Gesetzentwurf
der Bundesregierung

Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG[1]

A. Problem und Ziel

Die Bundesregierung hat seit längerem angekündigt, ein harmonisches Gesamtsystem der strafprozessualen heimlichen Ermittlungsmethoden zu schaffen (vgl. bereits in der 14. Legislaturperiode: BR-Drs. 702/01, S. 10 f.). Um eine entsprechende Neuregelung auf eine tragfähige Grundlage zu stellen, die die Bedürfnisse der Strafverfolgungspraxis und den Diskussionsstand in der Rechtswissenschaft berücksichtigt, hat die Bundesregierung rechtswissenschaftliche und rechtstatsächliche Gutachten eingeholt (vgl. Wolter/Schenke [Hrsg.], Zeugnisverweigerungsrechte bei [verdeckten] Ermittlungsmaßnahmen, 2002; Albrecht/Dorsch/Krüpe, Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen, 2003; Meyer-Wieck, Rechtswirklichkeit und Effizienz der akustischen Wohnraumüberwachung [„großer Lauschangriff“] nach § 100c I Nr. 3 StPO, 2004). Auch Erfahrungsberichte der staatsanwaltschaftlichen und polizeilichen Praxis tragen hierzu bei. Die hieraus gewonnenen Erkenntnisse belegen insbesondere im Bereich der Telekommunikationsüberwachung einen Änderungsbedarf aufgrund technischer Neuerungen und Schwierigkeiten in der Strafverfolgungspraxis bei der Anwendung der bisherigen gesetzlichen Regelungen.

Änderungsbedarf ergibt sich darüber hinaus aus mehreren Entscheidungen des Bundesverfassungsgerichts:

Mit Urteil vom 27. Juli 2005 – 1 BvR 668/04 – (BVerfGE 113, 348, 391) hat das Bundesverfassungsgericht klargestellt, dass auch im Bereich der Telekommunikationsüberwachung Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung erforderlich sind. Diese für die Überwachung der Telekommunikation im präventiven Bereich aufgestellte Forderung ist auf den Bereich der Strafprozessordnung (StPO) zu übertragen.

---

[1] Dieses Gesetz dient (auch) der Umsetzung der Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (ABl. EU Nr. L 105 S. 54 ff.).

- Die Entscheidungen vom 4. Februar 2005 – 2 BvR 308/04 – (NJW 2005, 1637, 1639 f.) und vom 2. März 2006 – 2 BvR 2099/04 – (BVerfGE 115, 166 ff.) veranlassen eine Klarstellung, nach welchen Rechtsvorschriften bei der Erhebung von Verkehrsdaten von Datenträgern zu verfahren ist, wenn diese sich nach Abschluss des Kommunikationsvorgangs nicht im Herrschaftsbereich des Telekommunikationsdienstleisters befinden.

- Schließlich ist es erforderlich, die Rechtsprechung des Bundesverfassungsgerichts zum – auch nachträglichen – Rechtsschutz (BVerfGE 30, 1, 23 f., 30 f; 65, 1, 46; 67, 157, 185; 100, 313, 361 f., 364; 103, 142, 151; 105, 239, 248; 107, 299, 337 f.), zur Datenlöschung (BVerfGE 69, 1, 49; 100, 313, 364 f.), zur Datenverwendung (BVerfGE 100, 313, 360; 107, 299, 328; 109, 279, 374, 379 f.; 110, 33, 73, 75) und zu der die Ordnungsmäßigkeit der Datenverwendung ermöglichenden Kennzeichnungspflicht (BVerfGE 100, 313, 360; 109, 279, 374, 379 f.) konsequent auf alle eingriffsintensiven verdeckten Ermittlungsmaßnahmen zu übertragen.

Änderungsbedarf ergibt sich außerdem aus den Vorgaben des Übereinkommens des Europarats über Computerkriminalität (so genannte Cybercrime-Konvention), dessen Ratifizierung durch Deutschland demnächst erfolgen soll.

Umzusetzen in innerstaatliches Recht sind ferner die Vorgaben der am 3. Mai 2006 in Kraft getretenen Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (ABl. EU Nr. L 105 S. 54 ff.), insbesondere hinsichtlich der innerstaatlichen Einführung von Speicherungspflichten für Verkehrsdaten sowie darauf bezogener statistischer Erhebungen und Berichtspflichten. Artikel 15 der Richtlinie 2006/24/EG sieht grundsätzlich eine Umsetzung bis zum 15. September 2007 vor.

B. Lösung

Das Recht der verdeckten strafprozessualen Ermittlungsmaßnahmen, das in den §§ 98a bis 101, 110a bis 110e und 163d bis 163f StPO geregelt ist, wird einer umfassenden Überarbeitung unterzogen.

Der Gesetzentwurf soll – unter Wahrung der bisherigen Systematik – die verfahrensrechtlichen Voraussetzungen und grundrechtssichernden Ausgestaltungen der verdeckten strafprozessualen Ermittlungsmaßnahmen harmonisieren und diesen Regelungskomplex dadurch insgesamt übersichtlicher und rechtsstaatlichen Geboten entsprechend gestalten, zugleich aber auch praktische Erfordernisse berücksichtigen. Wo dies geboten ist, sollen einzelne Ermittlungsmaßnahmen auf eine klare, verfassungsrechtlich unbedenkliche Rechtsgrundlage gestellt werden. Neuen technischen Entwicklungen soll der Gesetzentwurf – wo dies erforderlich und zulässig ist, auch zukunftsoffen – Rechnung tragen. Die verdeckten Ermittlungsmaßnahmen, die in jüngerer Zeit gegenüber den herkömmlichen „offenen" Maßnahmen der Strafverfolgungsbehörden erheblich an Bedeutung gewonnen und sich als unverzichtbares Instrument erwiesen haben zur Bekämpfung von schwer ermittelbarer Kriminalität, Transaktions- und Wirtschaftskriminalität sowie von Straftaten, die unter Nutzung moderner Kommunikationstechnologien begangen werden, sollen übersichtlicher und normenklarer geregelt werden, um dadurch sowohl den Rechtsschutz der von solchen Maßnahmen Betroffenen als auch die Praktikabilität dieser Regelungen in der staatsanwaltschaftlichen und polizeilichen Praxis zu verbessern. Im Einzelnen:

- Die neue Vorschrift des § 53b StPO-E führt ein harmonisiertes System zur Berücksichtigung der von den Zeugnisverweigerungsrechten der Berufsgeheimnisträger (§§ 53, 53a StPO) geschützten Interessen außerhalb der Vernehmungssituation ein.

- § 101 StPO-E wird zu einer die Regelungen der §§ 98a ff. StPO systematisch abschließenden Vorschrift umgestaltet:

Die bei allen eingriffsintensiveren verdeckten Ermittlungsmaßnahmen (Rasterfahndung, Postbeschlagnahme, Telekommunikationsüberwachung, akustische Überwachung innerhalb und außerhalb von Wohnungen, Verkehrsdatenerhebung, technische und langfristige Observation, Einsatz Verdeckter Ermittler, Schleppnetzfahndung, Ausschreibung zur polizeilichen Beobachtung) nach der Rechtsprechung des Bundesverfassungsgerichts (BVerfGE 100, 313 ff. – G 10-Gesetz; BVerfGE 109, 279 ff. – akustische Wohnraumüberwachung; BVerfGE 113, 348 ff. – Niedersächsisches SOG) gebotenen grundrechtssichernden Verfahrensregelungen werden dort allgemein und übersichtlich zusammengefasst, indem geregelt werden:

  - die Pflicht zur Kennzeichnung der durch verdeckte Ermittlungsmaßnahmen erlangten Erkenntnisse; damit wird sichergestellt, dass die für eingriffsintensive verdeckte Ermittlungsmaßnahmen geltenden beschränkenden Verwendungsregelungen (vgl. auch § 161 Abs. 2, § 477 Abs. 2 StPO-E) Beachtung finden können;

- die nachträgliche Benachrichtigung der von verdeckten Ermittlungsmaßnahmen betroffenen Personen;

- der zu benachrichtigende Personenkreis; durch die maßnahmespezifische Beschreibung dieses Kreises und konkreter Vorgaben, unter welchen Voraussetzungen von einer Benachrichtigung abzusehen oder diese zurückzustellen ist, werden Auslegungsunsicherheiten in der Praxis beseitigt;

- das Erfordernis einer – ggf. mehrfachen – gerichtlichen Zustimmung zur Zurückstellung der Benachrichtigung;

- die Möglichkeit eines nachträglichen – auch nach Erledigung der Maßnahme eingreifenden – gerichtlichen Rechtsschutzes für die von verdeckten Ermittlungsmaßnahmen betroffenen Personen;

- die Pflicht zur Löschung der aus verdeckten Ermittlungsmaßnahmen erlangten Erkenntnisse, sobald diese für Zwecke der Strafverfolgung sowie für einen etwaigen gerichtlichen Rechtschutz nicht mehr erforderlich sind.

- Die „Umwidmung“ der durch verdeckte Ermittlungsmaßnahmen erlangten Daten zur Verwendung als Beweismittel in anderen Strafverfahren und die Verwendung der durch verdeckte Ermittlungsmaßnahmen auf anderer – insbesondere präventiv-polizeilicher – Rechtsgrundlage erlangten Daten als Beweismittel in Strafverfahren wird, soweit die betreffenden Maßnahmen nach der Strafprozessordnung nur bei Verdacht bestimmter Straftaten zulässig sind, einheitlich davon abhängig gemacht, ob sich der neue Verwendungszweck ebenfalls auf Straftaten bezieht, die die Anwendung der Maßnahme nach der Strafprozessordnung erlauben (§ 161 Abs. 2, § 477 Abs. 2 StPO-E).

- Der Katalog der Anlassstraftaten, die Voraussetzung für eine Telekommunikationsüberwachung nach § 100a StPO sind, wird systematisch neu geordnet, inhaltlich überarbeitet und auf – auch im Einzelfall – schwere Straftaten beschränkt (§ 100a Abs. 1 und 2 StPO-E).

- Durch § 100a Abs. 4 StPO-E wird der Schutz des Kernbereichs privater Lebensgestaltung entsprechend den Vorgaben des Bundesverfassungsgerichts auch bei der Telekommunikationsüberwachung gewährleistet.

- Dem durch das Übereinkommen über Computerkriminalität des Europarats veranlassten Regelungsbedarf wird durch die Umgestaltung des § 100g StPO in eine Datenerhebungs-

befugnis und die Erstreckung der Befugnis zur Durchsicht von Datenträgern auf mit diesen vernetzte – aber räumlich getrennte – Speichermedien (§ 110 Abs. 3 StPO-E) nachgekommen.

- Durch die Schaffung einer Konzentrationsregelung für die Vornahme gerichtlicher Untersuchungshandlungen wird die mit dem Richtervorbehalt bezweckte rechtsstaatliche Kontrolle gestärkt (§ 162 Abs. 1 StPO-E).

- Auch bei den einzelnen Ermittlungsanordnungen wird die mit dem Richtervorbehalt bezweckte Kontrolle durch eine Harmonisierung der Anordnungskompetenzen und der Anordnungsdauer gestärkt (§ 100b Abs. 1 sowie § 100f Abs. 4, § 100g Abs. 2 Satz 1, § 100i Abs. 3, § 163f Abs. 3 Satz 3 jeweils i. V. m. § 100b Abs. 1 StPO-E).

- Zur Umsetzung der Richtlinie zur „Vorratsspeicherung“ von Verkehrsdaten werden im Telekommunikationsgesetz (insbesondere in den §§ 113a, 113b TKG-E) Regelungen über entsprechende Speicherungspflichten sowie in der Strafprozessordnung (§ 100g StPO-E) Regelungen über darauf bezogene statistische Erhebungen und Berichtspflichten geschaffen.

- Ferner wird mit § 100b Abs. 5 und 6 StPO-E eine einheitliche Bestimmung für statistische Erhebungen zu Telekommunikationsüberwachungsmaßnahmen nach § 100a StPO-E geschaffen, die § 110 Abs. 8 TKG ablöst und für die schon bislang erfolgenden statistischen Mitteilungen der Landesjustizverwaltungen und des Generalbundesanwalts beim Bundesgerichtshof eine ausdrückliche gesetzliche Regelung schafft.

- Aus Anlass der Einbeziehung von Steuerstraftaten in den Anlassstraftatenkatalog des § 100a Abs. 2 StPO-E beseitigt der Entwurf zudem Wertungswidersprüche und Problemkonstellationen in den §§ 370 ff. der Abgabenordnung (AO).

C. Alternativen

Keine.

D. Kosten der öffentlichen Haushalte

1. Haushaltsausgaben ohne Vollzugsaufwand

Keine.

2. Vollzugsaufwand

Die Neufassung der Regelung der verdeckten Ermittlungsmaßnahmen in der Strafprozessordnung (Artikel 1 des Gesetzentwurfs) wird für die Strafverfolgungsbehörden und Gerichte des Bundes und der Länder voraussichtlich sowohl zu Mehr- als auch zu Minderaufwand führen. In der Gesamtbetrachtung ist zu erwarten, dass der Mehr- und Minderaufwand sich annähernd ausgleichen wird, so dass die Neufassung der Regelungen zu verdeckten Ermittlungsmaßnahmen in der Strafprozessordnung eine aufwandsneutrale Wirkung hat.

Durch die Änderung der Vorschriften des Telekommunikationsgesetzes in Artikel 2 entsteht bei der Bundesnetzagentur sich in Sachinvestitionen und Personalkosten aufgliedernder zusätzlicher Vollzugsaufwand, den das Bundesministerium für Wirtschaft und Technologie wie folgt veranschlagt: Im Bereich des Automatisierten Auskunftsverfahrens nach § 112 TKG werden für die Erweiterung des Systems Investitionskosten in Höhe von einer Million Euro erwartet. Gleichzeitig ist für die qualifizierte Planung und Fortschreibung des Projektes ein personeller Bedarf von zwei Kräften des gehobenen Dienstes und zwei Kräften des mittleren Dienstes zu erwarten. Dies wird durch die Erweiterung der Abfragemöglichkeiten um E-Mail-Adressen und die damit verbundene Verfünffachung der anzuschließenden Unternehmen verursacht. Schließlich entsteht durch die Verpflichtung zur Verkehrsdatenspeicherung ein erhöhter Kontrollaufwand im Rahmen der Aufsicht nach § 115 TKG einschließlich der Anwendung der neuen Bußgeldtatbestände, der zwei Stellen des höheren Dienstes mit juristischer Vorbildung sowie zwei Kräfte des gehobenen Dienstes erforderlich macht. Damit ist ein Personalkostenaufwand in Höhe von insgesamt rd. 640.000 Euro pro Jahr zu erwarten.

Für die Kommunen entsteht kein Vollzugsaufwand.

E. Sonstige Kosten

Für die von der Speicherungspflicht für Verkehrsdaten betroffenen Unternehmen entsteht durch die Erfüllung der in den §§ 111, 113a TKG-E vorgesehenen Speicherungspflichten zusätzlicher Aufwand, der durch an anderer Stelle im Entwurf vorgesehene Entlastungen der Unternehmen nur zu einem geringen Teil kompensiert werden kann. Abhängig von der jeweiligen Größe des betroffenen Unternehmens und dessen bisheriger Handhabung bei der Speicherung der Daten kann der Mehraufwand zwischen einigen Tausend und mehreren Hunderttausend Euro betragen. Es ist zu erwarten, dass die betroffenen Unternehmen die zusätzlichen Kosten bei ihrer Preisgestaltung einkalkulieren und - soweit der der EU-weit von der Speicherungspflicht betroffene Telekommunikationsmarkt dies zulässt - an die Kunden weiter geben werden. Das Verbraucherpreisniveau im Bereich der Telekommunikationsdienstleistungen kann daher geringfügig steigen.

Darüber hinaus entstehen für die Wirtschaft, insbesondere mittelständische Unternehmen, keine Kosten. Weitere Auswirkungen auf Einzelpreise, das allgemeine Preisniveau und insbesondere das Verbraucherpreisniveau sind damit nicht zu erwarten.

F. Bürokratiekosten

Die Ressortabstimmung wurde vor dem 1. Dezember 2006 eingeleitet.

Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG[1]

Vom ...

Der Deutsche Bundestag hat das folgende Gesetz beschlossen:

Artikel 1
Änderung der Strafprozessordnung

Die Strafprozessordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), zuletzt geändert durch ..., wird wie folgt geändert:

1. Nach § 53a wird folgender § 53b eingefügt:

„§ 53b

(1) Eine Ermittlungsmaßnahme, die sich gegen eine in § 53 Abs. 1 Satz 1 Nr. 1, 2 oder Nr. 4 genannte Person richtet und voraussichtlich Erkenntnisse erbringen würde, über die diese Person das Zeugnis verweigern dürfte, ist unzulässig. Dennoch erlangte Erkenntnisse dürfen nicht verwertet werden. Aufzeichnungen hierüber sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und der Löschung der Aufzeichnungen ist aktenkundig zu machen. Die Sätze 2 bis 4 gelten entsprechend, wenn durch eine Ermittlungsmaßnahme, die sich nicht gegen eine in § 53 Abs. 1 Satz 1 Nr. 1, 2 oder Nr. 4 genannte Person richtet, von einer dort genannten Person Erkenntnisse erlangt werden, über die sie das Zeugnis verweigern dürfte.

(2) Soweit durch eine Ermittlungsmaßnahme eine in § 53 Abs. 1 Satz 1 Nr. 3 bis 3b oder Nr. 5 genannte Person betroffen wäre und dadurch voraussichtlich Erkenntnisse erlangt würden, über die diese Person das Zeugnis verweigern dürfte, ist dies im Rahmen der Prüfung der Verhältnismäßigkeit unter Würdigung des öffentlichen Interesses

[1] Dieses Gesetz dient (auch) der Umsetzung der Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (ABl. EU Nr. L 105 S. 54 ff.).

an den von dieser Person wahrgenommenen Aufgaben und des Interesses an der Geheimhaltung der dieser Person anvertrauten oder bekannt gewordenen Tatsachen besonders zu berücksichtigen. Soweit hiernach geboten, ist die Maßnahme zu unterlassen oder, soweit dies nach der Art der Maßnahme möglich ist, zu beschränken. Für die Verwertung von Erkenntnissen zu Beweiszwecken gilt Satz 1 entsprechend.

(3) Die Absätze 1 und 2 sind entsprechend anzuwenden, soweit die in § 53a Genannten das Zeugnis verweigern dürften.

(4) Die Absätze 1 bis 3 sind nicht anzuwenden, soweit gegen die zeugnisverweigerungsberechtigte Person ein Strafverfahren wegen des Verdachts der Beteiligung an der Tat oder der Begünstigung, Strafvereitelung oder Hehlerei eingeleitet ist. Ist die Tat nur auf Antrag oder nur mit Ermächtigung verfolgbar, ist Satz 1 in den Fällen des § 53 Abs. 1 Satz 1 Nr. 5 anzuwenden, sobald und soweit der Strafantrag gestellt oder die Ermächtigung erteilt ist.

(5) Die §§ 97 und 100c Abs. 6 bleiben unberührt.“

2. In § 58a Abs. 2 Satz 2 wird die Angabe „§ 100b Abs. 6“ durch die Angabe „§ 101 Abs. 10“ ersetzt.

3. § 97 wird wie folgt geändert:

a) Absatz 2 wird wie folgt geändert:

aa) In Satz 1 wird vor dem Wort „Gesundheitskarte“ das Wort „elektronische“ eingefügt.

bb) Satz 3 wird wie folgt gefasst:

„Die Beschränkungen der Beschlagnahme gelten nicht, wenn gegen die zur Verweigerung des Zeugnisses Berechtigten ein Strafverfahren wegen des Verdachts der Beteiligung an der Tat oder der Begünstigung, Strafvereitelung oder Hehlerei eingeleitet ist oder wenn es sich um Gegenstände han-

delt, die durch eine Straftat hervorgebracht oder zur Begehung einer Straftat gebraucht oder bestimmt sind oder die aus einer Straftat herrühren.“

b) In Absatz 5 Satz 2 wird das Wort „gilt“ durch die Wörter „und § 53b Abs. 4 Satz 2 gelten“ ersetzt.

4. § 98 wird wie folgt geändert:

a) In Absatz 1 Satz 1 und 2 werden jeweils die Wörter „den Richter“ durch die Wörter „das Gericht“ ersetzt.

b) Absatz 2 wird wie folgt geändert:

aa) In Satz 1 und 2 wird jeweils das Wort „richterliche“ durch das Wort „gerichtliche“ ersetzt.

bb) Die Sätze 3 bis 6 werden durch folgende Sätze ersetzt:

„Solange die öffentliche Klage noch nicht erhoben ist, entscheidet das nach § 162 Abs. 1 zuständige Gericht. Ist die öffentliche Klage erhoben, entscheidet das damit befasste Gericht. Der Betroffene kann den Antrag auch bei dem Amtsgericht einreichen, in dessen Bezirk die Beschlagnahme stattgefunden hat; dieses leitet den Antrag dem zuständigen Gericht zu.“

c) In Absatz 3 wird das Wort „Richter“ durch das Wort „Gericht“ ersetzt.

5. § 98b wird wie folgt geändert:

a) Absatz 1 wird wie folgt geändert:

aa) In Satz 1 werden die Wörter „den Richter“ durch die Wörter „das Gericht“ ersetzt.

bb) In Satz 2 wird das Wort „richterliche“ durch das Wort „gerichtliche“ ersetzt.

cc) In Satz 3 wird das Wort „Richter“ durch das Wort „Gericht“ ersetzt.

b) In Absatz 2 Satz 1 werden die Wörter „den Richter“ durch die Wörter „das Gericht“ und die Wörter „dem Richter“ durch die Wörter „dem Gericht“ ersetzt.

c) Absatz 3 Satz 3 wird aufgehoben.

d) Absatz 4 wird wie folgt geändert:

aa) Satz 1 wird aufgehoben.

bb) In dem bisherigen Satz 2 wird das Wort „gemäß“ durch das Wort „nach“ ersetzt.

6. § 100 wird wie folgt geändert:

a) In Absatz 1 werden die Wörter „der Richter“ durch die Wörter „das Gericht“ ersetzt.

b) In Absatz 2 werden die Wörter „von dem Richter“ durch das Wort „gerichtlich“ ersetzt.

c) Absatz 3 wird wie folgt geändert:

aa) In Satz 1 wird das Wort „Gegenstände“ durch das Wort „Postsendungen“ und das Wort „Richter“ durch das Wort „Gericht“ ersetzt.

bb) In Satz 2 wird das Wort „Er“ durch das Wort „Es“ ersetzt.

cc) In Satz 4 werden das Wort „Gegenstände“ durch das Wort „Postsendungen“ und das Wort „Richter“ durch das Wort „Gericht“ ersetzt.

d) Absatz 4 wird wie folgt geändert:

aa) In Satz 1 werden die Wörter „der nach § 98 zuständige Richter“ durch die Wörter „das nach § 98 zuständige Gericht“ ersetzt.

bb) In Satz 2 werden die Wörter „eines ausgelieferten Gegenstandes“ durch die Wörter „einer ausgelieferten Postsendung“ und die Wörter „der Richter, der“ durch die Wörter „das Gericht, das“ ersetzt.

e) Folgende Absätze 5 bis 6 werden angefügt:

„(5) Postsendungen, deren Öffnung nicht angeordnet worden ist, sind unverzüglich an den vorgesehenen Empfänger weiter zu leiten. Dasselbe gilt, soweit nach der Öffnung die Zurückbehaltung nicht erforderlich ist.

