (151), *BVerfG,* 2 BvR 1821/03 vom 8.4.2004, Absatz-Nr. 13.

93 BR-Drucks. 275/07, S. 46.

94 BR-Drucks. 275/07, S. 53.

95 *Albrecht/Dorsch/Krüpe* a. a. O. (Fn 29), S. 467; *Backes/Gusy* u. a. a. a. O. (Fn 29), S. 8 der Kurzfassung des Abschlussberichts.

nicht angebracht. Dies würde in der praktischen Konsequenz einer einen höheren Grundrechtsschutz besorgenden Intention zuwiderlaufen und wegen zu hoher Konzentration auf einen möglicherweise entfernteren Spruchkörper zu längerer Bearbeitungsdauer und in der Folge zur Ausweitung von staatsanwaltschaftlichen Anordnungen auf Grund von Gefahr im Verzug führen.

Der Ausschuss begrüßt daher auch die Regelung in § 162 StPO-E über die Konzentration der örtlichen Zuständigkeit des Ermittlungsrichters am Sitz der Staatsanwaltschaft. Diese Konzentration ist geeignet, eine Spezialisierung in der ermittlungsrichterlichen Tätigkeit zu fördern, und lässt eine gesteigerte Effektivität des Richtervorbehalts erwarten.

3. Kennzeichnung und Verwendung

a) Grundsatz der Zweckbindung

Die Speicherung und Verwendung der mit der Wohnraum- oder der Telekommunikationsüberwachung gewonnenen personenbezogenen Informationen und Daten sind grundsätzlich an den Zweck und auch an das Ermittlungsverfahren gebunden, für die sie erhoben worden sind.[96] Sollen die gewonnenen Informationen zu einem anderen Zweck als dem ursprünglich verfolgten verwendet werden, so stellt dies grundsätzlich einen eigenständigen Grundrechtseingriff dar, da sich der Schutz des Art. 13 Abs. 1 GG nicht nur auf die Phase der Datenerhebung in und aus Wohnungen beschränkt, sondern auch die Weitergabe einbezieht.[97] Zwar schließt der Grundsatz der Zweckbindung eine Zweckänderung nicht generell aus. Die **Zweckänderung** bedarf jedoch ihrerseits einer gesetzlichen Grundlage, die formell und materiell verfassungsmäßig ist. Dazu gehört, dass die Zweckänderung durch Allgemeinbelange gerechtfertigt ist, die die grundrechtlich geschützten Interessen überwiegen. Der neue Verwendungszweck muss sich auf die Aufgaben und Befugnisse der Behörde beziehen, der die Daten übermittelt werden, und hinreichend normenklar geregelt sein. Schließlich dürfen der ursprüngliche Verwendungszweck und der veränderte Verwendungszweck nicht miteinander unvereinbar sein.[98]

---

96 Vgl. BVerfGE 100, 313 (360) zu Art. 10 GG; 109, 279 (379 f.) zum Großen Lauschangriff
97 Vgl. BVerfGE 109, 279 (Abschnitt 333).
98 Vgl. BVerfGE 65, 1 (51, 62); 100, 313 (360); 109, 279 (Abschnitt 334).

b) Kennzeichnung

Die Zweckbindung lässt sich nur gewährleisten, wenn auch nach der Informationserhebung erkennbar bleibt, dass es sich um Daten handelt, die durch eine Maßnahme der akustischen Wohnraum- oder Telekommunikationsüberwachung gewonnen worden sind. Eine entsprechende Kennzeichnung der Daten ist daher von Verfassungs wegen geboten.[99] Der Gesetzgeber hat sowohl den datenerhebenden als auch den datenempfangenden Behörden zur Sicherung der Zweckbindung eine **Kennzeichnungspflicht** aufzuerlegen. Sonst könnten die aus der Wohnraum- oder Telekommunikationsüberwachung stammenden Daten in einer Weise gespeichert und mit anderen Daten vermischt werden, die ihre Herkunft nicht mehr erkennen lässt.[100]