(6) Der Teil einer zurückbehaltenen Postsendung, dessen Vorenthaltung nicht mit Rücksicht auf die Untersuchung geboten erscheint, ist dem vorgesehenen Empfänger abschriftlich mitzuteilen.“

7. Die §§ 100a und 100b werden wie folgt gefasst:

„§ 100a

(1) Auch ohne Wissen der Betroffenen darf die Telekommunikation überwacht und aufgezeichnet werden, wenn

1. bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in Absatz 2 bezeichnete schwere Straftat begangen, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht, oder durch eine Straftat vorbereitet hat,

2. die Tat auch im Einzelfall schwer wiegt und

3. die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre.

(2) Schwere Straftaten im Sinne des Absatzes 1 Nr. 1 sind:

1. aus dem Strafgesetzbuch:

a) Straftaten des Friedensverrats, des Hochverrats und der Gefährdung des demokratischen Rechtsstaates sowie des Landesverrats und der Gefährdung der äußeren Sicherheit nach den §§ 80 bis 82, 84 und 85, 87 bis 89, 94 bis 100a,

b) Abgeordnetenbestechung nach § 108e,

c) Straftaten gegen die Landesverteidigung nach den §§ 109d bis 109h,

d) Straftaten gegen die öffentliche Ordnung nach den §§ 129 bis 130,

e) Geld- und Wertzeichenfälschung nach den §§ 146 und 151, jeweils auch in Verbindung mit § 152, sowie nach § 152a Abs. 3 und § 152b Abs. 1 bis 4,

f) Straftaten gegen die sexuelle Selbstbestimmung in den Fällen der §§ 176a, 176b, 177 Abs. 2 Nr. 2 und des § 179 Abs. 5 Nr. 2,

g) Verbreitung, Erwerb und Besitz kinderpornografischer Schriften nach § 184b Abs. 1 bis 3,

h) Mord und Totschlag nach den §§ 211 und 212,

i) Straftaten gegen die persönliche Freiheit nach den §§ 232 bis 233a, 234, 234a, 239a und 239b,

j) Bandendiebstahl nach § 244 Abs. 1 Nr. 2 und schwerer Bandendiebstahl nach § 244a,

k) Straftaten des Raubes und der Erpressung nach den §§ 249 bis 255,

l) gewerbsmäßige Hehlerei, Bandenhehlerei und gewerbsmäßige Bandenhehlerei nach den §§ 260 und 260a,

m) Geldwäsche und Verschleierung unrechtmäßig erlangter Vermögenswerte nach § 261 Abs. 1, 2 und 4,

n) Betrug und Computerbetrug unter den in § 263 Abs. 3 Satz 2 genannten Voraussetzungen und im Falle des § 263 Abs. 5, jeweils auch in Verbindung mit § 263a Abs. 2,

o) Subventionsbetrug unter den in § 264 Abs. 2 Satz 2 genannten Voraussetzungen und im Falle des § 264 Abs. 3 in Verbindung mit § 263 Abs. 5,

p) Straftaten der Urkundenfälschung unter den in § 267 Abs. 3 Satz 2 genannten Voraussetzungen und im Fall des § 267 Abs. 4, jeweils auch in Verbindung mit § 268 Abs. 5 oder § 269 Abs. 3, sowie nach § 275 Abs. 2 und § 276 Abs. 2,

q) Bankrott unter den in § 283a Satz 2 genannten Voraussetzungen,

r) Straftaten gegen den Wettbewerb nach § 298 und, unter den in § 300 Satz 2 genannten Voraussetzungen, nach § 299,

s) gemeingefährliche Straftaten in den Fällen der §§ 306 bis 306c, 307 Abs. 1 bis 3, des § 308 Abs. 1 bis 3, des § 309 Abs. 1 bis 4, des § 310 Abs. 1, der §§ 313, 314, 315 Abs. 3, des § 315b Abs. 3 sowie der §§ 316a und 316c,

t) Bestechlichkeit und Bestechung nach den §§ 332 und 334;

2. aus der Abgabenordnung:

a) Steuerhinterziehung unter den in § 370 Abs. 3 Satz 2 Nr. 5 genannten Voraussetzungen,

b) gewerbsmäßiger, gewaltsamer und bandenmäßiger Schmuggel nach § 373,

c) Steuerhehlerei im Falle des § 374 Abs. 2,

3. aus dem Arzneimittelgesetz:

Straftaten nach § 95 Abs. 1 Nr. 2a unter den in § 95 Abs. 3 Satz 2 Nr. 2 Buchstabe b genannten Voraussetzungen,

4. aus dem Asylverfahrensgesetz:

a) Verleitung zur missbräuchlichen Asylantragstellung nach § 84 Abs. 3,

b) gewerbs- und bandenmäßige Verleitung zur missbräuchlichen Asylantragstellung nach § 84a,

5. aus dem Aufenthaltsgesetz:

a) Einschleusen von Ausländern nach § 96 Abs. 2,

b) Einschleusen mit Todesfolge und gewerbs- und bandenmäßiges Einschleusen nach § 97,

6. aus dem Außenwirtschaftsgesetz:

Straftaten nach § 34 Abs. 1 bis 6,

7. aus dem Betäubungsmittelgesetz:

a) Straftaten nach einer in § 29 Abs. 3 Satz 2 Nr. 1 in Bezug genommenen Vorschrift unter den dort genannten Voraussetzungen,

b) Straftaten nach den §§ 29a, 30 Abs. 1 Nr. 1, 2 und 4 sowie den §§ 30a und 30b,

8. aus dem Gesetz über die Kontrolle von Kriegswaffen:

a) Straftaten nach § 19 Abs. 1 bis 3 und § 20 Abs. 1 und 2 sowie § 20a Abs. 1 bis 3, jeweils auch in Verbindung mit § 21,

b) Straftaten nach § 22a Abs. 1 bis 3,

9. aus dem Völkerstrafgesetzbuch:

a) Völkermord nach § 6,

b) Verbrechen gegen die Menschlichkeit nach § 7,

c) Kriegsverbrechen nach den §§ 8 bis 12,

10. aus dem Waffengesetz:

a) Straftaten nach § 51 Abs. 1 bis 3,

b) Straftaten nach § 52 Abs. 1 Nr. 1, 2 Buchstabe c und d sowie Abs. 5 und 6,

(3) Die Anordnung darf sich nur gegen den Beschuldigten oder gegen Personen richten, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Beschuldigte ihren Anschluss benutzt.

(4) Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch eine Maßnahme nach Absatz 1 allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, ist die Maßnahme unzulässig. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch eine Maßnahme nach Absatz 1 erlangt wurden, dürfen nicht verwertet werden. Aufzeichnungen hierüber sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und Löschung ist aktenkundig zu machen.

§ 100b

(1) Maßnahmen nach § 100a dürfen nur auf Antrag der Staatsanwaltschaft durch das Gericht angeordnet werden. Bei Gefahr im Verzug kann die Anordnung auch durch die Staatsanwaltschaft getroffen werden. Soweit die Anordnung der Staatsanwaltschaft nicht binnen drei Werktagen von dem Gericht bestätigt wird, tritt sie außer Kraft; zwischenzeitlich erlangte personenbezogene Daten dürfen zu Beweiszwecken nur verwertet werden, wenn Gefahr im Verzug bestand. Die Anordnung ist auf höchstens zwei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als zwei Monate ist zulässig, soweit die Voraussetzungen der Anordnung unter Berücksichtigung der gewonnenen Ermittlungsergebnisse fortbestehen. Ist die Dauer der Anordnung auf insgesamt sechs Monate verlängert worden, so entscheidet über weitere Verlängerungen vorbehaltlich des § 169 das im Rechtszug übergeordnete Gericht.

(2) Die Anordnung ergeht schriftlich. In ihrer Entscheidungsformel sind anzugeben:

1. soweit möglich, der Name und die Anschrift des Betroffenen, gegen den sich die Maßnahme richtet,

2. die Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses oder des Endgerätes, wenn diese allein dem zu überwachenden Endgerät zuzuordnen ist,

3. Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunktes.

(3) Auf Grund der Anordnung hat jeder, der Telekommunikationsdienste erbringt oder daran mitwirkt, dem Gericht, der Staatsanwaltschaft und ihren im Polizeidienst tätigen Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) die Maßnahmen nach § 100a zu ermöglichen und die erforderlichen Auskünfte zu erteilen. Ob und in welchem Umfang hierfür Vorkehrungen zu treffen sind, bestimmt sich nach dem Telekommunikationsgesetz und der Telekommunikations-Überwachungsverordnung. § 95 Abs. 2 gilt entsprechend.

(4) Liegen die Voraussetzungen der Anordnung nicht mehr vor, so sind die auf Grund der Anordnung ergriffenen Maßnahmen unverzüglich zu beenden. Nach Beendigung der Maßnahme ist das anordnende Gericht über deren Verlauf und Ergebnisse zu unterrichten.

(5) Die Länder und der Generalbundesanwalt berichten dem Bundesamt für Justiz kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres über in ihrem Zuständigkeitsbereich angeordnete Maßnahmen nach § 100a. Das Bundesamt für Justiz erstellt eine Übersicht zu den im Berichtsjahr bundesweit angeordneten Maßnahmen und veröffentlicht diese im Internet[1].

(6) In den Berichten nach Absatz 5 sind anzugeben:

1. die Anzahl der Verfahren, in denen Maßnahmen nach § 100a Abs. 1 angeordnet worden sind;

2. die Anzahl der Überwachungsanordnungen nach § 100a Abs. 1, unterschieden nach

a) Erst- und Verlängerungsanordnungen sowie

b) Festnetz-, Mobilfunk- und Internettelekommunikation;

3. die jeweils zugrunde liegende Anlassstraftat nach Maßgabe der Unterteilung in § 100a Abs. 2;

4. die Anzahl der überwachten Telekommunikationsvorgänge nach Maßgabe der Unterteilung in Nummer 2 Buchstabe b.“

8. § 100c wird wie folgt geändert:

a) Absatz 1 wird wie folgt geändert:

aa) Das Wort „Ohne“ wird durch die Wörter „Auch ohne“ ersetzt.

bb) In Nummer 1 werden nach dem Wort „jemand“ die Wörter „als Täter oder Teilnehmer“ eingefügt.

b) Absatz 2 Nr. 1 wird wie folgt geändert:

aa) In Buchstabe a wird das Wort „oder“ durch das Wort „sowie“ ersetzt.

bb) Buchstabe c wird wie folgt gefasst:

„c) Geld- und Wertzeichenfälschung nach den §§ 146 und 151, jeweils auch in Verbindung mit § 152, sowie nach § 152a Abs. 3 und § 152b Abs. 1 bis 4,“.

c) Absatz 6 Satz 3 wird wie folgt gefasst:

„§ 53b Abs. 4 gilt entsprechend.“

---

[1] Amtlicher Hinweis: Die Internetadresse des Bundesamtes für Justiz lautet: www.bundesjustizamt.de

9. § 100d wird wie folgt geändert:

a) In Absatz 2 Satz 2 Nr. 1 wird das Wort „bekannt“ durch das Wort „möglich,“ ersetzt.

b) Absatz 5 wird aufgehoben.

c) Absatz 6 wird Absatz 5 und wie folgt geändert:

aa) In dem Satzteil vor Nummer 1 und in Nummer 1 wird das Wort „Informationen“ durch das Wort „Daten“ ersetzt.

bb) Nummer 2 wird wie folgt geändert:

aaa) In Satz 1 und 2 wird jeweils das Wort „Informationen“ durch das Wort „Daten“ ersetzt.

bbb) In Satz 3 werden das Wort „Informationen“ jeweils durch das Wort „Daten“ und das Wort „vernichten“ durch das Wort „löschen“ ersetzt.

ccc) Die Sätze 4 und 5 werden wie folgt gefasst:

„Die Löschung ist aktenkundig zu machen. Soweit die Löschung lediglich für eine etwaige vorgerichtliche oder gerichtliche Überprüfung zurückgestellt ist, dürfen die Daten nur für diesen Zweck verwendet werden; für eine Verwendung zu anderen Zwecken sind sie zu sperren.“

cc) In Nummer 3 werden das Wort „Informationen“ durch das Wort „Daten“ und die Wörter „diese Informationen“ durch das Wort „sie“ ersetzt.

d) Die Absätze 7 bis 10 werden aufgehoben.

10. § 100e wird wie folgt geändert:

a) Absatz 1 wird wie folgt gefasst:

„(1) Für die nach § 100c angeordneten Maßnahmen gilt § 100b Abs. 5 entsprechend. Vor der Veröffentlichung im Internet berichtet die Bundesregierung dem Deutschen Bundestag über die im jeweils vorangegangenen Kalenderjahr nach § 100c angeordneten Maßnahmen.“

b) In Absatz 2 Satz 1 Nr. 8 wird die Angabe „(§ 100d Abs. 8)“ durch die Angabe „(§ 101 Abs. 4 bis 7)“ ersetzt.

11. Die §§ 100f bis 101 werden wie folgt gefasst:

„§ 100f

(1) Auch ohne Wissen der Betroffenen darf außerhalb von Wohnungen das nichtöffentlich gesprochene Wort mit technischen Mitteln abgehört und aufgezeichnet werden, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand eine in § 100a Abs. 2 bezeichnete Straftat begangen hat, und die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre.

(2) Die Maßnahme darf sich nur gegen einen Beschuldigten richten. Gegen andere Personen darf die Maßnahme nur angeordnet werden, wenn auf Grund bestimmter Tatsachen anzunehmen ist, dass sie mit einem Beschuldigten in Verbindung stehen oder eine solche Verbindung hergestellt wird, die Maßnahme zur Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsortes eines Beschuldigten führen wird und dies auf andere Weise aussichtslos oder wesentlich erschwert wäre.

(3) Die Maßnahme darf auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.

(4) § 100b Abs. 1, 4 Satz 1 und § 100d Abs. 2 gelten entsprechend.

§ 100g

(1) Begründen bestimmte Tatsachen den Verdacht, dass jemand als Täter oder Teilnehmer

1. eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Abs. 2 bezeichnete Straftat, begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat oder durch eine Straftat vorbereitet hat oder

2. eine Straftat mittels Telekommunikation begangen hat,

so dürfen auch ohne Wissen des Betroffenen Verkehrsdaten (§ 96 Abs. 1, § 113a des Telekommunikationsgesetzes) erhoben werden, soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich ist. Im Falle des Satzes 1 Nr. 2 ist die Maßnahme nur zulässig, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos wäre und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht. Die Erhebung von Standortdaten in Echtzeit ist nur im Falle des Satzes 1 Nr. 1 zulässig.

(2) § 100a Abs. 3 und § 100b Abs. 1 bis 4 Satz 1 gelten entsprechend. Abweichend von § 100b Abs. 2 Satz 2 Nr. 2 genügt im Falle einer Straftat von erheblicher Bedeutung eine räumlich und zeitlich hinreichend bestimmte Bezeichnung der Telekommunikation, wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre.

(3) Erfolgt die Erhebung von Verkehrsdaten nicht beim Telekommunikationsdiensteanbieter, bestimmt sie sich nach Abschluss des Kommunikationsvorgangs nach den allgemeinen Vorschriften.

(4) Über Maßnahmen nach Absatz 1 ist entsprechend § 100b Abs. 5 jährlich eine Übersicht zu erstellen, in der anzugeben sind:

1. die Anzahl der Verfahren, in denen Maßnahmen nach Absatz 1 durchgeführt worden sind;

2. die Anzahl der Anordnungen von Maßnahmen nach Absatz 1, unterschieden nach Erst- und Verlängerungsanordnungen;

3. die jeweils zugrunde liegende Anlassstraftat, unterschieden nach Absatz 1 Satz 1 Nr. 1 und 2;

4. die Anzahl der zurückliegenden Monate, für die Verkehrsdaten nach Absatz 1 abgefragt wurden, bemessen ab dem Zeitpunkt der Anordnung;

5. die Anzahl der Maßnahmen, die ergebnislos geblieben sind, weil die abgefragten Daten ganz oder teilweise nicht verfügbar waren.

§ 100h

(1) Auch ohne Wissen der Betroffenen dürfen außerhalb von Wohnungen

1. Bildaufnahmen hergestellt werden,

2. sonstige besondere für Observationszwecke bestimmte technische Mittel verwendet werden,

wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Beschuldigten auf andere Weise weniger erfolgversprechend oder erschwert wäre. Eine Maßnahme nach Satz 1 Nr. 2 ist nur zulässig, wenn Gegenstand der Untersuchung eine Straftat von erheblicher Bedeutung ist.

(2) Die Maßnahmen dürfen sich nur gegen einen Beschuldigten richten. Gegen andere Personen sind

1. Maßnahmen nach Absatz 1 Nr. 1 nur zulässig, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Beschuldigten auf andere Weise erheblich weniger erfolgversprechend oder wesentlich erschwert wäre,

2. Maßnahmen nach Absatz 1 Nr. 2 nur zulässig, wenn auf Grund bestimmter Tatsachen anzunehmen ist, dass sie mit einem Beschuldigten in Verbindung stehen oder eine solche Verbindung hergestellt wird, die Maßnahme zur Erforschung des Sach-

verhalts oder zur Ermittlung des Aufenthaltsortes eines Beschuldigten führen wird und dies auf andere Weise aussichtslos oder wesentlich erschwert wäre.

(3) Die Maßnahmen dürfen auch durchgeführt werden, wenn Dritte unvermeidbar mitbetroffen werden.

§ 100i

(1) Begründen bestimmte Tatsachen den Verdacht, dass jemand eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Abs. 2 bezeichnete Straftat, begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat oder durch eine Straftat vorbereitet hat, so dürfen durch technische Mittel

1. die Gerätenummer eines Mobilfunkendgerätes und die Kartennummer der darin verwendeten Karte sowie

2. der Standort eines Mobilfunkendgeräts

ermittelt werden, soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich ist.

(2) Personenbezogene Daten Dritter dürfen anlässlich solcher Maßnahmen nur erhoben werden, wenn dies aus technischen Gründen zur Erreichung des Zwecks nach Absatz 1 unvermeidbar ist. Über den Datenabgleich zur Ermittlung der gesuchten Geräte- und Kartennummer hinaus dürfen sie nicht verwendet werden und sind nach Beendigung der Maßnahme unverzüglich zu löschen.

(3) § 100a Abs. 3 und § 100b Abs. 1 Satz 1 bis 3, Abs. 2 Satz 1 und Abs. 4 Satz 1 gelten entsprechend. Die Anordnung ist auf höchstens sechs Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als sechs weitere Monate ist zulässig, soweit die in Absatz 1 bezeichneten Voraussetzungen fortbestehen.

§ 101

(1) Für Maßnahmen nach den §§ 98a, 99, 100a, 100c bis 100i, 110a, 163d bis 163f gelten, soweit nichts anderes bestimmt ist, die nachstehenden Regelungen.

(2) Entscheidungen und sonstige Unterlagen über Maßnahmen nach den §§ 100c, 100f, 100h Abs. 1 Nr. 2 und § 110a werden bei der Staatsanwaltschaft verwahrt. Zu den Akten sind sie erst zu nehmen, wenn die Voraussetzungen für eine Benachrichtigung nach Absatz 5 erfüllt sind.

(3) Personenbezogene Daten, die durch Maßnahmen nach Absatz 1 erhoben wurden, sind entsprechend zu kennzeichnen. Nach einer Übermittlung an eine andere Stelle ist die Kennzeichnung durch diese aufrechtzuerhalten.

(4) Von den in Absatz 1 genannten Maßnahmen sind im Falle

1. des § 98a die betroffenen Personen, gegen die nach Auswertung der Daten weitere Ermittlungen geführt wurden,

2. des § 99 der Absender und der Adressat der Postsendung,

3. des § 100a die Beteiligten der überwachten Telekommunikation,

4. des § 100c

   a) der Beschuldigte, gegen den sich die Maßnahme richtete,

   b) sonstige überwachte Personen,

   c) Personen, die die überwachte Wohnung zur Zeit der Durchführung der Maßnahme innehatten oder bewohnten,

5. des § 100f die Zielperson sowie die erheblich mitbetroffenen Personen,

6. des § 100g die Beteiligten der betroffenen Telekommunikation,

7. des § 100h Abs. 1 die Zielperson sowie die erheblich mit betroffenen Personen,

8. des § 100i die Zielperson,

9. des § 110a

   a) die Zielperson,

   b) die erheblich mitbetroffenen Personen,

   c) die Personen, deren nicht allgemein zugängliche Wohnung der Verdeckte Ermittler betreten hat,

10. des § 163d die betroffenen Personen, gegen die nach Auswertung der Daten weitere Ermittlungen geführt wurden,

11. des § 163e die Zielperson und die Person, deren personenbezogene Daten gemeldet worden sind,

12. des § 163f die Zielperson sowie die erheblich mitbetroffenen Personen

zu benachrichtigen. Dabei ist auf die Möglichkeit nachträglichen Rechtsschutzes nach Absatz 9 und die dafür vorgesehene Frist hinzuweisen. Die Benachrichtigung unterbleibt, wenn ihr überwiegende schutzwürdige Belange einer betroffenen Person entgegenstehen. Zudem kann die Benachrichtigung einer in Satz 1 Nr. 2, 3, und 6 bezeichneten Person, gegen die sich die Maßnahme nicht gerichtet hat, unterbleiben, wenn diese von der Maßnahme nur unerheblich betroffen wurde und anzunehmen ist, dass sie kein Interesse an einer Benachrichtigung hat. Nachforschungen zur Feststellung der Identität einer in Satz 1 bezeichneten Person sind nur vorzunehmen, wenn dies unter Berücksichtigung der Eingriffsintensität der Maßnahme gegenüber dieser Person, des Aufwands für die Feststellung ihrer Identität sowie der daraus für diese oder andere Personen folgenden Beeinträchtigungen geboten ist.

(5) Die Benachrichtigung erfolgt, sobald dies ohne Gefährdung des Untersuchungszwecks, des Lebens, der körperlichen Unversehrtheit und der persönlichen Freiheit einer Person und von bedeutenden Vermögenswerten, im Fall des § 110a auch der Möglichkeit der weiteren Verwendung des Verdeckten Ermittlers möglich ist. Wird die Benachrichtigung nach Satz 1 zurückgestellt, sind die Gründe aktenkundig zu machen.

(6) Erfolgt die nach Absatz 5 zurückgestellte Benachrichtigung nicht binnen zwölf Monaten nach Beendigung der Maßnahme, bedarf die weitere Zurückstellung der gerichtlichen Zustimmung. Das Gericht bestimmt die Dauer der weiteren Zurückstellung; Verlängerungen der Zurückstellungsdauer sind zulässig. Sind mehrere Maßnahmen in einem engen zeitlichen Zusammenhang durchgeführt worden, so beginnt die in Satz 1 genannte Frist mit der Beendigung der letzten Maßnahme. Im Fall des § 100c beträgt die in Satz 1 genannte Frist sechs Monate, und die Dauer etwaiger Zurückstellungen nach Satz 2 ist auf jeweils höchstens sechs Monate zu bestimmen.

(7) Ist die Benachrichtigung für insgesamt fünf Jahre zurückgestellt worden und ergibt sich, dass die Voraussetzungen für eine Benachrichtigung mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft nicht eintreten werden, kann mit Zustimmung des Gerichts von einer Benachrichtigung endgültig abgesehen werden.

(8) Gerichtliche Entscheidungen nach den Absätzen 6 und 7 trifft das für die Anordnung der Maßnahme zuständige Gericht.

(9) Die in Absatz 4 Satz 1 genannten Personen können auch nach Beendigung der Maßnahme bis zu zwei Wochen nach ihrer Benachrichtigung die Überprüfung der Rechtmäßigkeit der Maßnahme sowie der Art und Weise ihres Vollzugs beantragen. Über den Antrag entscheidet das für die Anordnung der Maßnahme zuständige Gericht. Gegen die Entscheidung ist die sofortige Beschwerde statthaft. Ist die öffentliche Klage erhoben und der Angeklagte benachrichtigt worden, entscheidet über den Antrag das mit der Sache befasste Gericht in der das Verfahren abschließenden Entscheidung..

(10) Sind die durch die Maßnahme erlangten personenbezogenen Daten zur Strafverfolgung und für eine etwaige gerichtliche Überprüfung der Maßnahme nicht mehr erforderlich, so sind sie unverzüglich zu löschen. Die Löschung ist aktenkundig zu machen. Soweit die Löschung lediglich für eine etwaige gerichtliche Überprüfung der Maßnahme zurückgestellt ist, dürfen die Daten ohne Einwilligung der Betroffenen nur zu diesem Zweck verwendet werden; sie sind entsprechend zu sperren.“

12. Dem § 110 wird folgender Absatz 3 angefügt:

„(3) Die Durchsicht elektronischer Speichermedien darf auf räumlich getrennte Speichermedien, auf die der Betroffene den Zugriff zu gewähren berechtigt ist, erstreckt werden. Daten, die für die Untersuchung von Bedeutung sein können, dürfen gespeichert werden, wenn bis zur Sicherstellung der Datenträger ihr Verlust zu besorgen ist; sie sind zu löschen, sobald sie für die Strafverfolgung nicht mehr erforderlich sind."

13. Die §§ 110d und 110e werden aufgehoben.

14. § 161 wird wie folgt geändert:

a) Nach Absatz 1 wird folgender Absatz 2 eingefügt:

„(2) Ist eine Maßnahme nach diesem Gesetz nur bei Verdacht bestimmter Straftaten zulässig, so dürfen die auf Grund einer entsprechenden Maßnahme nach anderen Gesetzen erlangten personenbezogenen Daten ohne Einwilligung der von der Maßnahme betroffenen Personen zu Beweiszwecken im Strafverfahren nur zur Aufklärung solcher Straftaten verwendet werden, zu deren Aufklärung eine solche Maßnahme nach diesem Gesetz hätte angeordnet werden dürfen. § 100d Abs. 5 Nr. 3 bleibt unberührt."

b) Der bisherige Absatz 2 wird Absatz 3 und das Wort „Informationen" wird durch das Wort „Daten" ersetzt.

15. § 162 wird wie folgt gefasst:

„§ 162

(1) Erachtet die Staatsanwaltschaft die Vornahme einer gerichtlichen Untersuchungshandlung für erforderlich, so stellt sie ihre Anträge bei dem Amtsgericht, in dessen Bezirk sie oder ihre den Antrag stellende Zweigstelle ihren Sitz hat. Für gerichtliche Vernehmungen und Augenscheinnahmen ist das Amtsgericht zuständig, in dessen Bezirk diese Untersuchungshandlungen vorzunehmen sind, wenn die Staatsanwaltschaft dies zur Beschleunigung des Verfahrens oder zur Vermeidung von Belastungen Betroffener dort beantragt.

(2) Das Gericht hat zu prüfen, ob die beantragte Handlung nach den Umständen des Falles gesetzlich zulässig ist.“

16. § 163d wird wie folgt geändert:

a) In Absatz 1 Satz 1 Nr. 2 werden die Wörter „Satz 1 Nr. 3 und 4“ durch die Angabe „Abs. 2 Nr. 6 bis 8 und 10“ ersetzt.

b) Absatz 4 Satz 4 und 5 und Absatz 5 werden aufgehoben.

17. § 163e wird wie folgt geändert:

a) In Absatz 3 wird das Wort „Informationen“ durch das Wort „Daten“ ersetzt.

b) Absatz 4 wird wie folgt geändert:

aa) In Satz 1 werden die Wörter „den Richter“ durch die Wörter „das Gericht“ ersetzt.

bb) In Satz 3 wird das Wort „richterliche“ durch das Wort „gerichtliche“ ersetzt.

cc) In Satz 4 wird das Wort „Richter“ durch das Wort „Gericht“ ersetzt.

dd) Satz 6 wird wie folgt gefasst:

„Eine Verlängerung um jeweils nicht mehr als drei Monate ist zulässig, soweit die Voraussetzungen der Anordnung fortbestehen.“

18. § 163f wird wie folgt geändert:

a) Absatz 3 wird wie folgt gefasst:

„(3) Die Maßnahme darf nur durch das Gericht, bei Gefahr im Verzug auch durch die Staatsanwaltschaft und ihre Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) angeordnet werden. Die Anordnung der Staatsanwaltschaft oder ihrer Ermittlungspersonen tritt außer Kraft, wenn sie nicht binnen drei Werktagen von dem Gericht bestätigt wird. § 100b Abs. 1 Satz 3 Halbsatz 2, Satz 4 und 5, Abs. 2 Satz 1 gilt entsprechend.

b) Absatz 4 wird aufgehoben.

19. § 304 wird wie folgt geändert:

a) Absatz 1 Satz 2 Nr. 1 wird wie folgt gefasst:

„1. die Verhaftung, einstweilige Unterbringung, Unterbringung zur Beobachtung, Beschlagnahme, Durchsuchung oder die in § 101 Abs. 1 bezeichneten Maßnahmen betreffen,“.

b) Absatz 5 wird wie folgt gefasst:

„(5) Gegen Verfügungen des Ermittlungsrichters des Bundesgerichtshofes und des Oberlandesgerichts (§ 169 Abs. 1) ist die Beschwerde nur zulässig, wenn sie die Verhaftung, einstweilige Unterbringung, Beschlagnahme, Durchsuchung oder die in § 101 Abs. 1 bezeichneten Maßnahmen betreffen.“

20. § 477 wird wie folgt geändert:

a) Absatz 2 wird wie folgt gefasst:

„(2) Auskünfte aus Akten und Akteneinsicht sind zu versagen, wenn der Übermittlung Zwecke des Strafverfahrens oder besondere bundesgesetzliche oder entsprechende landesgesetzliche Verwendungsregelungen entgegenstehen. Ist eine Maßnahme nach diesem Gesetz nur bei Verdacht bestimmter Straftaten zulässig, so dürfen die auf Grund einer solchen Maßnahme erlangten personenbezogenen Daten ohne Einwilligung der von der Maßnahme betroffenen Personen zu Beweiszwecken in anderen Strafverfahren nur zur Aufklärung solcher Straftaten verwendet werden, zu deren Aufklärung eine solche Maßnahme nach diesem

Gesetz hätte angeordnet werden dürfen. Darüber hinaus dürfen personenbezogene Daten, die durch eine Maßnahme der in Satz 2 bezeichneten Art erlangt worden sind, ohne Einwilligung der von der Maßnahme betroffenen Personen nur verwendet werden

1. zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit,

2. für die Zwecke, für die eine Übermittlung nach § 18 des Bundesverfassungsschutzgesetzes zulässig ist, sowie

3. nach Maßgabe des § 476.

§ 100d Abs. 5 bleibt unberührt."

b) In Absatz 5 Satz 1 wird das Wort „Informationen" durch das Wort „Daten" ersetzt.

Artikel 2
Änderung des Telekommunikationsgesetzes

Das Telekommunikationsgesetzes in der Fassung der Bekanntmachung vom 22. Juni 2004 (BGBl. I S. 1190), zuletzt geändert durch …, wird wie folgt geändert:

1. § 97 wird wie folgt geändert:

a) § 97 Abs. 3 Satz 2 bis 4 wird durch folgende Sätze ersetzt:

„Diese Daten dürfen bis zu sechs Monate nach Versendung der Rechnung gespeichert werden. Für die Abrechnung nicht erforderliche Daten sind unverzüglich zu löschen, soweit sie nicht nach § 113a zu speichern sind. Hat der Teilnehmer gegen die Höhe der in Rechnung gestellten Verbindungsentgelte vor Ablauf der Frist nach Satz 2 Einwendungen erhoben, dürfen die Daten gespeichert werden, bis die Einwendungen abschließend geklärt sind."

b) Absatz 4 wird aufgehoben.

c) Die Absätze 5 und 6 werden zu Absätzen 4 und 5.

2. § 99 wird wie folgt geändert:

a) Absatz 1 wird wie folgt gefasst:

„(1) Dem Teilnehmer sind die gespeicherten Daten derjenigen Verbindungen, für die er entgeltpflichtig ist, nur dann mitzuteilen, wenn er vor dem maßgeblichen Abrechnungszeitraum in Textform einen Einzelverbindungsnachweis verlangt hat; auf Wunsch dürfen ihm auch die Daten pauschal abgegoltener Verbindungen mitgeteilt werden. Dabei entscheidet der Teilnehmer, ob ihm die von ihm gewählten Rufnummern ungekürzt oder unter Kürzung um die letzten drei Ziffern mitgeteilt werden. Bei Anschlüssen im Haushalt ist die Mitteilung nur zulässig, wenn der Teilnehmer in Textform erklärt hat, dass er alle zum Haushalt gehörenden Mitbenutzer des Anschlusses darüber informiert hat und künftige Mitbenutzer unverzüglich darüber informieren wird, dass ihm die Verkehrsdaten zur Erteilung des Nachweises bekannt gegeben werden. Bei Anschlüssen in Betrieben und Behörden ist die Mitteilung nur zulässig, wenn der Teilnehmer in Textform erklärt hat, dass die Mitarbeiter informiert worden sind und künftige Mitarbeiter unverzüglich informiert werden und dass der Betriebsrat oder die Personalvertretung entsprechend den gesetzlichen Vorschriften beteiligt worden ist oder eine solche Beteiligung nicht erforderlich ist. Soweit die öffentlich-rechtlichen Religionsgesellschaften für ihren Bereich eigene Mitarbeitervertreterregelungen erlassen haben, findet Satz 4 mit der Maßgabe Anwendung, dass an die Stelle des Betriebsrates oder der Personalvertretung die jeweilige Mitarbeitervertretung tritt. Dem Teilnehmer dürfen darüber hinaus die gespeicherten Daten mitgeteilt werden, wenn er Einwendungen gegen die Höhe der Verbindungsentgelte erhoben hat. Soweit ein Teilnehmer zur vollständigen oder teilweisen Übernahme der Entgelte für Verbindungen verpflichtet ist, die bei seinem Anschluss ankommen, dürfen ihm in dem für ihn bestimmten Einzelverbindungsnachweis die Nummern der Anschlüsse, von denen die Anrufe ausgehen, nur unter Kürzung um die letzten drei Ziffern mitgeteilt werden. Die Sätze 2 und 7 gelten nicht für Diensteanbieter, die als Anbieter für geschlossene Benutzergruppen ihre Dienste nur ihren Teilnehmern anbieten.“

b) In Absatz 3 Satz 2 wird die Angabe „Satz 2 oder 3“ durch die Angabe „Satz 3 oder Satz 4“ ersetzt.

3. § 110 wird wie folgt geändert:

a) Die Überschrift wird wie folgt gefasst:

„§ 110 Umsetzung von Überwachungsmaßnahmen, Erteilung von Auskünften“

b) Absatz 2 Nr. 1 Buchstabe a wird wie folgt gefasst:

„a) über die grundlegenden technischen Anforderungen und die organisatorischen Eckpunkte für die Umsetzung von Überwachungsmaßnahmen und die Erteilung von Auskünften einschließlich der Umsetzung von Überwachungsmaßnahmen und der Erteilung von Auskünften durch einen von dem Verpflichteten beauftragten Erfüllungsgehilfen,“

c) Absatz 8 wird aufgehoben.

4. § 111 wird wie folgt geändert:

a) Absatz 1 wird wie folgt gefasst:

„(1) Wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt und dabei Rufnummern oder andere Anschlusskennungen vergibt oder Telekommunikationsanschlüsse für von anderen vergebene Rufnummern oder andere Anschlusskennungen bereitstellt, hat für die Auskunftsverfahren nach den §§ 112 und 113

1. die Rufnummern und anderen Anschlusskennungen,

2. den Namen und die Anschrift des Anschlussinhabers,

3. bei natürlichen Personen deren Geburtsdatum,

4. bei Festnetzanschlüssen auch die Anschrift des Anschlusses,

5. in Fällen, in denen neben einem Mobilfunkanschluss auch ein Mobilfunkendgerät überlassen wird, die Gerätenummer dieses Gerätes sowie

6. das Datum des Vertragsbeginns

vor der Freischaltung zu erheben und unverzüglich zu speichern, auch soweit diese Daten für betriebliche Zwecke nicht erforderlich sind; das Datum des Vertragsendes ist bei Bekanntwerden ebenfalls zu speichern. Satz 1 gilt auch, soweit die Daten nicht in Teilnehmerverzeichnisse (§ 104) eingetragen werden. Die Verpflichtung zur unverzüglichen Speicherung nach Satz 1 gilt hinsichtlich der Daten nach Satz 1 Nr. 1 und 2 entsprechend für denjenigen, der geschäftsmäßig einen öffentlich zugänglichen Dienst der elektronischen Post erbringt und dabei Daten nach Satz 1 Nr. 1 und 2 erhebt, wobei an die Stelle der Daten nach Satz 1 Nr. 1 die Kennungen der elektronischen Postfächer und an die Stelle des Anschlussinhabers nach Satz 1 Nr. 2 der Inhaber des elektronischen Postfachs tritt. Wird dem Verpflichteten nach Satz 1 oder Satz 3 eine Änderung bekannt, hat er die Daten unverzüglich zu berichtigen; in diesem Zusammenhang hat der nach Satz 1 Verpflichtete bisher noch nicht erhobene Daten zu erheben und zu speichern, sofern ihm eine Erhebung der Daten ohne besonderen Aufwand möglich ist. Für das Auskunftsverfahren nach § 113 ist die Form der Datenspeicherung freigestellt.“

b) In Absatz 2 Satz 1 werden die Wörter „Absatz 1 Satz 1 eines Vertriebspartners“ durch die Wörter „Absatz 1 Satz 1 oder Satz 3 eines Vertriebspartners“ und die Wörter „Absatz 1 Satz 1 zu erheben“ durch die Wörter „Absatz 1 Satz 1 und 3 unter den dort genannten Voraussetzungen zu erheben“ ersetzt.

c) In Absatz 3 werden die Wörter „Absatz 1 Satz 1“ durch die Wörter „Absatz 1 Satz 1 oder Satz 3“ und die Wörter „des Absatzes 1 Satz 3“ durch die Wörter „des Absatzes 1 Satz 4“ ersetzt.

d) Folgende Absätze 4 und 5 werden angefügt:

„(4) Die Daten sind mit Ablauf des auf die Beendigung des Vertragsverhältnisses folgenden Kalenderjahres zu löschen.

(5) Eine Entschädigung für die Datenerhebung und -speicherung wird nicht gewährt.“

5. § 112 wird wie folgt geändert:

a) Absatz 1 wird wie folgt geändert:

aa) In Satz 1 werden die Wörter „Satz 1 und 3“ durch die Wörter „Satz 1, 3 und 4“ ersetzt.

bb) Satz 2 wird wie folgt gefasst:

„Für die Berichtigung und Löschung der in den Kundendateien gespeicherten Daten gilt § 111 Abs. 1 Satz 4 und Abs. 4 entsprechend.“

b) Absatz 3 Satz 1 Nr. 3 wird wie folgt gefasst:

„3. für Abrufe mit unvollständigen Abfragedaten und für die Suche mittels einer Ähnlichenfunktion

a) die Mindestanforderungen an den Umfang der einzugebenden Daten zur möglichst genauen Bestimmung der gesuchten Person,

b) die Zeichen, die in der Abfrage verwendet werden dürfen,

c) Anforderungen an den Einsatz sprachwissenschaftlicher Verfahren, die gewährleisten, dass unterschiedliche Schreibweisen eines Personen-, Straßen- oder Ortsnamens sowie Abweichungen, die sich aus der Vertauschung, Auslassung oder Hinzufügung von Namensbestandteilen ergeben, in die Suche und das Suchergebnis einbezogen werden,

d) die zulässige Menge der an die Bundesnetzagentur zu übermittelnden Antwortdatensätze.“

c) Absatz 4 Satz 4 wird wie folgt gefasst:

„Die Regulierungsbehörde protokolliert für Zwecke der Datenschutzkontrolle durch die jeweils zuständige Stelle bei jedem Abruf den Zeitpunkt, die bei der Durchführung des Abrufs verwendeten Daten, die abgerufenen Daten, ein die abrufende Person eindeutig bezeichnendes Datum sowie die ersuchende Stelle, deren Aktenzeichen und ein die ersuchende Person eindeutig bezeichnendes Datum."

6. Nach § 113 werden folgende §§ 113a und 113b eingefügt:

„§ 113a
Speicherungspflichten für Daten

(1) Wer öffentlich zugängliche Telekommunikationsdienste für Endnutzer erbringt, ist verpflichtet, von ihm bei der Nutzung seines Dienstes erzeugte oder verarbeitete Verkehrsdaten nach Maßgabe der Absätze 2 bis 5 sechs Monate im Inland oder in einem anderen Mitgliedstaat der Europäischen Union zu speichern. Wer öffentlich zugängliche Telekommunikationsdienste für Endnutzer erbringt, ohne selbst Verkehrsdaten zu erzeugen oder zu verarbeiten, hat sicherzustellen, dass die Daten gemäß Satz 1 gespeichert werden, und der Bundesnetzagentur auf deren Verlangen mitzuteilen, wer diese Daten speichert.

(2) Die Anbieter von öffentlich zugänglichen Telefondiensten speichern:

1. die Rufnummer oder andere Kennung des anrufenden und des angerufenen Anschlusses sowie im Falle von Um- oder Weiterschaltungen jedes weiteren beteiligten Anschlusses,

2. den Beginn und das Ende der Verbindung nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone,

3. in Fällen, in denen im Rahmen des Telefondienstes unterschiedliche Dienste genutzt werden können, Angaben zu dem genutzten Dienst,

4. im Fall mobiler Telefondienste ferner:

a) die internationale Kennung für mobile Teilnehmer für den anrufenden und den angerufenen Anschluss,

b) die internationale Kennung des anrufenden und des angerufenen Endgerätes,

c) die Bezeichnung der durch den anrufenden und den angerufenen Anschluss bei Beginn der Verbindung genutzten Funkzellen,

d) im Falle im Voraus bezahlter anonymer Dienste auch die erste Aktivierung des Dienstes nach Datum, Uhrzeit und Bezeichnung der Funkzelle,

5. im Falle von Internet-Telefondiensten auch die Internetprotokoll-Adresse des anrufenden und des angerufenen Anschlusses.

Satz 1 gilt entsprechend bei der Übermittlung einer Kurz-, Multimedia- oder ähnlichen Nachricht; hierbei sind anstelle der Angaben nach Satz 1 Nr. 2 die Zeitpunkte der Versendung und des Empfangs der Nachricht zu speichern.

(3) Die Anbieter von Diensten der elektronischen Post speichern:

1. bei Versendung einer Nachricht die Kennung des elektronischen Postfachs und die Internetprotokoll-Adresse des Absenders sowie die Kennung des elektronischen Postfachs jedes Empfängers der Nachricht,

2. bei Eingang einer Nachricht in einem elektronischen Postfach die Kennung des elektronischen Postfachs des Absenders und des Empfängers der Nachricht sowie die Internetprotokoll-Adresse der absendenden Telekommunikationsanlage,

3. bei Zugriff auf das elektronische Postfach dessen Kennung und die Internetprotokoll-Adresse des Abrufenden,

4. die Zeitpunkte der in den Nummern 1 bis 3 genannten Nutzungen des Dienstes nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone.

(4) Die Anbieter von Internetzugangsdiensten speichern:

1. die dem Teilnehmer für eine Internetnutzung zugewiesene Internetprotokoll-Adresse,

2. eine eindeutige Kennung des Anschlusses, über den die Internetnutzung erfolgt,

3. den Beginn und das Ende der Internetnutzung unter der zugewiesenen Internetprotokoll-Adresse nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone.

(5) Soweit Anbieter von Telefondiensten die in dieser Vorschrift genannten Verkehrsdaten für die in § 96 Abs. 2 genannten Zwecke auch dann speichern oder protokollieren, wenn der Anruf unbeantwortet bleibt oder wegen eines Eingriffs des Netzwerkmanagements erfolglos ist, sind die Verkehrsdaten auch nach Maßgabe dieser Vorschrift zu speichern.

(6) Wer Telekommunikationsdienste erbringt und hierbei die nach Maßgabe dieser Vorschrift zu speichernden Angaben verändert, ist zur Speicherung der ursprünglichen und der neuen Angabe sowie des Zeitpunktes der Umschreibung dieser Angaben nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone verpflichtet.

(7) Wer ein Mobilfunknetz für die Öffentlichkeit betreibt, ist verpflichtet, zu den nach Maßgabe dieser Vorschrift gespeicherten Bezeichnungen der Funkzellen auch Daten vorzuhalten, aus denen sich die geografischen Lagen der die jeweilige Funkzelle versorgenden Funkantennen sowie deren Hauptstrahlrichtungen ergeben.

(8) Der Inhalt der Kommunikation und Daten über aufgerufene Internetseiten dürfen auf Grund dieser Vorschrift nicht gespeichert werden.

(9) Die Speicherung der Daten nach den Absätzen 1 bis 7 hat so zu erfolgen, dass Auskunftsersuchen der berechtigten Stellen unverzüglich beantwortet werden können.

(10) Der nach dieser Vorschrift Verpflichtete hat betreffend die Qualität und den Schutz der gespeicherten Verkehrsdaten die im Bereich der Telekommunikation erforderliche Sorgfalt zu beachten. Er hat durch technische und organisatorische Maßnahmen sicherzustellen, dass der Zugang zu den gespeicherten Daten ausschließlich hierzu besonders ermächtigten Personen möglich ist.

(11) Der nach dieser Vorschrift Verpflichtete hat die allein auf Grund dieser Vorschrift gespeicherten Daten innerhalb eines Monats nach Ablauf der in Absatz 1 genannten Frist zu löschen oder die Löschung sicherzustellen.

§ 113b
Verwendung der nach § 113a gespeicherten Daten

Der nach § 113a Verpflichtete darf die allein auf Grund der Speicherungsverpflichtung nach § 113a gespeicherten Daten

1. zur Verfolgung von Straftaten,

2. zur Abwehr von erheblichen Gefahren für die öffentliche Sicherheit oder

3. zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes und des Militärischen Abschirmdienstes

an die zuständigen Stellen auf deren Verlangen übermitteln, soweit dies in den jeweiligen gesetzlichen Bestimmungen unter Bezugnahme auf § 113a vorgesehen und die Übermittlung im Einzelfall angeordnet ist; für andere Zwecke darf er die Daten nicht verwenden. § 113 Abs. 1 Satz 4 gilt entsprechend.“

7. § 115 Abs. 2 wird wie folgt geändert:

a) Satz 1 wird wie folgt geändert:

aa) In Nummer 1 wird die Angabe „5 oder 6“ durch die Angabe „5 oder Abs. 6, § 113a“ ersetzt.

bb) In Nummer 3 werden die Wörter „§ 111 Abs. 1 Satz 1 bis 4 und Abs. 2“ durch die Angabe „§ 111 Abs. 1, 2 und 4“ ersetzt.

b) In Satz 2 werden die Wörter „§ 111 Abs. 1 Satz 1 bis 4 und Abs. 2“ durch die Angabe „§ 111 Abs. 1, 2 oder Abs. 4“ ersetzt.