c) Erfüllung der Kennzeichnungspflicht durch § 101 Abs. 3 StPO-E

Den Vorgaben des Bundesverfassungsgerichts folgend erweitert der Entwurf die bisher nur für die akustische Wohnraumüberwachung getroffene Regelung in § 100d Abs. 7 StPO über die Kennzeichnung der durch diese Maßnahme erhobenen Daten in eine generelle Vorschrift, die für alle verdeckten Ermittlungsmaßnahmen (nach den §§ 98a, 99, 100a, 100c bis 100i, 110a, 163d bis 163f , also auch für die Rasterfahndung und die Postbeschlagnahme) gelten soll. § 101 Abs. 3 StPO-E bestimmt, dass personenbezogene Daten, die durch die aufgeführten Maßnahmen erhoben wurden, entsprechend zu kennzeichnen sind und dass die Kennzeichnung nach Übermittlung an eine andere Stelle durch diese aufrechtzuerhalten ist.

Die Erfüllung dieser Kennzeichnungspflichten wird für die Behörden und Gerichte des Bundes und der Länder Mehraufwand verursachen, der jedoch entsprechend den Vorgaben des Bundesverfassungsgerichts für die Sicherstellung einer ordnungsgemäßen Datenverwendung erforderlich ist. Die Erstreckung der Kennzeichnungspflicht auf alle speziell geregelten verdeckten Ermittlungsmaßnahmen ist konsequent.

---

99 Vgl. BVerfGE 100, 313 (360 f.); 109, 279 (Abschnitt 347).

100 Vgl. BVerfGE 100, 313 (396 f.); 109, 279 (Abschnitt 347); vgl. auch Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. März 2003 in Dresden zur Kennzeichnung von Daten aus Telefon-, Wohnraum- oder Postüberwachung.

d) Gewährleistung der Zweckbindung durch § 477 StPO-E

§ 477 Abs. 2 Satz 2 StPO-E bestimmt, dass die aufgrund einer Ermittlungsmaßnahme, die nur bei Verdacht bestimmter Straftaten zulässig ist, erlangten personenbezogenen Daten ohne Einwilligung der von der Maßnahme betroffenen Personen zu Beweiszwecken in anderen Strafverfahren nur zur Aufklärung solcher Straftaten übermittelt werden dürfen, zu deren Aufklärung eine solche Maßnahme nach diesem Gesetz hätte angeordnet werden dürfen. Dieser Regelung liegt die Rechtsfigur des „hypothetischen Ersatzeingriffs“[101] zugrunde.

Die **Postbeschlagnahme** (§ 99 StPO) steht zwar unter Kennzeichnungspflicht, sie soll aber nach der vom Entwurf vorgesehenen Regelung als eine Maßnahme, die nicht vom Verdacht bestimmter näher umschriebener Straftaten abhängig ist, nicht geeignet sein, das Eingreifen der Verwendungsbeschränkungen in § 477 Abs. 2 StPO-E auszulösen.

Hier muss auch insoweit eine **Übermittlungs- und Weiterverwendungsschranke** eingebaut werden; denn immerhin handelt es sich bei einer Maßnahme nach § 99 StPO um einen (zunächst meist heimlich vorgenommenen) Grundrechtseingriff, der am Verhältnismäßigkeitsgrundsatz zu messen ist und zumindest einen konkreten Tatverdacht für eine nicht nur geringfügige Tat erfordert – die Weitergabe von derart gewonnenen Daten für Verfahren wegen Bagatellstraftaten wäre nach den Vorgaben des Bundesverfassungsgerichts unzulässig.

4. Aktenführung, - verwahrung und - einsicht

In § 101 Abs. 2 StPO-E werden die bislang schon für

- die akustische Wohnraumüberwachung in § 100d Abs. 9 Satz 5 StPO,
- die akustische Überwachung außerhalb von Wohnräumen in § 101 Abs. 4 i. V. m. § 100f Abs. 2 StPO,
- den Einsatz technischer Observationsmittel in § 101 Abs. 4 i. V. m. § 100 f. Abs. 1 Nr. 2 StPO und
- den Einsatz Verdeckter Ermittler in § 110d Abs. 2 StPO

[101] Vgl. BVerfG v. 8.3.2002, 2 BvR 2081/01; BGHSt 24, 125 (130); 26, 298 (303); 27, 355 (358); 28, 122 (125 ff.); 44, 243; BGHR StPO § 100a Verwertungsverbot 4, 5, 10.

enthaltenen Regelungen zur getrennten Aktenführung und zur Verwahrung solcher Sonderakten bei der StA unverändert übernommen und in einer einzigen Vorschrift zusammengefasst.