8. § 149 wird wie folgt geändert:

a) Absatz 1 wird wie folgt geändert:

aa) Nummer 29 wird wie folgt gefasst:

„29. entgegen § 111 Abs. 1 Satz 1, auch in Verbindung mit Satz 2 oder Satz 3, oder § 111 Abs. 1 Satz 4 dort genannte Daten nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erhebt, nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig speichert oder nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig berichtigt,“.

bb) In Nummer 30 werden die Wörter „oder nicht oder nicht rechtzeitig übermittelt,“ durch die Wörter „oder nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig übermittelt,“ ersetzt.

cc) Nach Nummer 30 wird folgende Nummer 30a eingefügt:

„30a. entgegen § 111 Abs. 4 Daten nicht oder nicht rechtzeitig löscht,“.

dd) In Nummer 34 wird das Wort „oder“ durch ein Komma ersetzt.

ee) In Nummer 35 werden nach der Angabe „Satz 4“ ein Komma und die Wörter „auch in Verbindung mit § 113b Satz 2,“ eingefügt und am Ende der Punkt durch ein Komma ersetzt.

ff) Nach Nummer 35 werden folgende Nummern 36 bis 39 angefügt:

„36. entgegen § 113a Abs. 1 Satz 1 oder Abs. 6 Daten nicht, nicht richtig oder nicht für die vorgeschriebene Dauer speichert,

37. entgegen § 113a Abs. 1 Satz 2 nicht sicherstellt, dass die dort genannten Daten gespeichert werden, oder nicht mitteilt, wer diese Daten speichert,

38. entgegen § 113a Abs. 10 Satz 2 nicht sicherstellt, dass der Zugang zu den gespeicherten Daten ausschließlich dazu besonders ermächtigten Personen möglich ist, oder

39. entgegen § 113a Abs. 11 Daten nicht oder nicht rechtzeitig löscht oder nicht sicherstellt, dass die Daten rechtzeitig gelöscht werden.“.

b) In Absatz 2 Satz 1 werden die Angabe „27 und 31“ durch die Angabe „27, 31, 36 und 37“ und die Angabe „29 und 34“ durch die Angabe „29, 30a, 34, 38 und 39“ ersetzt.

9. In § 150 wird nach Absatz 12a folgender Absatz 12b eingefügt:

„(12b) Auf Verstöße gegen die Pflicht zur Speicherung nach § 113a Abs. 1 Satz 1 oder Abs. 6 oder gegen die Pflicht zur Sicherstellung der Speicherung nach § 113a Abs. 1 Satz 2 ist § 149 erstmalig ab dem 1. Januar 2009 anzuwenden.

Artikel 3
Änderung der Abgabenordnung

Die Abgabenordnung in der Fassung der Bekanntmachung vom 1. Oktober 2002 (BGBl. I S. 3866, 2003 I S. 61), zuletzt geändert durch ..., wird wie folgt geändert:

1. In der Inhaltsübersicht wird die Angabe zu § 370a wie folgt gefasst:

„§ 370a (weggefallen)“

2. § 370 Abs. 3 Satz 2 wird wie folgt geändert:

a) Nummer 1 wird wie folgt gefasst:

„1. in großem Ausmaß Steuern verkürzt oder nicht gerechtfertigte Steuervorteile erlangt,“.

b) In Nummer 3 wird das Wort „oder“ gestrichen.

c) In Nummer 4 wird der den Satz abschließende Punkt durch ein Komma ersetzt und das Wort „oder“ angefügt.

d) Folgende Nummer 5 wird angefügt:

„5. als Mitglied einer Bande, die sich zur fortgesetzten Begehung von Taten nach Absatz 1 verbunden hat, Umsatz- oder Verbrauchsteuern verkürzt oder nicht gerechtfertigte Umsatz- oder Verbrauchssteuervorteile erlangt.“

3. § 370a wird aufgehoben.

4. § 373 wird wie folgt geändert:

a) Absatz 1 wird wie folgt gefasst:

„(1) Wer gewerbsmäßig Einfuhr- oder Ausfuhrabgaben hinterzieht oder gewerbsmäßig durch Zuwiderhandlungen gegen Monopolvorschriften Bannbruch begeht, wird mit Freiheitsstrafe von sechs Monaten bis zu zehn Jahren bestraft. In minder schweren Fällen ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe.“

b) Absatz 2 Nr. 3 wird wie folgt gefasst:

„3. als Mitglied einer Bande, die sich zur fortgesetzten Begehung der Hinterziehung von Einfuhr- oder Ausfuhrabgaben oder des Bannbruchs verbunden hat, eine solche Tat begeht.“

c) Folgende Absätze 3 und 4 werden angefügt:

„(3) Der Versuch ist strafbar.

(4) § 370 Abs. 6 Satz 1 und Abs. 7 gilt entsprechend.“

5. § 374 wird wie folgt geändert:

a) In Absatz 1 wird die Angabe „nach § 370 Abs. 1 und 2, wenn er gewerbsmäßig handelt, nach § 373“ durch die Wörter „mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe“ ersetzt.

b) Nach Absatz 1 werden folgende Absätze 2 und 3 eingefügt:

„(2) Handelt der Täter gewerbsmäßig oder als Mitglied einer Bande, die sich zur fortgesetzten Begehung von Straftaten nach Absatz 1 verbunden hat, so ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren. In minder schweren Fällen ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe.

(3) Der Versuch ist strafbar.“

c) Der bisherige Absatz 2 wird Absatz 4 und wie folgt gefasst:

„(4) § 370 Abs. 6 Satz 1 und Abs. 7 gilt entsprechend.“

Artikel 4
Änderung des Strafgesetzbuchs

§ 261 Abs. 1 des Strafgesetzbuches in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl I S. 3322), das zuletzt durch ... geändert worden ist, wird wie folgt geändert:

1. Satz 2 wird wie folgt geändert:

a) Nummer 3 wird wie folgt geändert:

aa) Die Wörter „, wenn er gewerbsmäßig handelt,“ werden gestrichen.

bb) Nach der Angabe „§ 374“ wird die Angabe „Abs. 2“ eingefügt.

b) In Nummer 4 Buchstabe b wird das Wort „und“ durch ein Komma ersetzt und nach dem Wort „Asylverfahrensgesetzes“ die Wörter „und nach § 370 der Abgabenordnung“ eingefügt.

2. In Satz 3 wird die Angabe „§ 370a“ durch die Angabe „§ 370“ ersetzt.

Artikel 5
Änderung des Artikel 10-Gesetzes

In § 17 Abs. 1 des Artikel 10-Gesetzes vom 26. Juni 2001 (BGBl. I S. 1254, 2298), das zuletzt durch …geändert worden ist, wird das Wort „geschäftsmäßig“ gestrichen.

Artikel 6
Änderung des Vereinsgesetzes

In § 10 Abs. 2 Satz 4 des Vereinsgesetzes vom 5. August 1964 (BGBl. I S. 593), das zuletzt durch … geändert worden ist, wird die Angabe „§§ 99, 100 und 101“ durch die Wörter „§§ 99, 100 und 101 Abs. 3 bis 10“ ersetzt.

Artikel 7
Änderung des Bundeskriminalamtgesetzes

In § 16 Abs. 3 Satz 3 des Bundeskriminalamtsgesetzes vom 7. Juli 1997 (BGBl. I S. 1650), das zuletzt durch … geändert worden ist, wird die Angabe „§ 161 Abs. 2“ gestrichen.

Artikel 8
Änderung des Gerichtsverfassungsgesetzes

In § 120 Abs. 4 Satz 2 des Gerichtsverfassungsgesetzes in der Fassung der Bekanntmachung vom 9. Mai 1975 (BGBl. I S. 1077), das zuletzt durch …geändert worden ist, werden die Wörter „und § 100d Abs. 9 Satz 4“ gestrichen.

Artikel 9
Änderung des Einführungsgesetzes zur Strafprozessordnung

Nach § 11 des Einführungsgesetzes zur Strafprozessordnung vom 1. Februar 1877 (RGBl. S. 346), das zuletzt durch … geändert worden ist, wird folgender § 12 angefügt:

„§ 12
Übergangsregelungen zum
Gesetz zur Neuregelung der Telekommunikationsüberwachung
und anderer verdeckter Ermittlungsmaßnahmen
sowie zur Umsetzung der Richtlinie 2006/24/EG

(1) § 100b Abs. 5 und 6 sowie § 100g Abs. 4 der Strafprozessordnung sind erstmalig für das Berichtsjahr 2008 anzuwenden. Auf Berichte nach § 100e der Strafprozessordnung ist § 100b Abs. 5 der Strafprozessordnung bereits für das Berichtsjahr 2007 anzuwenden.

(2) § 110 Abs. 8 des Telekommunikationsgesetzes sowie § 1 Nr. 8, § 25 und die Anlage zu § 25 der Telekommunikations-Überwachungsverordnung sind letztmalig für das Berichtsjahr 2007 anzuwenden.“

Artikel 10
Änderung des IStGH-Gesetzes

§ 59 Abs. 1 des IStGH-Gesetzes vom 21. Juni 2002 (BGBl. I S. 2002, 2144), das zuletzt durch … geändert worden ist, wird wie folgt geändert:

1. In Nummer 2 wird die Angabe „§ 100a Abs. 1 Satz 1“ durch die Angabe „§ 100a Abs. 2“ ersetzt.

2. In Nummer 3 werden ersetzt:

   a) die Angabe „§ 101 Abs. 1“ durch die Angabe „§ 101 Abs. 4 bis 7“,

   b) die Wörter „Verwendung der erlangten Informationen“ durch die Wörter „Übermittlung der erlangten personenbezogenen Daten zu Beweiszwecken“,

c) die Angabe „§ 100b Abs. 5“ durch die Angabe „§ 477 Abs. 2 Satz 2“

d) das Wort „Vernichtung“ durch das Wort „Löschung“ und

e) die Angabe „§ 100b Abs. 6“ durch die Angabe „§ 101 Abs. 10“.

Artikel 11

Änderung des Wertpapierhandelsgesetzes

In § 16b Abs. 1 Satz 3 des Wertpapierhandelsgesetzes vom 9. September 1998 (BGBl. I S. 2708), das zuletzt durch … geändert worden ist, wird die Angabe „gemäß § 101“ durch die Wörter „entsprechend § 101 Abs. 4 und 5“ ersetzt.

Artikel 12

Änderung des Gesetzes über die Anwendung unmittelbaren Zwanges und die Ausübung besonderer Befugnisse durch Soldaten der Bundeswehr und verbündeter Streitkräfte sowie zivile Wachpersonen

In § 7 Abs. 2 Satz 2 des Gesetzes über die Anwendung unmittelbaren Zwanges und die Ausübung besonderer Befugnisse durch Soldaten der Bundeswehr und verbündeter Streitkräfte sowie zivile Wachpersonen vom 12. August 1965 (BGBl. I S. 796), das zuletzt durch … geändert worden ist, wird die Angabe „§§ 96, 97 und 110“ durch die Angabe „§§ 96, 97 und 110 Abs. 1 und 2“ ersetzt.

Artikel 13

Änderung der Telekommunikations-Überwachungsverordnung

Die Telekommunikations-Überwachungsverordnung in der Fassung der Bekanntmachung vom 3. November 2005 (BGBl. I S. 3136, 3149), zuletzt geändert durch …, wird wie folgt geändert:

1. § 1 wird wie folgt geändert:

a) In Nummer 8 wird der Punkt am Ende durch das Wort „und“ ersetzt.

b) Es wird folgende Nummer 9 angefügt:

„9. die Anforderungen an das Übermittlungsverfahren und das Datenformat für Auskunftsersuchen über Verkehrsdaten und der zugehörigen Ergebnisse.“

c) Nummer 8 wird aufgehoben und die bisherige Nummer 9 wird zu Nummer 8.

2. § 3 Abs. 2 wird wie folgt geändert:

a) In Satz 1 Nr. 5 wird die Angabe „1 000“ durch die Angabe „10 000“ ersetzt.

b) Nach Satz 2 wird folgender Satz eingefügt:

„Satz 1 Nr. 1 und 2 gilt nicht im Hinblick auf Vorkehrungen zur Erfüllung der Verpflichtung aus § 110 Abs. 1 Satz 1 Nr. 1a des Telekommunikationsgesetzes.“

3. In § 4 Abs. 2 Satz 3 werden die Wörter „Die §§ 21 und 22 sind“ durch die Angabe „§ 22 ist“ ersetzt.

4. § 7 Abs. 1 Satz 1 Nr. 7 wird wie folgt geändert:

a) Die Wörter „aus Mobilfunknetzen“ werden ersetzt durch die Wörter „, deren Nutzung nicht ortsgebunden ist,“.

b) Das Wort „Mobilfunkgerät“ wird durch das Wort „Endgerät“ und das Wort „Mobilfunkgerätes“ wird jeweils durch das Wort „Endgerätes“ ersetzt.

5. In § 11 Satz 1 wird nach der Angabe „§ 10 Satz 1 und 3,“ die Angabe „§ 12 Abs. 2 Satz 1,“ eingefügt.

6. § 12 Abs. 2 Satz 1 werden die Wörter „vorab per Telefax oder auf gesichertem elektronischen Weg“ durch die Wörter „auf gesichertem elektronischem Weg oder vorab per Telefax“ ersetzt.

7. In § 19 Abs. 3 Satz 2 Halbsatz 2 wird die Angabe „§ 21 oder“ gestrichen.

8. § 21 wird aufgehoben.

9. In der Überschrift von § 22 wird das Wort „Sonstige“ gestrichen.

10. § 25 und die Anlage zu § 25 werden aufgehoben.

11. In § 27 Abs. 8 Satz 1 werden die Wörter „§§ 15 und 21 Abs. 4 Nr. 1 entsprechend“ durch die Wörter „§ 15 entsprechend mit der von § 12 Abs. 1 Satz 1 bis 3 und Abs. 3 Satz 1 abweichenden Maßgabe, dass der Verpflichtete innerhalb seiner üblichen Geschäftszeiten jederzeit über das Vorliegen einer Anordnung und die Dringlichkeit ihrer Umsetzung benachrichtigt werden kann, er eine Anordnung entgegennehmen und Rückfragen zu einzelnen noch nicht abgeschlossenen Überwachungsmaßnahmen entgegennehmen kann“ ersetzt.

Artikel 14
Änderung des Gesetzes zur Änderung der Strafprozessordnung

Artikel 2 und Artikel 4 Satz 2 des Gesetzes zur Änderung der Strafprozessordnung vom 20. Dezember 2001 (BGBl. I S. 3879), zuletzt geändert durch …, werden aufgehoben.

Artikel 15
Zitiergebot

Durch die Artikel 1 und 2 dieses Gesetzes werden das Brief-, Post- und Fernmeldegeheimnis (Artikel 10 des Grundgesetzes) eingeschränkt.

Artikel 16
Inkrafttreten, Außerkrafttreten

(1) Dieses Gesetz tritt vorbehaltlich der Absätze 2 und 3 am 1. Januar 2008 in Kraft.

(2) Artikel 2 Nr. 3 Buchstabe c und Artikel 13 Nr. 1 Buchstabe c und Nr. 10 treten am 1. Januar 2009 in Kraft.

(3) Artikel 14 tritt am Tag nach der Verkündung in Kraft.

(4) § 12 des Einführungsgesetzes zur Strafprozessordnung tritt mit Ablauf des 31. Dezembers 2009 außer Kraft.

Begründung

A.
Allgemeines

I.

Der Entwurf verfolgt das Ziel, das Recht der verdeckten strafprozessualen Ermittlungsmaßnahmen zu harmonisieren und entsprechend den Vorgaben des Bundesverfassungsgerichts rechtsstaatlich auszugestalten. Hierzu sollen der Rechtsschutz der von solchen Maßnahmen Betroffenen gestärkt, bestehende Unsicherheiten und Lücken bei der Rechtsanwendung beseitigt und das Recht der verdeckten Ermittlungsmaßnahmen insgesamt transparenter und dadurch auch praktikabler gestaltet werden.

Der Gesetzgeber hat mit dem Gesetz zur Umsetzung des Urteils des Bundesverfassungsgerichts vom 3. März 2004 (akustische Wohnraumüberwachung) vom 24. Juni 2005 (BGBl. I S. 1841) die rechtsstaatliche Ausgestaltung der Wohnraumüberwachung im Lichte des Artikels 13 GG entsprechend den verfassungsrechtlichen Vorgaben ergänzt und erweitert. Die Vorgaben des Bundesverfassungsgerichts (BVerfGE 109, 279 ff.), die zur vorgenannten Neuregelung geführt hatten, sind – entgegen einer verbreiteten Auffassung im Schrifttum – nicht pauschal auf andere verdeckte Ermittlungsmaßnahmen zu übertragen (vgl. zum Verhältnis von Artikel 10 GG zu Artikel 13 GG BVerfG, 1 BvR 668/04 vom 27. Juli 2005, Absatz-Nr. 162 f., NJW 2005, 2603, 2611; zur a. A: Hirsch, in: Roggan [Hrsg.] Lauschen im Rechtsstaat. Zu den Konsequenzen des Urteils des Bundesverfassungsgerichts zum großen Lauschangriff, 2004, S. 87 ff.; Leutheusser-Schnarrenberger, DuD 2005, 323, 326 f.; dies., in: Roggan, a. a. O., S. 99 ff.; Bergemann, in: Roggan, a. a. O., S. 69 ff.; Baldus, in: Schaar [Hrsg.], Folgerungen aus dem Urteil des Bundesverfassungsgerichts zur akustischen Wohnraumüberwachung: Staatliche Eingriffsbefugnisse auf dem Prüfstand?, 2005, S. 9 ff.; Gusy, in: Schaar, a. a. O., S. 35 ff., 48 ff.; Kutscha, NJW 2005, 20, 22). Wegen der besonderen Bedeutung der Unverletzlichkeit der Wohnung (Artikel 13 Abs. 1 GG) und der durch diese Maßnahme in besonderer Weise begründeten Gefährdung für den unantastbaren Kernbereich privater Lebensgestaltung kommt der akustischen Wohnraumüberwachung innerhalb der verdeckten strafprozessualen Ermittlungsmaßnahmen eine Sonderstellung zu, die besondere einfachgesetzliche Regelungen mit grundrechtssichernder Funktion, insbesondere zum Schutz des Kernbereichs privater Lebensgestaltung, von nach den §§ 53, 53a StPO zeugnisverweigerungsberechtigten Personen und von durch die Maßnahme erlangten personenbezogenen Daten rechtfertigt (BVerfG, 1 BvR 668/04 vom 27. Juli 2005, Absatz-Nr. 162, NJW 2005, 2603, 2611). Dies gilt auch für die hohen materiellen Anordnungsvor-

aussetzungen der akustischen Wohnraumüberwachung und die diese absichernden Anordnungskompetenzen und Begründungspflichten.

Da die gesetzliche Beschränkung der Ermittlungstätigkeit die Wahrheitserforschung, die ein vorrangiges Ziel des Strafverfahrens darstellt, erheblich beeinträchtigen kann, bedarf mit Blick auf die Gewährleistung einer funktionstüchtigen Strafrechtspflege, ohne die Gerechtigkeit nicht durchgesetzt werden kann (BVerfGE 33, 367, 383; 107, 299, 316), jede solche Beschränkung der sorgfältigen Abwägung und besonderen Legitimation (vgl. BVerfGE 33, 367, 383; BVerfG, 1 BvR 77/96 vom 22. August 2000, NStZ 2001, 43 ff.). Der Gesetzgeber ist weder gehalten, noch steht es ihm frei, einzelnen Lebensbereichen den absoluten Vorrang vor wichtigen Gemeinschaftsgütern einzuräumen. Er hat bei dieser Abwägung die Erfordernisse einer rechtsstaatlichen Rechtspflege zu berücksichtigen, deren Aufgabe es ist, in den ihr gesetzten Grenzen Gerechtigkeit und Rechtsfrieden zu schaffen. Beides ist ohne Kenntnis der maßgeblichen Tatsachen nicht denkbar (vgl. dazu allgemein Neumann, ZStW 1989, 52 ff.; Kroepil, JZ 1998, 135 f.; Stock, in: FS für Mezger, S. 429, 433, 446 f.; Weigend, ZStW 2001, 271, 277, 279; Rieß, in: Löwe/Rosenberg, StPO, 25. Aufl., Einl. G, Rn. 43). Insoweit ist den unabweisbaren Bedürfnissen einer wirksamen Strafrechtspflege Rechnung zu tragen und die möglichst umfassende Wahrheitsermittlung ein wesentliches Ziel des Strafverfahrens. Die Verfolgung insbesondere schwerer Straftaten ist ein wichtiger Auftrag des rechtsstaatlichen Gemeinwesens. Dieser Auftrag kann durch Verfahrenvorschriften, die der Ermittlung der Wahrheit und damit einem gerechten Urteil entgegenstehen, empfindlich berührt sein. Betroffen ist dadurch auch der Anspruch des Beschuldigten auf ein faires Verfahren, weil dasjenige, was der Anklage entzogen ist, auch ihm entzogen ist. Allerdings darf die zur Wahrheitsermittlung notwendige Sachverhaltsaufklärung nicht „um jeden Preis“ erfolgen (BGHSt 14, 358, 365; 31, 304, 309). Vielmehr muss das öffentliche Interesse an der Verfolgung von Straftaten mit den schutzwürdigen Interessen der von Strafverfolgungsmaßnahmen Betroffenen bereits auf der Ebene der Rechtsetzung abgewogen werden.

II.

Einige verdeckte Ermittlungsmaßnahmen sind mit schwerwiegenden Eingriffen in die grundrechtlich verbürgten Rechte der Betroffenen verbunden. Allerdings kennzeichnet das Kriterium der Heimlichkeit auch Ermittlungsmaßnahmen mit geringer Eingriffsintensität, wie etwa die nach den §§ 161, 163 StPO zulässige kurzfristige Observation. Eine Missachtung seines Wertes als Mensch geht mit dem heimlichen Beobachten eines Menschen nicht zwingend einher (BVerfGE 109, 279, 313). Die verdeckten Maßnahmen erfolgen, ebenso wie offene

Maßnahmen, deren Untersuchungszweck nicht gefährdet werden soll, ohne vorherige Anhörung der Betroffenen (§ 33 StPO). Der Unterschied zu offenen Ermittlungsmaßnahmen besteht darin, dass der Betroffene einer verdeckten Maßnahme sich regelmäßig keiner solchen gegenüber sieht. Darüber hinaus haben verdeckte Ermittlungsmaßnahmen oftmals eine große „Streubreite“. So werden etwa bei Maßnahmen nach den §§ 100a, 100g StPO regelmäßig zahlreiche Personen in den Wirkungsbereich der Maßnahme einbezogen, ohne dafür einen Anlass gegeben zu haben (vgl. BVerfGE 90, 145, 172; 100, 313, 376, 380; 107, 299, 320 f.). Schließlich besteht bei einigen verdeckten Ermittlungsmaßnahmen die Gefahr, dass ohne Wissen der Betroffenen in deren Kernbereich privater Lebensgestaltung eingegriffen wird (vgl. BVerfGE 109, 279 ff.; BVerfG, 1 BvR 668/04 vom 27. Juli 2005, Absatz-Nr. 152 f., NJW 2005, 2603, 2610 f.).

Diesen Besonderheiten der verdeckten Ermittlungsmaßnahmen hat der Gesetzgeber bei der von ihm vorzunehmenden Abwägung zwischen Allgemein- und Individualinteressen Rechnung zu tragen.

Um eine vorbeugende Kontrolle solcher Maßnahmen durch eine unabhängige Instanz zu ermöglichen, stehen die mit Grundrechtseingriffen von einigem Gewicht einhergehenden verdeckten Ermittlungsmaßnahmen unter dem Vorbehalt gerichtlicher Anordnung. Da eine Anhörung der Betroffenen vor Anordnung und Durchführung verdeckter Ermittlungsmaßnahmen notwendig ausgeschlossen ist, ist es zur Gewährleistung rechtlichen Gehörs (Artikel 103 Abs. 1 GG) und eines effektiven Rechtsschutzes (Artikel 19 Abs. 4 GG) verfassungsrechtlich regelmäßig geboten, die Betroffenen bei grundrechtsrelevanten Maßnahmen nachträglich zu benachrichtigen und ihnen die Möglichkeit nachträglichen Rechtsschutzes zu eröffnen. Ferner kann der Gesetzgeber diesen Besonderheiten dadurch begegnen, dass er die Anordnung von verdeckten Ermittlungsmaßnahmen nur bei Verdacht bestimmter Straftaten und unter der Voraussetzung eines erhöhten Grades des Anfangsverdachts zulässt.

Aufgrund der zunehmenden technischen Möglichkeiten, auf verfügbare Daten zuzugreifen, wird durch verdeckte Ermittlungsmaßnahmen zudem oftmals eine Vielzahl von Daten erhoben. Da die Weitergabe und die weitere Verwendung solcher Daten (erneute) Eingriffe in das Recht auf informationelle Selbstbestimmung der Betroffenen darstellen und den vorangegangenen Eingriff vertiefen können, ist es Aufgabe des Gesetzgebers, einfachgesetzliche Vorkehrungen zu schaffen, um die Zweckbindung der Daten in angemessener Weise zu gewährleisten.

Soweit diese, die verdeckten Ermittlungsmaßnahmen allgemein kennzeichnenden Aspekte betroffen sind, ergeben sich aus der Entscheidung des Bundesverfassungsgerichts zur akustischen Wohnraumüberwachung trotz der Sonderstellung dieser Maßnahme innerhalb der verdeckten Ermittlungsmaßnahmen allgemeine Grundsätze, die unter Berücksichtigung der Besonderheiten der jeweiligen Maßnahme umzusetzen sind (vgl. BVerfGE 109, 279, 366 f., 374, 379 f.). Soweit hiervon Benachrichtigungspflichten (vgl. dazu BVerfGE 100, 313, 361 f., 364; 107, 299, 337 f.; BVerfG, 2 BvR 581/01 vom 12. April 2005, Absatz-Nr. 55, NJW 2005, 1338, 1340; 1 BvR 668/04 vom 1. Juli 2005, Absatz-Nr. 159, NJW 2005, 2603, 2611) und datenschutzrechtliche Regelungen (vgl. BVerfGE 69, 1, 49; 100, 313, 360, 364 f.) betroffen sind, entspricht diese Auffassung einer bereits gefestigten Rechtsprechung.

III.

Der Entwurf berücksichtigt die Erkenntnisse der zur Vorbereitung der Neuregelung des Rechts der verdeckten strafprozessualen Ermittlungsmaßnahmen in Auftrag gegebenen rechtswissenschaftlichen und rechtstatsächlichen Untersuchungen.

1.

Die Untersuchung von Albrecht, Dorsch und Krüpe zur „Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen“ (2003) analysiert auf der Grundlage einer Auswertung von 501 Strafverfahren aus dem Jahr 1998, in denen Telekommunikationsüberwachungsmaßnahmen durchgeführt wurden, sowie umfangreicher Expertenbefragungen eingehend die Praxis der Telekommunikationsüberwachung. Die Untersuchung belegt, dass es sich bei der Telekommunikationsüberwachung um ein wichtiges, erfolgreiches und letztlich unverzichtbares Mittel zur Aufklärung schwer ermittelbarer Kriminalität handelt (vgl. a. a. O., S. 355 ff.).

Die Untersuchung zeigt aber auch Probleme und Unzulänglichkeiten bei der Anwendung des Rechts der Telekommunikationsüberwachung auf, insbesondere soweit die in § 101 Abs. 1 Satz 1 StPO vorgesehene Benachrichtigungspflicht betroffen ist. So konnte den Akten nur für ein Drittel der überwachten Telekommunikationsanschlüsse eine Auseinandersetzung mit der Frage der Benachrichtigung entnommen werden (a. a. O., S. 276). Meinungsverschiedenheiten bestehen in der Praxis bei der Frage, welche Personen Beteiligte im Sinne des § 101 Abs. 1 Satz 1 StPO und damit zu benachrichtigen sind (a. a. O., S. 451). Diese Unzu-

länglichkeiten bei der Wahrnehmung der Benachrichtigungspflicht werden auch durch eine Studie der Universität Bielefeld belegt (Backes/Gusy, Wer kontrolliert die Telefonüberwachung?, 2003, S. 71 f.). Die Untersuchung von Albrecht, Dorsch und Krüpe belegt auch, dass das in der Praxis bestehende Defizit bei der Auseinandersetzung mit der Frage der Benachrichtigung nicht durch die Ausübung der Dienstaufsicht behoben wird. Vielmehr begründen die bestehenden Unsicherheiten, ob, wann und welche Personen zu benachrichtigen sind, einen gesetzgeberischen Handlungsbedarf, um der Praxis unter Berücksichtigung der verfassungsrechtlichen Vorgaben die notwendige Handreichung zu geben.

Der Entwurf erstreckt in Umsetzung der Rechtsprechung des Bundesverfassungsgerichts die Benachrichtigungspflichten daher nicht nur auf alle eingriffsintensiven verdeckten Ermittlungsmaßnahmen, sondern konkretisiert zugleich auch den Kreis der zu benachrichtigenden Personen. Damit wird der nachträgliche Rechtsschutz verbessert und das Bewusstsein der Praxis für die Benachrichtigungspflicht geschärft.

Durch die Untersuchung von Albrecht, Dorsch und Krüpe wurde ferner festgestellt, dass die tatsächliche Dauer von Telekommunikationsüberwachungsmaßnahmen sich in etwa drei Viertel aller Fälle über einen Zeitraum von maximal zwei Monaten erstreckte (a. a. O., S. 170 f.). Der Entwurf beschränkt daher die Anordnungsdauer der Telekommunikationsüberwachung – und der mit ihr vergleichbaren Überwachung des nichtöffentlich gesprochenen Wortes außerhalb von Wohnungen nach § 100f StPO-E – auf die Dauer von zwei Monaten; Verlängerungen der Anordnung sind ebenfalls für die Dauer von jeweils zwei Monaten zulässig.

Ausgehend von den Erkenntnissen der Untersuchung, die die Telekommunikationsüberwachung als ein wichtiges und unabdingbares Ermittlungsinstrument insbesondere im Bereich der opferlosen (Transaktions-)Kriminalität hervorhebt (a. a. O., S. 463), wird der Anlasstatenkatalog des § 100a StPO unter Berücksichtigung der Vorgaben des Bundesverfassungsgerichts (vgl. BVerfGE 107, 299, 322; 109, 279, 346; BVerfG, 1 BvR 668/04 vom 27. Juli 2005, Absatz-Nr. 154, NJW 2005, 2603, 2610 f.) einer umfassenden Bearbeitung unterzogen.

Die weitgehende Harmonisierung der formellen Anordnungsvoraussetzungen für verdeckte Maßnahmen sowie die neu gefasste Regelung in § 162 StPO-E über die Konzentration der örtlichen Zuständigkeit des Ermittlungsgerichts am Sitz der Staatsanwaltschaft dienen der von der Untersuchung nahe gelegten Stärkung der mit dem Richtervorbehalt bezweckten rechtsstaatlichen Kontrolle (a. a. O., S. 467).

Nicht gefolgt wird der Untersuchung hingegen, soweit dort als zusätzliche Kontrollmechanismen die Einbindung eines Rechtsanwalts als „Ombudsmann“ und die Einrichtung einer Kontrollkommission in Erwägung gezogen wird (a. a. O., S. 468 f.). Dies erscheint schon deshalb nicht geboten, weil die Staatsanwaltschaft die Interessen aller Beteiligten aus ihrer neutralen Stellung als Wächterin des Gesetzes, die dahin zu wirken hat, dass dem Gesetz genüge getan wird, zu berücksichtigen hat. Die Umsetzung beider Vorschläge erscheint darüber hinaus auch im Hinblick auf das Ziel einer Stärkung der unabhängigen Kontrolle durch das Ermittlungsgericht nicht geboten und wäre zudem mit hohem Kosten- und Personalaufwand verbunden. Es ist indessen eine der wichtigsten und vornehmsten – wie von den Landesjustizverwaltungen übermittelte Stellungnahmen aus der Praxis gezeigt haben, allerdings oftmals nicht oder zumindest nicht erfolgreich wahrgenommenen – Aufgaben der obersten Justizverwaltungen, dafür Sorge zu tragen, dass die zur Gewährleistung eines effektiven Rechtsschutzes notwendigen sächlichen und personellen Ressourcen bereitgestellt sind (BVerfGE 2, 176, 179; 100, 313, 401; 103, 142, 152; 105, 239, 248; 109, 279, 358; BVerfG, 2 BvR 1737/05 vom 29. November 2005, Absatz-Nr. 43).

Ebenfalls nicht gefolgt wird der Untersuchung, soweit dort besondere gesetzliche Regelungen für eine auch „proaktive“ Ausgestaltung der Telekommunikationsüberwachung etwa in Fällen der Transaktionskriminalität in Erwägung gezogen werden (a. a. O., S. 465 f.). Ein „begleitender“ Einsatz der Telekommunikationsüberwachung ist in diesen Fällen im Rahmen des Strafprozessrechts dadurch gewährleistet, dass auch Straftaten, durch die eine Anlasstat im Sinne des § 100a Abs. 2 StPO-E vorbereitet wird, als Anlasstaten in Betracht kommen (§ 100a Abs. 1 Nr. 1 StPO-E) und zudem einige Anlasstaten tatbestandlich so ausgestaltet sind, dass sie bereits im Vorfeld der eigentlichen Rechtsgutsverletzung eingreifen. Darüber hinaus ist ein rechtstatsächliches Bedürfnis zur Ermöglichung der Telekommunikationsüberwachung auch zur Vorsorge für die Verfolgung künftiger Straftaten bislang nicht hinreichend dargetan; der Entwurf sieht daher bewusst davon ab, in diesem Bereich eine Telekommunikationsüberwachung zu ermöglichen.

2.

Die durch die Untersuchung von Meyer-Wieck zur „Rechtswirklichkeit und Effizienz der akustischen Wohnraumüberwachung („großer Lauschangriff“) nach § 100c I Nr. 3 StPO“ (2004) erlangten Erkenntnisse, die sich teilweise mit denen von Albrecht/Dorsch/Krüpe decken, insbesondere soweit Defizite bei der Benachrichtigung Betroffener festgestellt werden (a. a. O., S. 79, 252 ff., 268 ff., 275 f., 365), wurden bereits im Rahmen der Neuregelung der akusti-

schen Wohnraumüberwachung durch das Gesetz zur Umsetzung des Urteils des Bundesverfassungsgerichts vom 3. März 2004 (akustische Wohnraumüberwachung) vom 24. Juni 2005 (BGBl. S. 1841) berücksichtigt.

3.

a) Die von Wolter und Schenke zusammengestellte Textsammlung „Zeugnisverweigerungsrechte bei (verdeckten) Ermittlungsmaßnahmen“ (2002) versammelt die vom Arbeitskreis Strafprozessrecht und Polizeirecht bei dem Mannheimer Institut für deutsches und europäisches Strafprozessrecht und Polizeirecht erarbeiteten Ergebnisse zu dem vom Bundesministerium der Justiz in Auftrag gegebenen Forschungsprojekt „Informationserhebung und Verwertung durch Vernehmung, Auskunft und heimliche Ermittlungsmaßnahmen“. Ziel dieses Forschungsprojekts war die Erarbeitung eines stimmigen Gesamtkonzepts im Bereich der verdeckten Ermittlungsmaßnahmen, das sowohl den von den Zeugnisverweigerungsrechten geschützten Interessen als auch den Belangen einer wirksamen Strafverfolgung besser als die geltende Rechtslage Rechnung trägt. Der vom Arbeitskreis erarbeitete Regelungsvorschlag sieht ein Beweiserhebungs- und -verwertungsverbot für verdeckte Ermittlungsmaßnahmen vor, durch die Informationen erlangt würden, auf die sich die Zeugnisverweigerungsrechte der Verteidiger, Abgeordneten und Pressemitarbeiter einschließlich der jeweiligen Berufshelfer (§ 53a StPO) erstrecken, und ein Beweisverwertungsverbot für solche Erkenntnisse, auf die sich die Zeugnisverweigerungsrechte der Geistlichen, Rechtsanwälte, Ärzte und der anderen in § 53 Abs. 1 Satz 1 Nr. 3 bis 3b StPO genannten Personen, ebenfalls einschließlich der jeweiligen Berufshelfer, erstrecken. Erkenntnisse, die durch das Zeugnisverweigerungsrecht naher Angehöriger gemäß § 52 StPO geschützt sind, sollen nach dem Vorschlag entsprechend einer besonderen Verhältnismäßigkeitsabwägung verwertet werden dürfen.

b) Die Thematik der gesetzlichen Grenzen von Ermittlungsmaßnahmen, insbesondere wenn diese ohne Wissen der Betroffenen durchgeführt werden, ist in der Rechtswissenschaft seit langem überaus umstritten (vgl. etwa Beling, Die Beweisverbote als Grenzen der Wahrheitserforschung im Strafprozess, 1903; Grünwald, JZ 1966, 489 ff.; Otto, GA 1970, 290 ff.; Sydow, Kritik der Lehre von den Beweisverboten, 1976; Dencker, Verwertungsverbote im Strafprozess, 1977; Rengier, Die Zeugnisverweigerungsrechte im geltenden und künftigen Strafverfahrensrecht, 1979; Rogall, ZStW 91 [1979], 1 ff.; Amelung, Informationsbeherrschungsrechte im Strafprozess, 1990; Fezer, Grund-

fragen der Beweisverwertungsverbote, 1995; Görtz-Leible, Die Beschlagnahmeverbote des § 97 Abs. 1 StPO im Lichte der Zeugnisverweigerungsrechte, 2000). Die Analyse der Literatur zeigt, dass es der Rechtswissenschaft bisher nicht gelungen ist, eine praktikable und in sich schlüssige Dogmatik dieser Grenzen zu entwickeln. Die Rechtsprechung folgt insoweit dem Grundsatz, dass zwischen dem öffentlichen Interesse an der Strafverfolgung und den schutzwürdigen Interessen der von Strafverfolgungsmaßnahmen Betroffenen im Einzelfall eine Abwägung vorzunehmen ist (so genannte Abwägungslehre, vgl. Krekeler/Löffelmann, Anwaltskommentar zur StPO, Einleitung, Rn. 140 ff.; Meyer-Goßner, StPO, 49. Aufl., Einl., Rn. 55a).

Ferner hat das Bundesverfassungsgericht entschieden, dass sich ein genereller Vorrang der schutzwürdigen Interessen zeugnisverweigerungsberechtigter Personen, etwa von Pressemitarbeitern, gegenüber dem Strafverfolgungsinteresse verfassungsrechtlich nicht begründen lässt, sondern insofern eine Abwägung im Einzelfall vorzunehmen ist (BVerfGE 107, 299, 332). Insbesondere sei den Zeugnisverweigerungsrechten der Presseangehörigen und der Abgeordneten kein unmittelbarer Bezug zum Kernbereich privater Lebensgestaltung eigen, sondern werde um der Funktionsfähigkeit der Institutionen willen und nicht wegen des Persönlichkeitsschutzes des Beschuldigten gewährt (BVerfGE 109, 279, 323).

c) Vor dem Hintergrund dieser Rechtsprechung wird der Vorschlag des Arbeitskreises nicht umfassend der verfassungsrechtlich gebotenen Flexibilität einer gesetzlichen Regelung zum Ausgleich der widerstreitenden Interessen gerecht. Vielmehr ist bei der Schaffung von Regelungen, die die Ermittlung des wahren Sachverhalts gefährden und damit zu ungerechten – weil materiell unrichtigen – Verfahrensergebnissen führen können, besondere Zurückhaltung geboten. Die wirksame Strafverfolgung, das Interesse an einer umfassenden Wahrheitsermittlung und die Aufklärung von schweren Straftaten ist wesentlicher Auftrag des Rechtsstaates. Der Gesetzgeber hat daher bei der Prüfung der Gewährung eines absoluten Vorrangs bestimmter Interessen gegenüber anderen wichtigen Gemeinschaftsgütern den Erfordernissen einer an rechtsstaatlichen Garantien ausgerichteten Rechtspflege Rechnung zu tragen. Auch können Regelungen, die die Wahrheitsermittlung beschränken, nicht nur die Interessen des rechtsstaatlichen Gemeinwesens, sondern auch das Recht des Beschuldigten auf ein faires, rechtsstaatliches Verfahren beeinträchtigen, weil die aufgrund von Erhebungs- und Verwertungsverboten nicht verfügbaren Erkenntnisse nicht nur der Anklage sondern auch der Verteidigung entzogen sind. Zeugnisverweigerungsrechte und Ermittlungsverbote beschränken mithin die Möglichkeit des Beschuldigten, einen gegen ihn

erhobenen Verdacht auszuräumen. Beweiserhebungs- und -verwertungsverbote stellen damit Ausnahmen von der Pflicht zur umfassenden Aufklärung der materiellen Wahrheit dar und begründen die Gefahr unrichtiger Entscheidungen. Die Begründung solcher Ausnahmen bedarf stets einer Legitimation, die vor dem Rechtsstaatsprinzip bestand hat (BVerfGE 33, 367, 383; vgl. auch Löffelmann, ZStW 118 [2006], S. 358, 373 f.).

d) Der Entwurf verfolgt daher mit der Einfügung eines neuen § 53b StPO-E ein sich zwar systematisch an den Vorschlag des Arbeitskreises anlehnendes, inhaltlich hiervon aber zum Teil deutlich abweichendes Konzept der Begründung von Erhebungs- und Verwertungsverboten bei zeugnisverweigerungsberechtigten Berufsgeheimnisträgern:

- Ein umfassendes – absolutes – Erhebungs- und Verwertungsverbot ist nur gerechtfertigt, wenn ein entsprechend absolut geschützter Belang dies fordert. Dies hat das Bundesverfassungsgericht in seiner Entscheidung zur akustischen Wohnraumüberwachung (a. a. O., Rn. 148) mit Blick auf die Menschenwürde hinsichtlich des seelsorgerischen Gesprächs mit einem Geistlichen sowie des Gesprächs mit dem Verteidiger angenommen. Dem trägt das Erhebungs- und Verwertungsverbot in § 53b Abs. 1 StPO-E Rechnung.

- Einbezogen in dieses absolute Erhebungs- und Verwertungsverbot werden auch die Parlamentsabgeordneten. Deren Zeugnisverweigerungsrecht weist zwar nach den Darlegungen des Bundesverfassungsgerichts keinen unmittelbaren Bezug zu dem aus der Menschenwürde resultierenden Kernbereich privater Lebensgestaltung auf. Die Kommunikation mit Abgeordneten unter einen besonderen, Erhebungen ohne Billigung des Abgeordneten ausschließenden Schutz zu stellen, rechtfertigt sich indessen aus Artikel 47 GG, der für diese Berufsgruppe ein Zeugnisverweigerungsrecht und ein dieses flankierendes Beschlagnahmeverbot ausdrücklich vorgibt. Sind aber bereits diese offenen Ermittlungsmaßnahmen gegenüber Abgeordneten von deren Einverständnis (Nichtausübung des Zeugnisverweigerungsrechts) abhängig, so spricht der damit vom Grundgesetzgeber intendierte weitreichende Schutz der Abgeordneten dafür, auch andere, insbesondere verdeckte Ermittlungsmaßnahmen zu untersagen, soweit das Zeugnisverweigerungsrecht der Abgeordneten reicht.

- Hinsichtlich der übrigen Berufsgeheimnisträger, denen § 53 Abs. 1 Satz 1 Nr. 3 bis 3b und Nr. 5 StPO ein Zeugnisverweigerungsrecht zubilligt, sieht § 53b Abs. 2 StPO-E ein relatives Beweiserhebungs- und –verwertungsverbot vor, dessen

Reichweite im Einzelfall durch eine Verhältnismäßigkeitsprüfung zu bestimmen ist; dies erfordert eine Abwägung der widerstreitenden Interessen im konkreten Fall.

- Berufshelfer (§ 53a StPO) werden durch § 53b Abs. 3 StPO-E in diese Regelungen in Akzessorietät zum jeweiligen Berufsgeheimnisträger einbezogen.

- § 53b Abs. 4 Satz 1 StPO-E stellt klar, dass diese Schutzregelungen keine Anwendung finden, wenn die zeugnisverweigerungsberechtigte Person in die aufzuklärende Straftat verstrickt und deshalb ein Ermittlungsverfahren gegen sie eingeleitet ist. In Ansehung der Presseangehörigen findet diese Verstrickungsregelung bei Straftaten, die nur auf Antrag oder Ermächtigung verfolgbar sind, nur Anwendung, wenn der Strafantrag gestellt bzw. die Ermächtigung erteilt ist (vgl. § 53b Abs. 4 Satz 2 StPO-E). Damit wird dem rechtspolitischen Willen Rechnung getragen, den institutionellen Schutz der Presse im Verfahrensrecht nochmals weiter auszubauen.

- Die Neuregelung des § 53b StPO-E ist schließlich – anders als der Vorschlag des Arbeitskreises – nicht auf den Bereich der verdeckten Ermittlungsmaßnahmen beschränkt, sondern gilt grundsätzlich bei allen Ermittlungsmaßnahmen. Denn für eine Differenzierung zwischen verdeckten und offenen Ermittlungsmaßnahmen sind insoweit keine durchgreifenden tragfähigen Gründe erkennbar. Eine Ausnahme hiervon ergibt sich lediglich aus § 53b Abs. 5 StPO-E, der klarstellt, dass die im geltenden Recht speziell normierten besonderen Erhebungsverbote im Bereich der Beschlagnahme und der akustischen Wohnraumüberwachung (§§ 97, 100c Abs. 6 StPO) unberührt bleiben, § 53b StPO-E also zugunsten dieser spezielleren Regelungen insoweit keine Anwendung findet. Auch bleibt das von der Neuregelung in § 53b StPO-E vorausgesetzte Recht zur Zeugnisverweigerung nach den §§ 53, 53a StPO – selbstverständlich – unberührt; insbesondere werden die Zeugnisverweigerungsrechte der in § 53 Abs. 1 Satz 1 Nr. 3 bis 3b und Nr. 5 StPO genannten Berufsgeheimnisträger nicht durch die Regelung in § 53b Abs. 2 StPO-E relativiert, sondern bleiben im vollen Umfang erhalten. Entsprechendes gilt, soweit das Gesetz den zur Zeugnisverweigerung Berechtigten die Möglichkeit einräumt, die Maßnahmen aufgrund des Zeugnisverweigerungsrechts zu verweigern, wie dies in § 81c Abs. 3 Satz 1 StPO der Fall ist.

IV.

Der Entwurf zielt auch auf die Behebung von Unsicherheiten, die in der Rechtsanwendung beim Einsatz verdeckter Ermittlungsmaßnahmen aufgetreten sind.

- Schwierigkeiten bereitet der Praxis etwa, dass die Auskunftsanordnung über Verkehrsdaten nach § 100h Abs. 1 Satz 1 StPO sowie die Anordnung der Telekommunikationsüberwachung nach den §§ 100a, 100b StPO den Namen und die Anschrift der Person, gegen die sie sich richtet, enthalten muss, was bei namentlich noch nicht genau bekannten Beschuldigten nicht möglich ist. Der Entwurf trägt dieser Problematik Rechnung, indem er diese Angaben nur noch verlangt, soweit dies möglich ist, die Angaben also bekannt sind (§ 100b Abs. 2 Satz 2 Nr. 1 StPO-E).

- Durch die in § 100b Abs. 2 Satz 2 Nr. 2 StPO-E aufgenommene Anknüpfung auch an die Endgerätekennung wird die – bisher umstrittene, in § 23b Abs. 4 Satz 2 Nr. 2 Zollfahndungsdienstgesetz (ZFdG) vom Gesetzgeber indessen bereits grundsätzlich bejahte – Zulässigkeit der so genannten „IMEI[1]-gestützten“ Telekommunikationsüberwachung klargestellt.