Der Entwurf entscheidet sich ausdrücklich gegen eine im Sinne einer harmonischen Gesamtregelung in Betracht kommende Ausweitung der getrennten Aktenführung auch auf andere verdeckte Ermittlungsmaßnahmen, weil anderenfalls die sich aus den Sonderregelungen ergebende Beschränkung der Akteneinsichtsrechte auch auf alle anderen verdeckten Ermittlungsmaßnahmen ausgedehnt würde[102].

Die bisher schon geltenden Vorschriften (§ 100d Abs. 9 Satz 5 StPO, § 101 Abs. 4 i. V. m. § 100 f Abs. 2 StPO, § 101 Abs. 4 i. V. m. § 100 f Abs. 1 Nr. 2 StPO und § 110d Abs. 2 StPO) enthalten weitgehende – und verfassungsrechtlich nicht unbedenkliche – Beschränkungen des Grundsatzes der Aktenwahrheit[103] und des Akteneinsichtsrechts[104] und sollten daher Ausnahmevorschriften bleiben.

5. Benachrichtigungspflichten

a) Ziele des Entwurfs

In der Entwurfsbegründung wird festgestellt[105], dass in der gerichtlichen Praxis schwerwiegende Defizite bei der Erfüllung der Benachrichtigungspflichten bestehen. Der Entwurf will daher

- in Umsetzung der Rechtsprechung des Bundesverfassungsgerichts[106] die Benachrichtigungspflichten nicht nur auf alle eingriffsintensiven verdeckten Ermittlungsmaßnahmen erstrecken, sondern zugleich auch
- den Kreis der zu benachrichtigenden Personen konkretisieren und so
- den nachträglichen Rechtsschutz stärken und
- das Bewusstsein der Praxis für die Benachrichtigungspflicht schärfen.

102 BR-Drucks. 275/07, S. 131.
103 Vgl. BVerfGE 63, 45; BGH StV 1995, 247.
104 Vgl. dazu KK-*Nack* § 110c StPO Rn 21 ff.
105 BR-Drucks. 275/07, S. 45 – 47 unter Berufung auf *Albrecht/Dorsch/Krüpe,* a. a. O., S. 451, und *Backes/Gusy,* a. a. O., S. 71 f.
106 Vgl. BVerfGE 100, 313 (361 f., 364); 107, 299 (337 f.); BVerfG v. 12.4.2005, 2 BvR 581/01, Absatz - Nr. 55 = NJW 2005, 1338 (1340); v. 1.7.2005, 1 BvR 668/04, Absatz - Nr. 159 = NJW 2005, 2603, (2611); vgl. auch vgl. BVerfGE 69, 1 (49).

Dieses Bestreben ist anerkennenswert und wird ausdrücklich begrüßt.

b) Mehraufwand

Die Erfüllung dieser Benachrichtigungspflichten wird für die Behörden und Gerichte des Bundes und der Länder Mehraufwand verursachen,[107] der jedoch entsprechend den Vorgaben des Bundesverfassungsgerichts zur Gewährleistung des Rechtsschutzes Eingriffsbetroffener erforderlich ist.

c) Die Benachrichtigungsregelungen im Einzelnen

In § 101 Abs. 4 StPO-E werden die bisher in § 101 Abs. 1 Satz 1 StPO und § 100d Abs. 8 und 9 StPO enthaltenen Benachrichtigungspflichten an zentraler Stelle zusammen gefasst und, maßnahmenbezogen differenziert, neu gefasst.

Allgemeine Benachrichtigungspflicht: § 101 Abs. 4 Satz 1 StPO-E. Satz 1 bestimmt, dass die von den in § 101 Absatz 1 StPO-E genannten verdeckten Ermittlungsmaßnahmen Betroffenen von der Maßnahme zu benachrichtigen sind.