- Zu zeitweise erheblicher Unsicherheit, nach welchen Vorschriften bei der Beschlagnahme von Datenträgern, auf denen Verkehrsdaten gespeichert sind, verfahren werden muss, hat der Beschluss des Bundesverfassungsgerichts vom 4. Februar 2005 - 2 BvR 308/04 – geführt (vgl. NJW 2005, 1637 ff.). Der Entwurf stellt in § 100g Abs. 3 StPO-E für die Zulässigkeit der Erhebung solcher Daten die Anwendbarkeit der allgemeinen Vorschriften klar. Neben den allgemeinen Befugnisregelungen in §§ 161, 163 StPO kommen somit für eine zwangsweise Sicherstellung insbesondere die §§ 94 ff. StPO zur Anwendung. Dies entspricht auch den verfassungsrechtlichen Vorgaben, wie sich aus dem inzwischen ergangenen Urteil des Bundesverfassungsgericht vom 2. März 2006, 2 BvR 2099/04, ergibt, wonach die im Herrschaftsbereich des Kommunikationsteilnehmers gespeicherten Verkehrsdaten nicht durch das Fernmeldegeheimnis nach Artikel 10 Abs. 1 GG sondern durch das Recht auf informationelle Selbstbestimmung nach Artikel 2 Abs. 1 i. V. m. Artikel 1 Abs. 1 GG geschützt werden (BVerfG, 2 BvR 2099/04 vom 2. März 2006, Absatz-Nr. 72 = BVerfGE 115, 166 ff.). In diesem Zusammenhang ist ferner festzuhalten, dass sich auch die Erhebung und die ggf. zwangsweise Sicherstellung von Bestands- und Nutzungsdaten bei Telemediendiensten im Strafverfahren nach den allgemeinen Bestimmungen richten, es insoweit also keiner speziellen gesetzlichen Regelung bedarf, wie sie sich

[1] IMEI = International Mobile Equipment Identity.

etwa für die Befugnisse des Bundesamtes für Verfassungsschutz in § 8a BVerfSchG findet.

- In der Praxis besteht gelegentlich auch Unsicherheit, welches Gericht für Überwachungs- und Auskunftsanordnungen zuständig ist, wenn ein Anbieter von Telekommunikationsdiensten an einem anderen Ort als dem Sitz der Gesellschaft eine Niederlassung oder Abteilung errichtet, die die Überwachungsmaßnahme technisch umsetzt. Der Entwurf löst dieses Problem durch die Konzentrationsregelung des § 162 Abs. 1 StPO-E, die zugleich eine Spezialisierung in der ermittlungsgerichtlichen Tätigkeit fördert und damit eine gesteigerte Effektivität der mit dem Richtervorbehalt bezweckten rechtsstaatlichen Kontrolle erwarten lässt.

- Unsicherheiten bestanden in der Praxis auch bei der Frage, ob die Auskunft über den Inhaber einer dynamischen IP-Adresse auf ein Auskunftsersuchen nach den §§ 161, 163 StPO i. V. m. § 113 TKG gestützt werden kann oder nur nach Maßgabe der §§ 100g, 100h StPO zu erlangen ist. Es wurde deshalb erwogen, dieser Unsicherheit durch eine klarstellende Regelung in § 113 TKG zu begegnen. Dies erscheint jedoch aufgrund der inzwischen gefestigten und zutreffenden Rechtsprechung, die zur Anwendbarkeit des § 113 TKG gelangt, nicht mehr erforderlich (vgl. LG Stuttgart, MMR 2005, 628 ff.; MMR 2005, 624 ff.; LG Hamburg, MMR 2005, 711; LG Würzburg, NStZ-RR 2006, 46; LG Hechingen, Beschluss vom 19. April 2005 – 1 Qs 41/05; vgl. auch zum österreichischen Recht: OGH, ZUM RD 2006, 59; a. A. – soweit ersichtlich – nur noch LG Bonn, DuD 2005, 832 ff.). Dem folgt ein Teil der Literatur (vgl. Löffelmann, AnwBl 2006, 598, 601; Meyer-Goßner, a. a. O., §100g, Rn. 4; Sankol, MMR 2006, 361, 365; im Ergebnis auch Seitz, Strafverfolgungsmaßnahmen im Internet, 2004, S. 96 ff.). Soweit in der Literatur teilweise die gegenteilige Auffassung vertreten wird (vgl. Bär, MMR 2005, 626 f., und Gercke, CR 2005, 598 ff., jeweils in Anmerkungen zu den vorgenannten Beschlüssen des LG Stuttgart; Gnirck/Lichtenberg, DuD 2004, 598; Köbele, DuD 2004, 609), überzeugen die dafür vorgebrachten Gründe nicht.

  Dass für die Auskunft über Bestandsdaten zu einer statischen IP-Adresse die Regelungen der §§ 111 ff. TKG i. V. m. den in § 161 Abs. 1 Satz 1 und § 163 StPO enthaltenen allgemeinen Befugnissen der Strafverfolgungsbehörden einschlägig sind, entspricht allgemeiner Auffassung. Für die Auskunft über Bestandsdaten zu einer dynamischen IP-Adresse gilt indessen nichts anderes. Maßgebend ist, dass entsprechende Auskunftsersuchen der Strafverfolgungsbehörden allein auf die Mitteilung der den Regelungen der §§ 111 ff. TKG unterfallenden Bestandsdaten gerichtet sind und nicht auf die Erhebung von – bei Stel-

lung des Auskunftsersuchens den Strafverfolgungsbehörden notwendigerweise bereits bekannten – Verkehrsdaten, die in besonderer Weise von Artikel 10 GG geschützt sind. Der Umstand, dass der zur Auskunft verpflichtete Dienstleister zur Erfüllung des Auskunftsanspruchs bei dynamischen IP-Adressen regelmäßig anhand interner Verkehrsdatenaufzeichnungen eine Zuordnung zu einer Kundenkennung vornehmen und sodann anhand dieser den Namen und die Anschrift des Kunden aus den Bestandsdaten recherchieren und beauskunften muss, ändert nichts daran, dass die Strafverfolgungsbehörden insoweit lediglich ein Bestandsdatum erheben. Dies hat der Gesetzgeber bereits bei der Einfügung der §§ 100g, 100h StPO in der 14. Legislaturperiode klar zum Ausdruck gebracht, indem er darauf hingewiesen hat, dass sich Auskünfte über den Namen der „hinter einer“ IP- oder E-Mail-Adresse stehenden Person nach den Regelungen des Telekommunikationsgesetzes über die Bestandsdatenabfrage richten (vgl. BT-Drs. 14/7008, S. 7). Der Bundesrat hat sich diese Auffassung in seiner Stellungnahme zum Entwurf eines Gesetzes zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums inhaltlich zu Eigen gemacht (BR-Drs 64/07 [Beschluss] S. 7 ff.).

V.

Der Entwurf verfolgt auch das Ziel, die das Strafverfahrensrecht betreffenden Vorgaben des von Deutschland am 23. November 2001 unterzeichneten Übereinkommens des Europarats über Computerkriminalität (Nr. 185 der Sammlung der Europäischen Verträge [SEV]) in das nationale Recht umzusetzen.

- Artikel 16 Abs. 1 des Übereinkommens verpflichtet die Vertragsparteien, die erforderlichen gesetzgeberischen Maßnahmen zu treffen, damit ihre zuständigen Behörden die beschleunigte Sicherung bestimmter Computerdaten einschließlich Verkehrsdaten, die mittels eines Computersystems gespeichert wurden, anordnen oder in ähnlicher Weise bewirken können, insbesondere wenn Grund zu der Annahme besteht, dass bei diesen Computerdaten eine besondere Gefahr des Verlusts oder der Veränderung besteht.

  Die Beschlagnahme von Computerdaten erfolgt nach deutschem Strafverfahrensrecht durch Beschlagnahme der Datenträger, auf denen die Daten gespeichert sind (vgl. Schäfer, in: Löwe/Rosenberg, StPO, 25. Aufl., § 94, Rn. 14, 27 f.; Meyer-Goßner, a. a. O., § 94, Rn. 4; Nack, in: Karlsruher Kommentar zur StPO, 5. Aufl., § 94, Rn. 4; Bär, Der Zugriff auf Computerdaten im Strafverfahren, 1992, 246 ff.; Germann, Gefahrenabwehr und Strafverfolgung im Internet, 2000, 533 ff.; Gercke, MMR 2004, 801, 805). Die von Ar-

tikel 16 Abs. 1 des Übereinkommens geforderte Ermöglichung einer beschleunigten Sicherung gespeicherter Computerdaten kann zwar im deutschen Recht bei Gefahr im Verzug durch eine Beschlagnahmeanordnung der Staatsanwaltschaft und ihrer Ermittlungspersonen nach § 98 Abs. 1 Satz 1 StPO erfolgen. Problematisch ist dies allerdings, wenn ein Zugriff auf vom Zugangsgerät (z. B. Personal Computer) räumlich getrennte Teile eines Computersystems (z. B. Netzwerkrechner im Intra- oder Internet) erfolgen soll und die Gefahr besteht, dass bis zur physischen Beschlagnahme des Datenträgers beweisrelevante Daten gelöscht werden. Artikel 19 Abs. 2 des Übereinkommens verpflichtet die Vertragsparteien daher auch, die erforderlichen gesetzgeberischen Maßnahmen zu treffen, um sicherzustellen, dass ihre Behörden eine Durchsuchung oder einen ähnlichen Zugriff schnell auf ein weiteres Computersystem ausdehnen können, wenn sie ein bestimmtes Computersystem oder einen Teil davon durchsuchen oder in ähnlicher Weise darauf Zugriff nehmen und Grund zu der Annahme haben, dass die gesuchten Daten in einem anderen Computersystem oder einem Teil davon in ihrem Hoheitsgebiet gespeichert sind, und diese Daten von dem ersten System aus rechtmäßig zugänglich oder verfügbar sind. In diesem Zusammenhang sieht Artikel 32 des Übereinkommens unter den dort genannten Voraussetzungen vor, dass die Durchsuchung auch auf zugängliche Daten im Ausland erstreckt werden kann.

Da die Möglichkeit, die Durchsuchung auf weitere Computersysteme auszudehnen, im geltenden Recht noch nicht verankert ist (vgl. Bär, a. a. O., S. 217 ff.; Germann, a. a. O., S. 544 f.; Matzky, Zugriff auf EDV im Strafprozess, 1999, S. 238), erlaubt § 110 Abs. 3 StPO-E die Durchsicht elektronischer Datenträger auf räumlich getrennte Speichereinheiten, auf die der Betroffene Zugriff zu gewähren berechtigt ist, zu erstrecken und Daten, die für die Untersuchung von Bedeutung sein können, zu speichern, wenn bis zur Sicherstellung der räumlich getrennten Datenträger ihr Verlust zu besorgen ist.

- Im Zusammenhang mit der von Artikel 17 des Übereinkommens angesprochenen beschleunigten Sicherung von Verkehrsdaten ist ferner problematisch, dass die zur Erteilung einer Auskunft nach den §§ 100g, 100h StPO benötigten Daten derzeit oftmals entweder überhaupt nicht gespeichert werden oder mitunter bereits gelöscht sind, bevor eine gerichtliche Auskunftsanordnung erwirkt werden kann. Es ist daher fraglich, ob die grundsätzlich notwendige gerichtliche Anordnung der Auskunftserteilung die von Artikel 17 i. V. m. Artikel 16 Abs. 1 des Übereinkommens geforderte beschleunigte Sicherung von Verkehrsdaten in ausreichender Weise zulässt (vgl. Gercke, CR 2004, 782, 790; ders., MMR 2004, 801, 802). Um einen Verlust der benötigten Daten zu vermeiden und rechtsstaatlichen Bedenken gegen die verbreitet praktizierte informelle telefonische Kontaktauf-

nahme durch die Strafverfolgungsbehörden mit den Diensteanbietern mit der Bitte um vorläufige Sicherung der benötigten Daten (vgl. Gercke, MMR 2004, 801, 802) zu begegnen, wurde zunächst erwogen, in § 100g StPO-E die zur Beauskunftung Verpflichteten auch zu verpflichten, die von ihnen erhobenen Verkehrsdaten aufgrund einer polizeilichen oder staatsanwaltschaftlichen Anordnung für die Dauer von einer Woche bereitzuhalten, wenn die Strafverfolgungsbehörden die Beantragung einer gerichtlichen Anordnung zur Erhebung der Daten ankündigen. Dies hat sich indessen aufgrund der Richtlinie 2006/24/EG über die „Vorratsspeicherung“ von Verkehrsdaten als entbehrlich erwiesen (vgl. dazu nachfolgend unter VI.).

- Artikel 16 und 17 des Übereinkommens zielen generell auf die Sicherung gespeicherter Computer- und Verkehrsdaten für die Verwendung in Strafverfahren. Eine Beschränkung der Auskunftspflicht auf Stellen, die Telekommunikationsdienste geschäftsmäßig erbringen, wie bisher in § 100g Abs. 1 Satz 1 StPO geregelt, sehen die Vorschriften nur unter der Vorbehaltsmöglichkeit von Artikel 16 Abs. 4 i. V. m. Artikel 14 Abs. 3 Buchstabe b des Übereinkommens vor, also nur, soweit die Erhebung von Verkehrsdaten in Echtzeit betroffen ist. Der Entwurf erweitert daher den Anwendungsbereich des § 100g StPO auf alle Personen und Stellen, die in den Übermittlungsvorgang eingeschaltet sind, unabhängig davon, ob sie entsprechende Dienste geschäftsmäßig erbringen.

- Artikel 20 Abs. 1 Buchstabe a des Übereinkommens verpflichtet die Vertragsparteien schließlich, die erforderlichen gesetzgeberischen Maßnahmen zu treffen, um die Erhebung von solchen Verkehrsdaten in Echtzeit zu ermöglichen, die „mit bestimmten in ihrem Hoheitsgebiet mittels eines Computersystems übermittelten Kommunikationen in Zusammenhang stehen“. Eine Beschränkung der Echtzeiterhebung auf bestimmte Straftaten ist in Artikel 20 des Übereinkommens nicht vorgesehen, wäre aber aufgrund der Vorbehaltsmöglichkeit nach Artikel 20 Abs. 4 i. V. m. Artikel 14 Abs. 3 Buchstabe a des Übereinkommens möglich. Die bislang geltende deutsche Regelung einer Gleichbehandlung der Echtzeiterhebung von Verkehrsdaten und Daten über den Inhalt einer Telekommunikation nach Maßgabe des § 100a StPO würde zugleich die äußerste Grenze eines nach Artikel 14 Abs. 3 Buchstabe b des Übereinkommens zulässigen Vorbehalts darstellen. Eine Echtzeiterhebung von Verkehrsdaten ist nach dem Übereinkommen also jedenfalls für solche Straftaten vorzusehen, für die auch eine inhaltliche Überwachung der Telekommunikation erlaubt ist, mithin für alle Katalogstraftaten des § 100a StPO.

  Allerdings haben sich die Vertragsparteien in Artikel 14 Abs. 2 Satz 5 des Übereinkommens verpflichtet, die Möglichkeit zu prüfen, einen solchen Vorbehalt zu beschränken,

damit die Erhebung von Verkehrsdaten in Echtzeit im weitest möglichen Umfang angewendet werden kann. Diese Prüfung hat ergeben:

Eine im Sinne der Vorbehaltsoption mögliche – eine effektive Strafverfolgung freilich beeinträchtigende – Beschränkung der Echtzeiterhebung von Verkehrsdaten entsprechend den Regelungen zur Erhebung von Inhaltsdaten im Sinne des § 100a StPO ist nach deutschem Recht aufgrund der unterschiedlichen Eingriffsintensität beider Maßnahmen verfassungsrechtlich nicht geboten. Die bereits bisher in § 100g Abs. 1 StPO enthaltenen – und zumal die aufgrund des gegenständlichen Entwurfs hinzukommenden – materiellen Beschränkungen der Erlangung von Verkehrsdaten gewährleisten vielmehr auch hinsichtlich der Erhebung von Verkehrsdaten in Echtzeit eine ausreichende Begrenzung der Maßnahme. Hinzu kommt, dass durch die Harmonisierung des § 100g StPO-E mit den Verfahrensregelungen in den §§ 100b, 101 StPO-E auch bei der Erhebung von Verkehrsdaten der Rechtsschutz Betroffener gegenüber der bisherigen Rechtslage verbessert wird. Es ist deshalb sinnvoll und sachgerecht, die Befugnis zur Verkehrsdatenerhebung grundsätzlich so auszugestalten, dass auch die Echtzeiterhebung dieser Daten unter den Voraussetzungen des § 100g StPO möglich ist. Dies wird regelungstechnisch insbesondere durch die weitgehende Bezugnahme in § 100g Abs. 2 Satz 1 StPO-E auf § 100b StPO-E erreicht.

Die Erhebung von Standortdaten in Echtzeit soll allerdings – bei Vorliegen der weiteren Anordnungsvoraussetzungen – wegen der damit verbundenen Möglichkeit, ein aktuelles Bewegungsbild des Betroffenen zu erstellen, lediglich bei einer Straftat von auch im Einzelfall erheblicher Bedeutung, nicht jedoch bei sämtlichen mittels Telekommunikation begangenen Straftaten zulässig sein. Dies wird in § 100g Abs. 1 Satz 3 StPO-E klargestellt. Ein Abweichen von den Vorgaben des Artikels 20 des Übereinkommens des Europarats über Computerkriminalität ist damit nicht verbunden. Denn danach ist die Echtzeiterhebung nur bei solchen Verkehrsdaten geboten, die das Übereinkommen in Artikel 1 Buchstabe d als Verkehrsdaten definiert. Von der dortigen Definition sind aber die Standortdaten nicht erfasst.

VI.

Schließlich dient der Entwurf der Umsetzung der Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder

öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (ABl. EU Nr. L 105 S. 54 ff.).

1.

Die wesentlichen Eckpunkte der Richtlinie sind wie folgt zu beschreiben:

Nach ihrem Artikel 1 Abs. 1 dient die Richtlinie zunächst der Harmonisierung der Vorschriften über die obligatorische Speicherung von Verkehrsdaten in den Mitgliedstaaten und bezweckt zugleich, die Verfügbarkeit dieser Daten für Strafverfolgungszwecke sicherzustellen.

Gemäß Artikel 3 Abs. 1 der Richtlinie haben die Mitgliedstaaten dafür Sorge zu tragen, dass die in Artikel 5 Abs. 1 der Richtlinie im Einzelnen bestimmten Arten von Daten ohne einzelfallbezogenen Anlass („auf Vorrat“) gespeichert werden, soweit sie von den Diensteanbietern bei der Bereitstellung ihrer Telekommunikationsdienste erzeugt oder verarbeitet werden. Nach Artikel 6 der Richtlinie ist eine Speicherungsdauer von mindestens sechs und höchstens 24 Monaten vorzusehen. Artikel 5 Abs. 2 der Richtlinie stellt klar, dass Daten, die Aufschluss über den Inhalt der Kommunikation geben, nach dieser Richtlinie nicht gespeichert werden dürfen.

Aus der Beschreibung des Speicherungszwecks in Artikel 1 Abs. 1 der Richtlinie folgt zugleich, dass eine Verwendung der nach Maßgabe der Richtlinie gespeicherten Daten für die dort genannten Strafverfolgungszwecke zulässig ist. Zu der Frage, ob diese Daten zu weiteren Zwecken sollen Verwendung finden dürfen, verhält sich die Richtlinie bewusst nicht. Artikel 11 der Richtlinie i. V. m. Artikel 15 Abs. 1 der Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG) bringt vielmehr zum Ausdruck, dass die Richtlinie insoweit keine abschließende Regelung darstellt und die „auf Vorrat“ gespeicherten Daten daher – in den Grenzen von Artikel 15 Abs. 1 der Richtlinie 2002/58/EG – für weitere Zwecke verwendet werden dürfen. Unabhängig von der Frage der zulässigen Verwendungszwecke verpflichtet Artikel 4 der Richtlinie die Mitgliedstaaten zur Schaffung angemessener Vorschriften über die Weitergabe der und den Zugang zu den nach Maßgabe der Richtlinie gespeicherten Daten.

Artikel 7 und 13 der Richtlinie machen Vorgaben zu Datenschutz und Datensicherheit sowie zu Rechtsbehelfen, Haftung und Sanktionen, die weitgehend der geltenden Rechtslage ent-

sprechen und deren Geltung auch im Zusammenhang mit den nach Maßgabe der Richtlinie zu speichernden Daten klarstellen.

Artikel 10 der Richtlinie verpflichtet die Mitgliedstaaten, der Kommission jährlich eine Statistik mit in Artikel 10 im Einzelnen beschriebenen Angaben zu übermitteln. Die Angaben sollen einfließen in die von der Kommission nach Artikel 14 der Richtlinie bis zum 15. September 2010 vorzulegende Bewertung der Anwendung der Richtlinie sowie ihrer Auswirkungen auf Wirtschaft und Verbraucher. Diese Bewertung soll der Feststellung etwa erforderlicher Änderungen der Richtlinie insbesondere aufgrund fortschreitender Entwicklungen in der Telekommunikationstechnologie dienen.

2.

Die Frage, auf welche Rechtsgrundlage ein Instrument der EU zur Einführung von Speicherungspflichten für Verkehrsdaten zu stützen ist, war Gegenstand kontroverser Diskussionen während der Beratungen auf europäischer Ebene und in den Mitgliedstaaten und wird bis heute unterschiedlich beurteilt. Sowohl der von Frankreich, Schweden, Irland und Großbritannien am 28. April 2004 vorgelegte und zunächst beratene Entwurf für einen Rahmenbeschluss, der auf die Artikel 31 und 34 des Vertrages über die Europäische Union (EU-Vertrag) gestützt war, als auch der Kommissionsvorschlag für eine auf Artikel 95 des Vertrages zur Gründung der Europäischen Gemeinschaft (EG-Vertrag) gestützte Richtlinie vom 21. September 2005 war dem Einwand einer verfehlten Rechtsgrundlagenwahl ausgesetzt.

Die juristischen Dienste der Kommission und des Rates vertraten in ihren gutachterlichen Stellungnahmen vom 22. März 2005 bzw. 5. April 2005 übereinstimmend die Auffassung, dass es sich bei der Einführung von Speicherungspflichten für Verkehrsdaten um eine gemeinschaftsrechtliche Angelegenheit handele, die nicht Gegenstand eines Rahmenbeschlusses in der so genannten „Dritten Säule“ der EU (Titel VI des EU-Vertrages über die polizeiliche und justizielle Zusammenarbeit in Strafsachen) sein könne. Zur Begründung wurde im Wesentlichen angeführt, dass der Umgang mit Verkehrsdaten bereits in Artikel 6 Abs. 1 der Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG) geregelt sei, der grundsätzlich eine Löschung oder Anonymisierung der Daten vorsehe. Ein Rechtsinstrument, das die Mitgliedstaaten zum Erlass von Regelungen zur Speicherung dieser Daten verpflichte, berühre diese Vorschrift und sei somit nach Artikel 47 des EU-Vertrages in der „Dritten Säule“ unzulässig. Auch die in Artikel 15 Abs. 1 der Datenschutzrichtlinie für elektronische Kommunikation enthaltene Öffnungsklausel für bestimmte abweichende Rechtsvor-

schriften in den Mitgliedstaaten führe nicht zu einer anderen Bewertung, da sie als Ausnahmeregelung restriktiv auszulegen sei und grundsätzlich nur abweichende Regelungen im Einzelfall zulasse. Dass die einzelnen Mitgliedstaaten teils keinerlei, teils sehr unterschiedliche Speicherungsvorschriften für Verkehrsdaten erlassen hätten, beeinträchtige den Binnenmarkt für elektronische Kommunikation, da die zumeist grenzüberschreitend tätigen Diensteanbieter mit unterschiedlichen Rechtsvorschriften konfrontiert seien. Ein Rechtsinstrument zur Einführung EU-weit einheitlicher Speicherungspflichten diene der Harmonisierung dieser unterschiedlichen Rechtsregime und fördere damit das Funktionieren des Binnenmarktes. Somit sei ein solches Rechtsinstrument auf Artikel 95 des EG-Vertrages zu stützen und im Verfahren der Mitentscheidung des Europäischen Parlaments nach Artikel 251 des EG-Vertrages zu erlassen. Diese Ansicht wurde zuletzt auch von allen Mitgliedstaaten (mit Ausnahme Irlands und der Slowakei) vertreten.

Auch die Bundesregierung vermochte sich den dargelegten Erwägungen letztlich nicht zu verschließen, zumal ihre zunächst – in Übereinstimmung mit dem Deutschen Bundestag und dem Bundesrat – vertretene gegenteilige Haltung durch das Urteil des Europäischen Gerichtshofs vom 13. September 2005 (Rs. C-176/03), durch das der Rahmenbeschluss des Rates über den Schutz der Umwelt durch das Strafrecht für nichtig erklärt worden war, weil er in die der Gemeinschaft übertragenen Zuständigkeiten übergegriffen habe, erheblich geschwächt wurde. Vor diesem Hintergrund hat die Bundesregierung der Richtlinie beim Ministerrat für Justiz und Inneres am 21. Februar 2006 zugestimmt, nachdem sie hierzu durch Beschluss des Deutschen Bundestages vom 16. Februar 2006 (BT-Drs. 16/545, S. 4) aufgefordert worden war.

3.

Die zur Umsetzung der Richtlinie erforderlichen Rechtsvorschriften sind nach Artikel 15 Abs. 1 Satz 1 der Richtlinie hinsichtlich der Verkehrsdaten aus den Bereichen der Festnetz- und der Mobilfunktelefonie bis zum 15. September 2007 in Kraft zu setzen. Betreffend die Speicherungspflichten für Verkehrsdaten aus dem Bereich des Internets hat sich Deutschland – neben 15 weiteren Mitgliedstaaten – die von Artikel 15 Abs. 3 der Richtlinie eingeräumte Möglichkeit vorbehalten, das Inkrafttreten insoweit bis zum 15. März 2009 aufzuschieben.

Diese zeitlichen Vorgaben sind unabhängig von den Erfolgsaussichten der von Irland unter dem 5. Juli 2006 gegen die Richtlinie beim Europäischen Gerichtshof erhobenen Nichtig-

keitsklage (Rs. C-301/06) zu beachten. Der verschiedentlich geforderte Aufschub der Umsetzung bis zur Entscheidung des Europäischen Gerichtshofs in der vorgenannten Rechtssache kommt schon aus rechtlichen Gründen nicht in Betracht, da der erhobenen Nichtigkeitsklage gemäß Artikel 242 Satz 1 des EG-Vertrages eine aufschiebende Wirkung nicht zukommt. Die anhängige Klage entbindet die Mitgliedstaaten mithin nicht von ihrer aus Artikel 249 des EG-Vertrages folgenden Pflicht zur Umsetzung der Richtlinie und rechtfertigt nicht einen Verstoß gegen das Gemeinschaftsrecht. Hinzu kommt, dass der Deutsche Bundestag die Bundesregierung in seinem Beschluss vom 16. Februar 2006 (BT-Drs. 16/545, S. 4) aufgefordert hat, alsbald den Entwurf eines Umsetzungsgesetzes vorzulegen.

4.

Der vorliegende Entwurf berücksichtigt die Forderungen des Deutschen Bundestages, hinsichtlich der Speicherungsdauer und der erfassten Datenarten keine über die Mindestvorgaben der Richtlinie hinausgehenden Regelungen vorzusehen und die Verwendung der gespeicherten Daten für Strafverfolgungszwecke nur bei erheblichen oder mittels Telekommunikation begangenen Straftaten zuzulassen (BT-Drs. 16/545, S. 4). Nach Maßgabe dieser Forderungen setzt Artikel 2 dieses Entwurfs (Änderungen des TKG) die Vorgaben der Richtlinie im Wesentlichen wie folgt um:

Die Bestimmung der von den Diensteanbietern nach § 113a Abs. 2 bis 4 TKG-E zu speichernden Datenarten beschränkt sich auf die Vorgaben des Artikels 5 Abs. 1 der Richtlinie.

Eine Pflicht zur Speicherung dieser Daten auch im Falle „erfolgloser Anrufversuche“ i. S. v. Artikel 3 Abs. 2, Artikel 2 Abs. 2 Buchstabe f der Richtlinie besteht nach § 113a Abs. 5 TKG-E lediglich, soweit diese Daten von den Diensteanbietern ohnehin für die in § 96 Abs. 2 TKG genannten Zwecke gespeichert oder protokolliert werden. Nach § 113a Abs. 2 Nr. 4 Buchstabe c TKG-E werden nur die Standortdaten des anrufenden und des angerufenen Anschlusses bei Beginn der Mobilfunkverbindung zu speichern sein.

Gemäß § 113a Abs. 8 TKG-E dürfen der Inhalt der Kommunikation und Daten über aufgerufene Internetseiten auf Grund der vorstehenden Speicherungsregelungen nicht gespeichert werden.

§ 113a Abs. 1 Satz 1 TKG-E sieht eine Speicherungsdauer von sechs Monaten vor.

Die Verwendung der gespeicherten Verkehrsdaten ist nach § 113b Satz 1 TKG-E für die Zwecke der Strafverfolgung, der Abwehr erheblicher Gefahren für die öffentliche Sicherheit sowie der Erfüllung der gesetzlichen Aufgaben der Nachrichtendienste zulässig. Strafverfolgungsbehörden können nach § 100g Abs. 1 StPO-E (i. V. m. § 100b Abs. 3 StPO-E) von den Diensteanbietern Auskunft über gespeicherte Verkehrsdaten zur Verfolgung von Straftaten von auch im Einzelfall erheblicher Bedeutung sowie zur Verfolgung von mittels Telekommunikation begangenen Straftaten verlangen, wobei § 100g Abs. 1 Satz 2 StPO-E die Verwendung der Daten für die letztgenannte Fallgruppe durch eine enge Subsidiaritätsklausel einschränkt und zudem betont, dass die Datenerhebung in einem angemessenen Verhältnis zur Bedeutung der Sache stehen muss.

Eine Entschädigung der Diensteanbieter für mit der Erfüllung der Speicherungspflichten etwa verbundene Investitionsaufwendungen sieht der Entwurf nicht vor. Dies entspricht der bisherigen Rechtslage nach § 110 Abs. 9 Satz 2 TKG, an der festgehalten werden soll. Die zu erwartenden Investitionskosten werden voraussichtlich nicht so erheblich sein, wie im Zuge der Beratungen der Richtlinie zunächst zu befürchten war, insbesondere da besonders kostenträchtige Speicherungsvorgaben auf europäischer Ebene verhindert werden konnten (z. B. Speicherung „erfolgloser Anrufversuche“, auch wenn diese von den Diensteanbietern bisher nicht gespeichert oder protokolliert werden; Speicherung von Standortdaten auch während und am Ende von Mobilfunkverbindungen). Zudem werden auch in vergleichbaren Fallgestaltungen etwa erforderliche Investitionsaufwendungen zur Erfüllung von Speicherungspflichten (etwa nach § 9 des Geldwäschegesetzes) nicht erstattet. Überdies wäre eine Entschädigung mit erheblichen praktischen Problemen verbunden, weil kaum zuverlässig festzustellen sein wird, in welcher Höhe ein konkreter Investitionsbedarf allein durch die Einführung der Speicherungspflichten ausgelöst wurde, zumal gerade die Telekommunikationsbranche von einer besonders dynamischen Entwicklung auch der Anlagen- und Systemtechnik geprägt ist. Hinzu kommt, dass die Diensteanbieter für die Inanspruchnahme im Zuge hoheitlicher Ermittlungsmaßnahmen im Einzelfall nach dem Justizvergütungs- und -entschädigungsgesetz entschädigt werden.

Schließlich ist im Bundesministerium der Justiz derzeit – wie vom Deutschen Bundestag in seinem Beschluss vom 16. Februar 2006 (BT-Drs. 16/545, S. 4) gefordert – eine Überarbeitung der Vorschriften des Justizvergütungs- und -entschädigungsgesetzes (JVEG) über die Entschädigung der Diensteanbieter für die Inanspruchnahme im Zuge hoheitlicher Ermittlungsmaßnahmen in Aussicht genommen, die insbesondere auch eine Vereinfachung der Entschädigungsberechnung und -abrechnung einführen soll; auch dies dürfte die administrativen Aufwände sowohl der Diensteanbieter als auch der Bedarfsträger verringern und damit

zur Kostenvermeidung beitragen. Auch werden zurzeit zwischen den Bedarfsträgern und den Diensteanbietern – unter Einbeziehung der Bundesregierung − weitere Möglichkeiten zur Vereinheitlichung und Vereinfachung der Auskunftsverfahren diskutiert, deren Realisierung eine Reduzierung des Aufwands für die Diensteanbieter erwarten ließe und deren Entwicklung zunächst abzuwarten bleibt.

5.

Die Umsetzung der Richtlinie ist in der Ausgestaltung des vorliegenden Entwurfs verfassungsrechtlich zulässig. Die Einführung gesetzlicher Vorschriften zur obligatorischen Speicherung von Verkehrsdaten durch die Diensteanbieter greift zwar in das Fernmeldegeheimnis der Telekommunikationsnutzer nach Artikel 10 Abs. 1 GG und in die Berufsausübungsfreiheit der Anbieter der Telekommunikationsdienste nach Artikel 12 Abs. 1 GG ein. Diese Grundrechte sind jedoch nicht vorbehaltlos gewährleistet. Ihre gesetzliche Einschränkung ist zur Verfolgung vernünftiger Gemeinwohlbelange zulässig, wenn hierbei insbesondere die Grenzen der Verhältnismäßigkeit gewahrt werden, also die einschränkende gesetzliche Regelung zur Erreichung des angestrebten Zwecks geeignet und erforderlich ist und die Schwere der Einbuße an grundrechtlich geschützter Freiheit nicht außer Verhältnis zu den Gemeinwohlbelangen steht, denen die Grundrechtsbeschränkung dient.

Die gesetzliche Pflicht zur Speicherung bestimmter Verkehrsdaten durch die Diensteanbieter bezweckt insbesondere die Gewährleistung einer wirksamen Strafverfolgung und verfolgt damit einen vernünftigen Gemeinwohlbelang.

Sie ist zur Erreichung dieses Zwecks auch geeignet, da sie sicherstellt, dass die relevanten Verkehrsdaten für einen bestimmten Zeitraum für Strafverfolgungszwecke verfügbar sind, auch wenn sie von den Diensteanbietern für geschäftliche Zwecke nicht oder nicht mehr benötigt werden. Die Möglichkeit, auf vorhandene Verkehrsdaten zuzugreifen, ist für eine wirksame Strafverfolgung von großer Wichtigkeit (vgl. Seitz, Strafverfolgungsmaßnahmen im Internet, 2004, S. 147; Breyer, Die systematische Aufzeichnung und Vorhaltung von Telekommunikations-Verkehrsdaten für staatliche Zwecke in Deutschland, 2005, S. 9 f. u. passim; Zöller, in: FG für Hilger, S. 291, 304 f.; Welp, GA 2002, 535, 536 f.; Wohlers/Demko, StV 2003, 241; Wolter, in: Systematischer Kommentar zur StPO, § 100g, Rn. 5). Dies ist auch in der Rechtsprechung des Bundesverfassungsgerichts anerkannt (vgl. BVerfG, 2 BvR 2099/04 vom 2. März 2006, Absatz-Nr. 103 = BVerfGE 115, 166 ff.; BVerfGE 107, 299, 316). Die Befugnis der Strafverfolgungsbehörden, Auskunft von Diensteanbietern über ge-

speicherte Verkehrsdaten zu verlangen, hat sich in vielen Kriminalitätsbereichen als wichtiges Ermittlungsinstrument erwiesen; zur Aufdeckung komplexer Täterstrukturen, wie sie gerade für den internationalen Terrorismus und die organisierte Kriminalität kennzeichnend sind, und zur Aufklärung von mittels Telekommunikation begangenen Straftaten ist die Kenntnis von Verkehrsdaten inzwischen weithin unverzichtbar.

Die Einführung der „Vorratsdatenspeicherung“ ist auch erforderlich, da weniger eingriffsintensive Mittel nicht in gleicher Weise zur Erreichung des angestrebten Zwecks geeignet sind. Dies gilt namentlich für die als Alternative gelegentlich angeführte einzelfallbezogene Aufbewahrungsanordnung, wie sie für eine besondere Fallgestaltung bereits in § 16b Abs. 1 Satz 1 des Wertpapierhandelsgesetzes geregelt ist (so genanntes „Quick Freeze“, vgl. hierzu Artikel-29-Datenschutzgruppe, Stellungnahme 4/2005 vom 21. Oktober 2005, S. 7; Wissenschaftlicher Dienst des Deutschen Bundestages, WD 3 – 282/06, S. 12; Bäumler, DuD 2001, 348, 351; Alvaro, RDV 2005, 47, 48; Büllingen, DuD 2005, 349, 351). Die gesetzliche Regelung einer solchen Aufbewahrungsanordnung im Einzelfall, die die Diensteanbieter verpflichtet, gespeicherte Verkehrsdaten nicht zu löschen, ist nicht in gleicher Weise zur Förderung einer wirksamen Strafverfolgung geeignet (so auch Seitz, a. a. O., S. 242; Breyer, a. a. O., S. 346). Das „schnelle Einfrieren“ der benötigten Verkehrsdaten durch die Diensteanbieter „auf Zuruf“ der Strafverfolgungsbehörden geht notwendig ins Leere, wenn die relevanten Verkehrsdaten vom Diensteanbieter überhaupt nicht gespeichert oder zwischenzeitlich bereits gelöscht wurden und daher nicht gesichert werden können. Dies ist aufgrund der zunehmenden Verbreitung von Pauschaltarifen, bei denen die Diensteanbieter Verkehrsdaten für Abrechnungszwecke nicht benötigen und diese daher nach geltendem Recht grundsätzlich auch nicht speichern dürfen (vgl. LG Darmstadt, MMR 2006, 330 ff., rechtskräftig aufgrund des Beschlusses des Bundesgerichtshofs vom 26. Oktober 2006, III ZR 40/06), immer häufiger der Fall. Auch nach Einführung der gesetzlichen Voraussetzungen für kurzfristige Aufbewahrungsanordnungen im Einzelfall hinge die Wirksamkeit einer Ermittlungsmaßnahme nach § 100g StPO von dem jeweils zwischen dem Diensteanbieter und seinem Kunden vereinbarten Entgelttarif ab.

Schließlich stehen die zur Umsetzung der Richtlinie vorgesehenen Regelungen auch nicht außer Verhältnis zu der mit ihnen angestrebten Förderung einer wirksamen Strafverfolgung.

Im Rahmen der gebotenen Gesamtabwägung ist hinsichtlich des Eingriffs in das Fernmeldegeheimnis der Telekommunikationsnutzer zu berücksichtigen, dass Verkehrsdaten einen besonders schutzwürdigen Aussagegehalt haben, da sie im Einzelfall erhebliche Rückschlüsse auf das Kommunikations- und Bewegungsverhalten der Telekommunikationsnutzer

zulassen (vgl. BVerfG, 2 BvR 2099/04 vom 2. März 2006, Absatz-Nr. 92 = BVerfGE 115, 166 ff.). Hinzu kommt, dass die Datenspeicherung unabhängig von einem im Einzelfall bestehenden Tatverdacht erfolgt und eine unbestimmte Vielzahl von Personen erfasst. Hinsichtlich des Eingriffs in die Berufsausübungsfreiheit der betroffenen Diensteanbieter ist festzustellen, dass die Umsetzung der gesetzlichen Speicherungspflichten voraussichtlich mit Belastungen verbunden sein wird, wenn auch seitens der Telekommunikationswirtschaft konkrete, detaillierte und nachvollziehbare, mithin für die Bundesregierung belastbare Angaben zu den tatsächlich zu erwartenden Kosten nicht vorgelegt wurden.

Auf der anderen Seite kommt der Gewährleistung einer wirksamen Strafverfolgung eine hohe Bedeutung zu. Das Bundesverfassungsgericht hat wiederholt die unabweisbaren Bedürfnisse einer wirksamen Strafverfolgung hervorgehoben, das öffentliche Interesse an einer möglichst vollständigen Wahrheitsermittlung im Strafverfahren betont und die wirksame Aufklärung gerade schwerer Straftaten als einen wesentlichen Auftrag eines rechtsstaatlichen Gemeinwesens bezeichnet (vgl. nur BVerfG, 2 BvR 2099/04 vom 2. März 2006, Absatz-Nr. 98 = BVerfGE 115, 166 ff.; BVerfGE 100, 313, 388 f.; 107, 299, 316). Zur Erfüllung dieses Auftrags leistet die gesicherte Verfügbarkeit von Verkehrsdaten für Strafverfolgungszwecke einen wichtigen, in einigen Deliktsbereichen (insbesondere zur Aufklärung komplexer Täterstrukturen und bei mittels Telekommunikation begangenen Straftaten) unverzichtbaren Beitrag.

Im Rahmen der Gesamtabwägung ist auch erheblich, dass bei den Verhandlungen auf europäischer Ebene eine Begrenzung der Speicherungspflichten auf das aus Strafverfolgungssicht unverzichtbare Minimum erreicht und zunächst geforderte weitergehende Regelungen insbesondere im Bereich des Internets und der Mobilfunktelefonie verhindert werden konnten und dass die innerstaatlich vorgesehenen Speicherungspflichten lediglich der Umsetzung dieser Mindestvorgaben dienen. Speziell im Hinblick auf den Eingriff in das Fernmeldegeheimnis ist überdies zu berücksichtigen, dass die Speicherung automatisch, also ohne eine Kenntnisnahme durch Personen erfolgt und dass der Zugriff auf die gespeicherten Verkehrsdaten gemäß § 100g Abs. 2 Satz 1 i. V. m. § 100b Abs. 1 StPO-E weiterhin grundsätzlich einer gerichtlichen Anordnung bedarf. Schließlich ist ein Zugriff der Strafverfolgungsbehörden auf die nach Maßgabe von § 113a TKG-E gespeicherten Verkehrsdaten nur zulässig zur Verfolgung von Straftaten von auch im Einzelfall erheblicher Bedeutung sowie zur Verfolgung von mittels Telekommunikation begangenen Straftaten, wenn die Erforschung des Sachverhalts auf andere Weise ausgeschlossen wäre und die Datenerhebung in einem angemessenen Verhältnis zur Bedeutung der Sache steht.

Der Einführung von Speicherungspflichten für Verkehrsdaten steht auch die verfassungsgerichtliche Rechtsprechung nicht entgegen (vgl. Seitz, a. a. O., S. 243 f.). Soweit in Entscheidungen des Bundesverfassungsgerichts ein „striktes Verbot der Sammlung personenbezogener Daten auf Vorrat“ betont wird (zuletzt BVerfG, 1 BvR 518/02 vom 4. April 2006, Absatz-Nr. 105 = BVerfGE 115, 320 ff.), bezieht sich dies auf die Sammlung personenbezogener Daten „auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken“ (vgl. BVerfGE 65, 1, 46; 100, 313, 360). Eine solche Datensammlung zu unbestimmten oder noch nicht bestimmbaren Zwecken ist nicht Gegenstand des vorliegenden Entwurfs. Die Einführung von Speicherungspflichten für Verkehrsdaten soll sicherstellen, dass diese Daten für Zwecke der Strafverfolgung zur Verfügung stehen.

VII.

Zusammenfassend lassen sich die Eckpunkte des Entwurfs folgendermaßen kennzeichnen. Der Entwurf bezweckt die

- Harmonisierung und Stärkung des Rechtsschutzes der von verdeckten Ermittlungsmaßnahmen Betroffenen,

- Harmonisierung und Ergänzung der Regelungen zur Verwendung von aus solchen Maßnahmen erlangten personenbezogenen Daten,

- Klarstellung der Grenzen der Wahrheitserforschung und Hervorhebung der besonderen Schutzwürdigkeit von Berufsgeheimnisträgern,

- Behebung von Unsicherheiten, die in der Rechtsanwendung der verdeckten Ermittlungsmaßnahmen aufgetreten sind,

- Umsetzung der Vorgaben des Übereinkommens des Europarats über Computerkriminalität und der EU-Richtlinie zur „Vorratsspeicherung“ von Verkehrsdaten.

Insgesamt soll durch die Neuregelung der von der Praxis kritisierten (vgl. Albrecht/Dorsch/Krüpe, a. a. O., S. 461) Regelungsfülle und unklaren Terminologie des betroffenen Rechtsbereichs unter grundsätzlicher Wahrung seiner bisherigen Systematik begegnet werden.

Aus Anlass der Einbeziehung von Steuerstraftaten in den Anlassstraftatenkatalog des § 100a Abs. 2 StPO-E beseitigt der Entwurf mit den in Artikel 3 vorgesehenen Änderungen

der Abgabenordnung zudem Wertungswidersprüche und Problemkonstellationen in den §§ 370 ff. AO.

VIII.

Die Gesetzgebungskompetenz des Bundes folgt im Wesentlichen aus Artikel 74 Abs. 1 Nr. 1 GG (Strafrecht, gerichtliches Verfahren, Gerichtsverfassung) sowie Artikel 73 Abs. 1 Nr. 7 GG (Telekommunikation).

IX.

1.

Der Entwurf berücksichtigt die Vorschrift des § 1 Abs. 2 Bundesgleichstellungsgesetz, der zufolge die Rechts- und Verwaltungsvorschriften des Bundes die Gleichstellung von Frauen und Männern auch sprachlich zum Ausdruck bringen sollen. Eine geschlechterneutrale Sprache wird überall verwendet, wo nicht die Beibehaltung legal definierter Begriffe (vgl. § 157 StPO: „der Beschuldigte“, „der Angeklagte“; § 76 Abs. 1 GVG: „der Vorsitzende“, § 19 BDSG: „der Betroffene“) erforderlich ist.

2.

Der Entwurf ist mit europäischem Recht vereinbar. Insbesondere trägt er den Umsetzungsverpflichtungen aus der Richtlinie 2006/24/EG Rechnung.

X.

Von dem Entwurf sind folgende kostenrelevante Auswirkungen zu erwarten:

1.

Kostenrelevante Auswirkungen für
Strafverfolgungsbehörden und Gerichte in Bund und Ländern

Für die Strafverfolgungsbehörden und Gerichte des Bundes und der Länder ergibt sich im Wesentlichen folgender Mehr- bzw. Minderaufwand:

- Die Regelungen in § 53b StPO-E lassen – im Hinblick darauf, dass Berufsgeheimnisträger schon bislang nur in Einzelfällen von Ermittlungsmaßnahmen betroffenen werden – keinen kostenrelevanten Mehr- oder Minderaufwand erwarten.

- Die Änderungen zur Telekommunikationsüberwachung in den §§ 100a, 100b StPO-E, insbesondere die Beschränkung auf auch im Einzelfall schwere Straftaten unter maßvoller Modifizierung des Anlassstraftatenkatalogs, lässt einen noch zielgerichteteren Einsatz dieses Ermittlungsinstruments und damit jedenfalls keinen Mehraufwand erwarten. Die Einbeziehung von Straftatbeständen nach der Abgabenordnung trägt darüber hinaus zur Sicherung von Steuereinnahmen bei und hat damit eine – nicht näher quantifizierbare – positive Auswirkung auf die Fiskalhaushalte. Die in § 100b Abs. 5 und 6 vorgesehenen statistischen Erhebungen schreiben im Wesentlichen die derzeitige freiwillige Handhabung fest und lassen damit keine erheblichen zusätzlichen Belastungen erwarten.