Absehen von der Benachrichtigung. Von der allgemeinen Benachrichtigungspflicht sieht § 101 Absatz 4 Satz 1 2. Halbsatz StPO-E folgende Ausnahmen vor:

- die zu benachrichtigenden Personen sind nicht bekannt,
- deren Ermittlung wäre mit weiteren Eingriffen oder aber mit einem erheblichen, im Einzelfall ggf. unangemessenen Aufwand (z. B. Feststellung der Betroffenen im Ausland im Wege der Rechtshilfe) verbunden und daher unverhältnismäßig,
- der Benachrichtigung stünden überwiegende schutzwürdige Interessen anderer Betroffener (z. B. des Nachrichtenmittlers, wenn zufällig dessen Gespräch mit einem unbeteiligten Geschäftspartner erfasst wurde) entgegen.

In diesen Fällen soll ein Absehen von der Benachrichtigung möglich sein. Dagegen ist nichts einzuwenden. So könnte der abzusehende Mehraufwand auch in erträglichen Grenzen gehalten werden. Zu fordern ist allerdings, dass der Staatsanwalt seine Entscheidung auch mit kurzer Begründung aktenkundig zu machen hat, damit auch sein Bewusstsein für die Benachrichtigungspflicht geschärft wird und später die Gründe für das Absehen der Benachrichtigung nachvollziehbar sind.

---

[107] Dies sieht auch der Deutsche Richterbund in seiner Stellungnahme vom Januar 2007 (S. 5) voraus: „erheblicher zusätzlicher Personalbedarf".

Hinweis auf die Möglichkeit nachträglichen Rechtsschutzes. § 101 Absatz 4 Satz 2 StPO-E bestimmt, dass im Rahmen der Benachrichtigung auf die Möglichkeit nachträglichen Rechtsschutzes nach § 101 Absatz 9 StPO-E und die dafür vorgesehene Frist hinzuweisen ist. Die Regelung ist § 100d Abs. 8 Satz 2 StPO nachgebildet und dient der Gewähr effektiven Rechtsschutzes des Betroffenen.

Maßnahmespezifische Bestimmung der zu benachrichtigenden Personen. § 101 Absatz 4 Satz 3 StPO-E führt die zu benachrichtigenden Personen maßnahmespezifisch auf. Durch die Aufzählung (in 12 Ziffern) wird die Vorschrift aufgebläht. Man muss aber die Intention der Aufzählungsregelung anerkennen: damit soll den Unsicherheiten Rechnung getragen, die in der Praxis[108] bei der Anwendung der bisher geltenden Bestimmung insbesondere daraus resultieren, dass die bislang im Gesetz verwandten Begriffe des „Betroffenen“ (§ 100b Abs. 1 Satz 2 StPO) und des „Beteiligten“ (§ 101 Abs. 1 Satz 1 StPO) als Definitions- und Abgrenzungskriterien wenig tauglich sind und insbesondere kaum eine hinreichende Hilfestellung zur Bestimmung der zu benachrichtigenden Personen geben. Der Aufzählung § 101 Absatz 4 Satz 3 StPO-E als solcher wird daher nicht entgegengetreten.

Bei einem **Einsatz des „IMSI-Catchers“** nach § 100i StPO-E sieht der Entwurf nur die Benachrichtigung der Zielperson vor. Die Nichteinbeziehung der sonstigen von der Maßnahme betroffenen Personen wird damit begründet, dass die vorübergehend erhobenen Geräte- und Kartennummer sowie Standorte bezüglich der Mobilfunkgeräte Dritter nach § 100i Abs. 4 StPO E nur im Rahmen des technisch Unvermeidbaren erhoben werden und über den Datenabgleich hinaus nicht verwendet werden dürfen, sondern nach Beendigung der Maßnahme unverzüglich zu löschen sind. Das ist nachvollziehbar.

Nicht erörtert werden Benachrichtigungspflichten, die sich bei einer **Funkzellenabfrage** (§ 100g Abs. 2 Satz 2 StPO-E) ergeben könnten. Sofern es um die Verkehrsdaten einer Vielzahl zufällig in dem umschriebenen Bereich anwesender Personen geht, muss man anerkennen, dass, wie zuvor, die vorübergehend erhobenen Daten bezüglich der Mobilfunkgeräte Dritter nur im Rahmen des technisch Unvermeidbaren erhoben werden und über den Datenabgleich hinaus nicht verwendet werden dürfen; auch würde hier wohl die Ausnahme des § 101 Absatz 4 Satz 1 2. Halbsatz StPO-E der allgemeinen Benachrichtigungspflicht zur Anwendung kommen, wonach dann von einer Benachrichtigung abgesehen werden kann, wenn die zu benachrichtigen Personen nicht

108 Vgl. *Albrecht/Dorsch/Krüpe,* a. a. O., S. 470.

bekannt sind und deren Ermittlung mit weiteren Eingriffen oder aber mit einem erheblichen, im Einzelfall ggf. unangemessenen Aufwand verbunden wäre.

Die bislang in § 101 Abs. 1 StPO vorgesehene Benachrichtigungspflicht bei Maßnahmen nach § 81e StPO (**DNA-Analyse**) soll entfallen, weil § 81e StPO in den Anwendungsbereich des § 101 StPO-E nicht einbezogen worden ist. Die dafür angeführte Entwurfsbegründung[109] ist einleuchtend.

d) Zurückstellung der Benachrichtigung

§ 101 Abs. 5 StPO-E enthält eine Regelung zur zeitweisen Zurückstellung einer Benachrichtigung, die der bislang geltenden Regelung in § 100d Abs. 8 Satz 5 StPO nachgebildet ist. Die dafür angegebene Begründung ist plausibel, die Regelung kann akzeptiert werden.

§ 101 Abs. 5 Satz 2 StPO-E bestimmt, dass die Zurückstellung der Benachrichtigung aus einem der in Satz 1 genannten Gründe aktenkundig zu machen ist. Diese Regelung ist nötig zur Sicherung der Benachrichtigungspflichten und deren Beachtung durch die Strafverfolgungsorgane; sie dient auch dazu, die ordnungsgemäße Handhabung der Benachrichtigungsregelungen nachvollziehbar zu machen.

§ 101 Abs. 6 StPO-E trifft Regelungen über eine gerichtliche Kontrolle der Anwendung der in Absatz 5 enthaltenen Zurückstellungsgründe. Diese Kontrolle durch eine unabhängige Stelle hat das Bundesverfassungsgericht als unerlässlich zur Gewährleistung eines effektiven Rechtsschutzes des Betroffenen angesehen.

§ 101 Abs. 7 StPO-E trifft eine Regelung zum endgültigen Absehen von der Benachrichtigung. Voraussetzung soll sein, dass die Benachrichtigung bereits für insgesamt fünf Jahre zurückgestellt worden ist und sich nach diesen fünf Jahren ergibt, dass die Voraussetzungen für eine Benachrichtigung mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft nicht eintreten werden. In diesem Fall kann mit Zustimmung des Gerichts endgültig von einer Benachrichtigung abgesehen werden.

Der Strafrechtsausschuss hält es für verfehlt, diese kaum vorstellbare Fallgestaltung[110] zum Anlass für eine Ausnahmeregelung zu nehmen, die insgesamt die intendierte

---

[109] BT-Drucks. 275/07, S. 130 unter Berufung auf die Kritik an der Benachrichtigungspflicht des § 101 Abs. 1 StPO durch *Löffelmann*, ZStW 118 (2006) 358, 367.

[110] So auch der Entwurf S. 137 - 142.

Stärkung des nachträglichen Rechtsschutzes teilweise zurücknähme und so dem Konzept des Entwurfs zuwiderliefe.

Man darf erwarten, dass der Staat es bei einem Grundrechtseingriff mit verdeckten Ermittlungsmaßnahmen jedenfalls binnen eines Zeitraums von 5 Jahren schaffen sollte, dass bei Benachrichtigung der Eingriffsbetroffenen keine Gefahr mehr für andere Personen oder die Rechtsgüter des § 101 Abs. 5 Satz 1 StPO-E besteht.

Der Strafrechtsausschuss unterbreitet daher folgenden Gesetzesvorschlag:

„Spätestens fünf Jahre nach Beendigung der Maßnahme sind die in Absatz 4 Satz 1 genannten Personen gem. Absatz 5 zu benachrichtigen."

6. Nachträglicher Rechtsschutz (§ 101 Abs. 9 StPO-E)

Die in § 101 Abs. 4 StPO-E enthaltenen Mitteilungspflichten in den Fällen, in denen ohne Wissen des Grundrechtsträgers in eines seiner Grundrechte eingegriffen worden war, dienen vor allem dazu, den von einer solchen Maßnahme Betroffenen die Möglichkeit nachträglichen Rechtsschutzes[111] zu gewähren, damit sie sich gegen den Eingriff jedenfalls noch nachträglich zur Wehr setzen zu können.[112]

a) Ziele des Entwurfs

§ 101 Abs. 9 StPO-E soll nach der Entwurfsbegründung[113] klarstellen, dass gegen die in Absatz 1 aufgeführten, regelmäßig in nicht unerheblicher Weise eingriffsintensiven verdeckten Ermittlungsmaßnahmen nachträglicher Rechtsschutz zu gewähren ist. Regelungstechnisch ist die Vorschrift § 100d Abs. 10 StPO nachgebildet.

Der Entwurf will die von solchen Maßnahmen erheblich Betroffenen von der konkreten Darlegung eines Rechtsschutzbedürfnisses im Einzelfall entlasten und ihnen mit § 101 Abs. 9 StPO-E durchgehend eine nachträgliche Rechtsschutzmöglichkeit eröffnen.

---

111 Vgl. BVerfGE 100, 313 (361 f., 364); 107, 299 (337 f.); BVerfG v. 12.4.2005, 2 BvR 581/01, Absatz - Nr. 55 = NJW 2005, 1338 (1340); v. 1.7.2005, 1 BvR 668/04, Absatz - Nr. 159 = NJW 2005, 2603, (2611); vgl. auch BVerfGE 69, 1 (49).

112 Vgl. auch BGHSt 36, 305 (311) m. Anm. *Hassemer* JuS 1990, 587.

113 BR-Drucks. 275/07, S. 141.

Der Ausschuss begrüßt diese Regelung, weil angenommen werden darf, dass dadurch die in der Praxis immer wieder anzutreffenden Unsicherheiten, unter welchen Voraussetzungen ein solches Rechtsschutzbedürfnis gegeben ist[114], beseitigt werden.

b) Die Ausgestaltung des nachträglichen Rechtsschutzes

§ 101 Abs. 9 Satz 1 StPO-E stellt klar, dass die in § 101 Absatz 4 Satz 1 StPO-E maßnahmespezifisch aufgeführten Betroffenen Rechtsschutz auch **nach** Beendigung der Maßnahme erlangen können. Damit wird in Ergänzung zu den Benachrichtigungspflichten dem Gebot der Gewährleistung effektiven Rechtsschutzes (Artikel 19 Abs. 4 GG) Rechnung getragen.

In zeitlicher Hinsicht setzt Satz 1 eine tatsächlich erfolgte Benachrichtigung nicht voraus. Rechtsschutz kann auch erwirkt werden, wenn der Betroffene anderweitig von der Maßnahme Kenntnis erlangt hat.

Die in **§ 101 Abs. 9 Satz 1 StPO-E vorgesehene zweiwöchige Frist** greift als Ausschlussfrist mithin nur im Falle der Benachrichtigung ein. Diese Frist ist indessen **zu kurz bemessen**. Der Betroffene muss einen Rechtsanwalt beauftragen (nur so erhält er umfassende Akteneinsicht), der Anwalt muss Akteneinsicht nehmen (man kann sich leicht vorstellen, wie nach der – wie zu erwarten ist: gleichzeitigen – Benachrichtigung vieler Personen von einer Telekommunikationsüberwachung diese Akte rundum begehrt ist) und dann dem Mandanten vorschlagen, ob er mit Aussicht auf Erfolg die Überprüfung der Rechtmäßigkeit der Maßnahme sowie der Art und Weise ihres Vollzugs beantragen soll oder nicht, und dann muss ggf. der Rechtsschutzantrag formuliert werden. Wenn die Frist nicht auf einen Monat verlängert wird, züchtet man sich Rechtschutzanträge, die allein zur Fristwahrung eingereicht werden.

Der Strafrechtsausschuss fordert daher, die Ausschlussfrist für den nachträglichen Rechtsschutz gegen verdeckte Ermittlungsmaßnahmen auf **1 Monat** festzulegen.

§ 101 Abs. 9 Satz 2 StPO-E bestimmt als für die Entscheidung über den nachträglichen Rechtsschutz dasjenige Gericht für zuständig, das auch für die Anordnung der Maßnahme zuständig ist. Das ist regelmäßig der Ermittlungsrichter des Amtsgerichts am Sitz der Staatsanwaltschaft, im Fall der akustischen Wohnraumüberwachung die in § 74a Abs. 4 GVG genannte Kammer des Landgerichts. Das ist sachgerecht, weil mit dem

---

114 BR-Drucks. 275/07, S. 141 bezieht sich hierzu auf die Darstellung der einzelnen Fallgestaltungen bei der Beschlagnahme bei KK-*Nack*, § 98, Rn. 24 ff.

nachträglichen Rechtschutz nach § 101 Abs. 9 StPO-E das bei verdeckten Maßnahmen zunächst nicht mögliche rechtliche Gehör des Betroffenen nachgeholt werden soll.

§ 101 Abs. 9 Satz 3 StPO-E trifft für den Fall, dass im Zeitpunkt des Antrags auf nachträglichen Rechtsschutz bereits Anklage erhoben und der Angeklagte benachrichtigt worden ist, aus Gründen der Zweckmäßigkeit und Effizienz eine Sonderregelung zur gerichtlichen Zuständigkeit dahingehend, dass über solche Anträge das mit der Sache befasste Gericht befindet. Auch das ist sachgerecht, und zwar im Sinne einer effizienten Verfahrensweise sowie zur Vermeidung divergierender Entscheidungen auch insoweit, als diese Ausnahme nur aktuell anhängige, noch nicht abgeschlossene Verfahren betrifft: In einem Fall, in dem ein ehemaliger Angeklagte um nachträglichen Rechtsschutz nachsucht, verbleibt es bei der Zuständigkeit des Gerichts, das auch für die Anordnung der Maßnahme zuständig ist (§ 101 Abs. 9 Satz 2 StPO-E). Anderenfalls käme es zu unterschiedlichen Zuständigkeiten für nachträgliche Rechtschutzentscheidungen, wenn nämlich für entsprechende Rechtsschutzbegehren anderer Betroffener weiterhin das Anordnungsgericht zuständig bliebe und für Anträge ehemaliger Angeklagter das mit der Sache befasste Gericht (§ 101 Abs. 9 Satz 3 StPO-E).

Die vorgesehene Vorschrift des § 101 Abs. 9 Satz 4 StPO-E enthält Regelungen zur Überprüfung der im Rahmen nachträglichen Rechtsschutzes ergehenden Entscheidungen des Anordnungsgerichts durch die **sofortige Beschwerde**. Die vorgesehenen Normen erscheinen sachgerecht und sinnvoll.

Der Bemerkung der Entwurfsbegründung, dass die Möglichkeit der Erlangung nachträglichen Rechtsschutzes eine unabdingbare Voraussetzung für die rechtsstaatliche Ausgestaltung verdeckter Ermittlungsmaßnahmen sei[115], ist uneingeschränkt zuzustimmen.

7. Löschung von Daten (§ 101 Abs. 10 StPO-E)

§ 101 Abs. 10 StPO-E betrifft nicht die Pflicht zur unverzüglichen Löschung von Aufzeichnungen solcher Informationen, die unzulässig erlangt sind (vgl. § 53b Absatz 1 Satz 4, § 100a Absatz 4 Satz 3, § 100d Absatz 5 Satz 3 StPO-E), sondern eine dem geltenden § 100d Abs. 5 StPO nachgebildete, redaktionell klarer gefasste Regelung über die Löschung nicht mehr benötigter personenbezogener Daten, die aus einer der in § 101

[115] BR-Drucks. 275/07, S. 141.

Abs. 1 StPO-E genannten Maßnahmen erlangt worden sind. Der Entwurf hat sich mit nachvollziehbaren Gründen[116] gegen feste Löschungsprüffristen entschieden.

* * *

116 BR-Drucks. 275/07, S. 144 f..