- Die Möglichkeiten zur Erhebung von Verkehrsdaten nach § 100g StPO(-E) wird durch die in Artikel 2 erfolgende Umsetzung der Richtlinie zur „Vorratsspeicherung“ erweitert. Dies führt voraussichtlich zu vermehrten, der Entschädigungspflicht nach § 23 JVEG unterliegenden Auskunftsersuchen der Strafverfolgungsbehörden an Telekommunikationsunternehmen nach § 100g StPO. In welchem Umfang sich hierdurch die Summe der aus den Haushalten von Bund und Ländern zu erbringenden Entschädigungszahlungen erhöhen wird, lässt sich nicht verlässlich schätzen, weil nicht bekannt ist, in wie vielen Fällen derzeit von entsprechenden Ersuchen in Ermangelung einer die Erfolgsaussicht der Anfrage begründenden Speicherungspflicht abgesehen wird. Bei angenommenen zusätzlichen 10.000 Auskunftsersuchen pro Jahr ergibt sich bei dem von § 23 JVEG vorgegebenen Stundensatz von maximal 17 Euro und einer angenommenen Bearbeitungszeit von einer Stunde pro Auskunftsersuchen ein Ausgabevolumen von 170.000 Euro pro Jahr, das im Hinblick auf die primäre Zuständigkeit der Länder für die Strafverfolgung zum ganz überwiegenden Teil aus den Länderhaushalten zu finanzieren sein wird. Dem stehen erhebliche Effektivitätsgewinne gegenüber, weil aufgrund der in § 113a TKG-E enthaltenen Verpflichtung zur Speicherung von Verkehrsdaten ergebnislos verlaufende Auskunftsersuchen abnehmen und durch erfolgreiche

Auskunftsersuchen alternativ in Betracht zu ziehende – meist aufwändigere – Ermittlungen vermieden werden können.

- Ein Mehraufwand ergibt sich aus den in § 100g Abs. 4 StPO-E vorgesehenen statistischen Erhebungen. Dieser – nicht näher quantifizierbare – Mehraufwand lässt sich aufgrund der Vorgaben aus Artikel 10 der RL 2006/24/EG nicht vermeiden.

- Die in § 101 Abs. 3 StPO-E geregelten Kennzeichnungspflichten sind aufgrund verfassungsrechtlicher Vorgaben nicht zu vermeiden und können durch einfache Kennzeichnungsvermerke (z. B. Stempelaufdrucke) erfüllt werden. Oftmals bedarf es auch keiner besonderen Kennzeichnung, weil bereits aufgrund der derzeit geübten Praxis aus den zu kennzeichnenden Daten bzw. Unterlagen hervorgeht, die vielfach schon jetzt in Sonderheften geführt werden, dass sie aus Maßnahmen nach § 101 Abs. 1 StPO-E herrühren. Dies wird etwa bei Auswertungsprotokollen aus Telekommunikationsüberwachungsmaßnahmen regelmäßig der Fall sein.

- Die in § 101 Abs. 4 bis 8 StPO-E in Umsetzung der verfassungsgerichtlichen Rechtsprechung geregelten Benachrichtigungspflichten sind – im Vergleich zur geltenden Rechtslage – aufwandsneutral zu erfüllen:

  Der Kreis von Maßnahmen, die Benachrichtigungspflichten entstehen lassen, wird zwar einerseits erweitert (Ausdehnung der Benachrichtigungspflichten auf Maßnahmen nach den §§ 100h, 100i, 110a, 163e StPO-E), andererseits aber auch eingeschränkt (Wegfall der Benachrichtigungspflicht bei Maßnahmen nach § 81e StPO). Nach dem geltendem § 101 Abs. 1 StPO sind von den dort in Bezug genommenen Maßnahmen indessen – alle – Beteiligten zu unterrichten. Dies sind beispielsweise im Falle einer Telekommunikationsüberwachung auch all jene Personen, mit denen der überwachte Beschuldigte telekommuniziert hat; ob die gewonnenen Erkenntnisse verwertet worden sind, ist unerheblich (vgl. Meyer-Goßner, a. a. O., § 101 Rn. 2). Denn der Schutzzweck der Benachrichtigungspflichten besteht darin, den Beteiligten, deren vorherige Anhörung den Zweck der Maßnahme in aller Regel gefährden, wenn nicht vereiteln würde (§ 33 Abs. 4 Satz 1 StPO), nachträglich rechtliches Gehör zu gewähren, um ihnen die Möglichkeit zu eröffnen, sich gegen diesen Eingriff zur Wehr zu setzen (BGHSt 36, 305, 311 m. w. N.). Die Neuregelung greift deshalb diese Verpflichtung zur Benachrichtigung jedes Beteiligten in § 101 Abs. 4 Satz 1 Nr. 3 StPO-E zwar auf, regelt aber zugleich – auch für die sonstigen in § 101 Abs. 4 Satz 1 StPO-E aufgeführten verdeckten Ermittlungsmaßnahmen – in § 101 Abs. 4 Satz 3 bis 5 StPO-E innerhalb des verfassungsrechtlich Zulässigen erstmals weitreichende und damit für die Praxis deutliche Erleichterungen mit sich bringende Ausnahmen hiervon, so dass sich – im Ver-

gleich zur bisherigen Gesetzeslage – wenn nicht ein erheblicher Minderaufwand, so doch zumindest eine neutrale Aufwandslage ergibt.

Wenn demgegenüber seitens der Praxis darauf hingewiesen wird, die Neuregelung in § 101 Abs. 4 StPO-E bedinge einen erheblichen zusätzlichen Benachrichtigungsaufwand, insbesondere bei Telekommunikationsüberwachungsmaßnahmen, so beruht diese Einschätzung offenbar auf dem auch in der Untersuchung von Albrecht/Dorsch/Krüpe bestätigten Befund, wonach die Praxis insoweit den bestehenden Benachrichtigungspflichten nicht immer in der vom geltenden Recht geforderten Weise Rechnung trägt. Ein etwaiger künftiger Mehraufwand wird damit aber nicht aus der gesetzlichen Neuregelung resultieren, sondern aus einem offenbar nicht selten unzulänglichen Vollzug der bereits bestehenden gesetzlichen Vorgaben.

- Der in § 101 Abs. 9 StPO-E vorgesehene nachträgliche Rechtsschutz schreibt die verfassungsgerichtliche Rechtsprechung fest, wonach dem durch eine eingriffsintensive verdeckte Ermittlungsmaßnahme Betroffenen im Wege des nachträgliches Rechtschutzes rechtliches Gehör zu gewähren ist. Es handelt sich damit bei der Neuregelung um eine gesetzliche Klarstellung, die der insoweit immer wieder anzutreffenden Unsicherheiten in der instanzgerichtlichen Rechtsprechung zur Frage des Rechtsschutzbedürfnisses entgegenwirkt. Die Erfahrungen mit der seit 1998 bestehenden Regelung zum nachträglichen Rechtsschutz bei einer akustischen Wohnraumüberwachung lassen im Übrigen erwarten, dass die Betroffenen von dieser Möglichkeit nur sehr zurückhaltend Gebrauch machen werden. Bislang ist aus der Praxis kein Fall berichtet worden, in dem ein von einer akustischen Wohnraumüberwachung Betroffener die nachträgliche Rechtsschutzmöglichkeit ergriffen hat.

- Die in § 110 Abs. 3 StPO-E vorgesehene Möglichkeit einer offenen Online-Durchsuchung effektiviert die Ermittlungen und erspart damit nicht näher quantifizierbaren Mehraufwand für alternativ in Betracht zu ziehende – regelmäßig aufwändigere – alternative Ermittlungen.

- Die in § 162 Abs. 1 StPO-E vorgesehene Konzentration der örtlichen Zuständigkeit des Ermittlungsgerichts fördert dessen Spezialisierung, trägt damit zur effektiveren Aufgabenerfüllung bei und bedingt somit einen nicht näher quantifizierbaren Minderaufwand.

In der Gesamtbetrachtung ist zu erwarten, dass die einzelnen Mehr- und Minderaufwände sich ausgleichen, so dass die Neufassung der Regelungen zu verdeckten Ermittlungsmaß-

nahmen in der Strafprozessordnung von den Strafverfolgungsbehörden und Gerichten voraussichtlich insgesamt aufwandsneutral zu erfüllen sein wird.

2.

Kostenrelevante Auswirkungen bei anderen öffentlichen Stellen in Bund und Ländern

Durch die Änderung der Vorschriften des Telekommunikationsgesetzes in Artikel 2 entsteht bei der Bundesnetzagentur sich in Sachinvestitionen und Personalkosten aufgliedernder zusätzlicher Vollzugsaufwand, den das Bundesministerium für Wirtschaft und Technologie wie folgt veranschlagt: Im Bereich des Automatisierten Auskunftsverfahrens nach § 112 TKG werden für die Erweiterung des Systems Investitionskosten in Höhe von einer Million Euro erwartet. Gleichzeitig ist für die qualifizierte Planung und Fortschreibung des Projektes ein personeller Bedarf von zwei Kräften des gehobenen Dienstes und zwei Kräften des mittleren Dienstes zu erwarten. Dies wird durch die Erweiterung der Abfragemöglichkeiten um E-Mail-Adressen und die damit verbundene Verfünffachung der anzuschließenden Unternehmen verursacht. Schließlich entsteht durch die Verpflichtung zur Verkehrsdatenspeicherung ein erhöhter Kontrollaufwand im Rahmen der Aufsicht nach § 115 TKG einschließlich der Anwendung der neuen Bußgeldtatbestände, der zwei Stellen des höheren Dienstes mit juristischer Vorbildung sowie zwei Kräfte des gehobenen Dienstes erforderlich macht. Damit ist ein Personalkostenaufwand in Höhe von insgesamt rd. 640.000 Euro pro Jahr zu erwarten.

Bei anderen öffentlichen Stellen werden sich nicht näher bezifferbare unmittelbare und mittelbare Einsparungen dadurch ergeben, dass die Ermittlungsmöglichkeiten im Strafverfahren effektiviert und damit die hohe gesamtgesellschaftliche Schäden verursachende Kriminalität besser bekämpft werden kann.

3.

Kostenrelevante Auswirkungen auf die Kommunen

Auswirkungen auf die Haushalte der Kommunen sind nicht zu erwarten.

4.

Haushaltsausgaben ohne Vollzugsaufwand

Haushaltsausgaben ohne Vollzugsaufwand sind nicht zu erwarten.

5.

Kostenrelevante Auswirkungen für die Wirtschaft

Für die von der Speicherungspflicht für Verkehrsdaten betroffenen Unternehmen entsteht durch die Erfüllung der in den §§ 111 und 113a TKG-E vorgesehenen Speicherungspflicht zusätzlicher Aufwand. In welchem bezifferbaren Umfang dies der Fall sein wird, konnte trotz mehrfach bei der Telekommunikationswirtschaft angeforderten Stellungnahmen und insoweit intensiv geführten Diskussionen nicht geklärt werden. In plausibler Weise dargelegt wurde im Wesentlichen, dass der Zusatzaufwand in Abhängigkeit von der bisherigen – sehr unterschiedlichen und dem Wandel unterzogenen – Handhabung bei der Speicherung der Daten und der Unternehmensgröße verschieden groß sein wird und von einigen Tausend bis zu mehreren Hunderttausend Euro reichen kann. Konkrete und im Einzelnen nachvollziehbare Berechnungen hat die Telekommunikationswirtschaft indessen nicht vorgelegt (zur Problematik nicht nachvollziehbarer Kostenangaben im Zusammenhang mit notwendigen Umstellungen bei der Speicherung bzw. Löschung von Verkehrsdaten bei Pauschaltarifen vgl. auch den Beschluss des Bundesgerichtshofs vom 26. Oktober 2006, III ZR 40/06, S. 4 ff.). Zum Teil wird die erforderliche Umstellung in der von stetigem technischen Wandel gekennzeichneten Telekommunikationswirtschaft im Rahmen von ohnehin regelmäßig anstehenden technischen Anpassungen erfolgen und damit den allein durch die Speicherungspflicht ausgelösten Aufwand reduzieren können.

Eine belastbare nähere Quantifizierung des insgesamt für die Telekommunikationswirtschaft entstehenden zusätzlichen Aufwandes ist – auch im Wege einer Schätzung – angesichts des dargestellten Befundes nicht möglich.

Bei kleineren Unternehmen wird von der in § 3 Abs. 2 Nr. 5 TKÜV-E vorgesehenen Anhebung der so genannte Marginaliengrenze von 1 000 auf 10 000 Teilnehmer bzw. sonstigen Nutzungsberechtigte eine deutliche Entlastung ausgehen. Zudem werden die betroffenen Unternehmen in gewissem Maße dadurch entlastet, dass die in der Praxis aufwändig umzusetzende Zielwahlsuche (§ 100g Abs. 2 StPO) aufgrund der Regelungen über die Speicherungspflichten, die auch ankommende Anrufe einbeziehen, weitgehend entbehrlich wird und

die bislang in § 110 Abs. 8 TKG vorgesehene Verpflichtung der Unternehmen zur Erhebung und Übermittlung statistischer Angaben über Anordnungen nach den §§ 100a, 100b StPO aufgehoben wird, weil diese Aufgaben künftig aufgrund der Regelungen in § 100b Abs. 5 und 6 StPO-E von öffentlichen Stellen (Strafverfolgungsbehörden) wahrzunehmen sind.

Während der Aufwand für die Beauskunftung von Verkehrsdaten nach § 23 Abs. 1 Nr. 2 JVEG entschädigt wird, sieht der Entwurf für die zur Erfüllung der Speicherungspflichten erforderlichen Investitionen und ggf. gesteigerten Betriebskosten keine Kostenerstattung vor. Es ist daher zu erwarten, dass die betroffenen Unternehmen diese Kosten, die durch die vorgenannten Entlastungen voraussichtlich nicht kompensiert werden, grundsätzlich bei ihrer Preisgestaltung einkalkulieren und damit gegebenenfalls auf ihre Kunden abwälzen werden, soweit der EU-weit von der Speicherungspflicht betroffene Telekommunikationsmarkt dies zulässt. Das Verbraucherpreisniveau im Bereich der Telekommunikationsdienstleistungen kann daher geringfügig steigen.

Darüber hinaus entstehen für die Wirtschaft, insbesondere mittelständische Unternehmen, keine Kosten. Weitere Auswirkungen auf Einzelpreise, das allgemeine Preisniveau und insbesondere das Verbraucherpreisniveau sind damit nicht zu erwarten.

6.

Künftige Neuregelung der Entschädigungspflichten

Der Entwurf enthält keine Neuregelungen zur Entschädigung der Telekommunikationsunternehmen. Eine solche Neuregelung und die Frage ihres Standortes werden Gegenstand eines besonderen Gesetzgebungsverfahrens, das parallel vorbereitet wird und mit hoher Priorität durchgeführt werden sollte. Der entsprechende Gesetzentwurf wird sobald wie möglich dem Parlament zur Beschlussfassung vorgelegt.

B.
Zu den einzelnen Vorschriften

Zu Artikel 1 (Änderung der Strafprozessordnung)

Zu Nummer 1 (§ 53b StPO-E)

Die neu eingefügte Vorschrift führt ein harmonisiertes System zur Berücksichtigung der von den Zeugnisverweigerungsrechten der Berufsgeheimnisträger (§§ 53, 53a StPO) geschützten Interessen außerhalb der Vernehmungssituation ein. Zur grundsätzlichen Konzeption wird auf die obigen Ausführungen im Allgemeinen Teil der Begründung (dort unter A. III. 3.) Bezug genommen

Zu Absatz 1

Absatz 1 begründet – flankiert durch Löschungs- und Dokumentationspflichten – ein Beweiserhebungs- und -verwertungsverbot für Erkenntnisse, die vom Zeugnisverweigerungsrecht der Geistlichen (in ihrer Eigenschaft als Seelsorger), Verteidiger und Abgeordneten (§ 53 Abs. 1 Satz 1 Nr. 1, 2 und 4 StPO) umfasst sind. Die Regelung übernimmt damit die vom Gesetzgeber bereits in § 100h Abs. 2 StPO getroffene Wertung, diese Berufsgruppen im Rahmen des ihnen zukommenden Zeugnisverweigerungsrechts in besonderer Weise von staatlichen Ermittlungsmaßnahmen freizustellen. Zugleich wird damit die bisherige Spezialregelung in § 100h Abs. 2 StPO entbehrlich. Der damit einhergehende Schutz der Vertraulichkeit der Kommunikation mit diesen Berufsgeheimnisträgern ist – vorbehaltlich der Verstrickungsregelung in Absatz 4, die auch in § 97 Abs. 2 Satz 3, § 100c Abs. 6 Satz 3 und § 100h Abs. 2 Satz 2 enthalten ist – absolut ausgestaltet, hängt mithin nicht von Erwägungen zur Verhältnismäßigkeit im Einzelfall ab. Die Kommunikation mit einem Verteidiger, einem Seelsorger oder einem Abgeordneten darf demnach, soweit die Genannten im Wirkungsbereich ihres jeweiligen Zeugnisverweigerungsrechtes tätig werden, durch Ermittlungsmaßnahmen gleich welcher Art nicht zielgerichtet beeinträchtigt werden. Dieser absolute Schutz ist verfassungsrechtlich geboten:

Der Gewährleistung ausreichender Verteidigungsrechte kommt für die Rechtsstaatlichkeit des Strafverfahrens eine wichtige Bedeutung zu. Die Möglichkeit, den Beistand eines Strafverteidigers in Anspruch zu nehmen, gewährleistet eine sachgerechte Wahrung der Rechte des Beschuldigten und trägt dazu bei, dass dieser nicht zum bloßen Objekt des Strafverfahrens wird. In diesem Sinne kommt dem Gespräch mit dem Verteidiger eine wichtige Funktion

zur Wahrung der Menschenwürde zu (BVerfGE 109, 279, 322). Der Kontakt mit dem Verteidiger darf daher nach gefestigter Rechtsprechung nicht in einer Weise beeinträchtigt werden, die die Verteidigungsmöglichkeiten des Beschuldigten schmälert; dasselbe gilt, soweit sich der Beschuldigte selbst Unterlagen zu seiner Verteidigung anfertigt (arg. ex § 148 StPO, vgl. BVerfG, 2 BvR 2248/00 vom 30. Januar 2002, NJW 2002, 1410 f.; BGHSt 38, 372 ff.; 42, 15, 18 ff.; 42, 170 ff.; 44, 46, 48 ff.; BGHR StPO § 97 Verteidigungsunterlagen 1, 2; BGH, 1 BJs 6/71, StB 34/73 vom 13. August 1973, NJW 1973, 2035).

Gleiches gilt für Geistliche in ihrer Eigenschaft als Seelsorger. Das Zwiegespräch mit dem Seelsorger ist dem Kernbereich privater Lebensgestaltung zuzurechnen, der dem staatlichen Zugriff schlechthin entzogen ist, und bedarf daher umfassenden Schutzes vor staatlicher Kenntnisnahme (BVerfGE 109, 279, 322).

Das Zeugnisverweigerungsrecht des Abgeordneten und das damit korrespondierende Beschlagnahmeverbot ist bereits in Artikel 47 GG sowie den entsprechenden Regelungen der Landesverfassungen (z. B. Artikel 49 Abs. 1 VerfNW) enthalten und schützt das mandatsbezogene Vertrauensverhältnis zwischen dem Abgeordneten und Dritten. Dieser bereits verfassungsrechtlich unabhängig von Verhältnismäßigkeitserwägungen im Einzelfall vorgegebene Schutz bezweckt eine Stärkung des freien Mandats und zugleich der ungestörten parlamentarischen Arbeit sowie daraus folgend der Funktionsfähigkeit der Volksvertretung. Diesem Schutz dienen auch die Immunitätsregelungen in den Verfassungen des Bundes und der Länder (vgl. z. B. Artikel 46 GG). Es erscheint sachgerecht, die bereits bestehenden – letztlich deklaratorischen – einfachgesetzlichen Regelungen in § 53 Abs. 1 Satz 1 Nr. 4 und § 97 Abs. 3 StPO zum Zeugnisverweigerungsrecht und zum Beschlagnahmeverbot bei Abgeordneten durch das in § 53b Abs. 1 StPO-E enthaltene umfassende Erhebungs- und Verwertungsverbot zu ergänzen und damit das einem Abgeordneten Anvertraute einem umfassenden Schutz zu unterstellen (so schon auf der Grundlage des geltenden Rechts im Hinblick auf die Telekommunikationsüberwachung Rudolphi, in: Systematischer Kommentar zur StPO, § 100a, Rn. 20).

Satz 1 regelt daher, dass Ermittlungsmaßnahmen unzulässig sind, wenn sie sich gegen einen Verteidiger, Geistlichen oder Abgeordneten richten und dadurch voraussichtlich Erkenntnisse erbringen würden, über die diese Personen das Zeugnis verweigern dürften. Maßnahmen, die sich gegen andere Personen – etwa einen Beschuldigten oder einen Dritten – richten, bleiben dagegen zulässig, und zwar auch dann, wenn nicht ausgeschlossen werden kann oder gar zu erwarten ist, dass möglicherweise auch die Kommunikation mit den

vorgenannten Berufsgeheimnisträgern über vom Zeugnisverweigerungsrecht umfasste Inhalte betroffen sein wird.

Der letztgenannten Konstellation einer zufälligen Betroffenheit auch des Berufsgeheimnisträgers begegnet die Neuregelung durch das in Satz 5 durch die dortige Bezugnahme auf Satz 2 enthaltene Verbot der Verwertung von Erkenntnissen, die von dem Berufsgeheimnisträger erlangt wurden und über die dieser das Zeugnis verweigern dürfte. Aus diesem Verwertungsverbot kann sich in besonderen Einzelfällen unter Anwendung des Grundsatzes der Verhältnismäßigkeit die Verpflichtung ergeben, die Maßnahme gegen einen Dritten zu unterbrechen, so wenn es sich etwa um eine ausnahmsweise in Echtzeit erfolgende Telekommunikationsüberwachung handelt und dabei ein Gespräch etwa als Verteidigergespräch erkannt wird. In diesem Fall dürfen keine Erkenntnisse erhoben werden, die nach dem in Satz 2 enthaltenen Verwertungsverbot nicht verwertet werden dürften. Eine Pflicht zur Echtzeiterhebung ergibt sich daraus indessen nicht und wäre auch nicht praktikabel (s. u. Begründung zu § 100a Abs. 4 StPO-E). Dieses Verwertungsverbot gewährleistet die Vertraulichkeit der Kommunikation mit den genannten Berufsgeheimnisträgern im Rahmen der ihnen zustehenden Zeugnisverweigerungsrechte. Zugleich sichert es die Einhaltung des Erhebungsverbots nach Satz 1. Da aus einem Erhebungsverbot nicht notwendig ein Verwertungsverbot folgt, dieses vielmehr eine bewusste Selbstbeschränkung des Staates bei der Ermittlung der Wahrheit in Strafverfahren bedeutet und die Findung einer gerechten Entscheidung durchaus erheblich beeinträchtigen kann, war das Verwertungsverbot auch ausdrücklich im Gesetzestext zu verankern.

Das Verwertungsverbot – wie auch die Vorschrift des § 53b StPO-E insgesamt – gilt selbstverständlich nicht für die Vernehmung des Berufsgeheimnisträgers als Zeuge. In diesem Fall greift vielmehr die Regelung des § 53 StPO (Recht zur Zeugnisverweigerung) mitsamt den dort in Absatz 2 enthaltenen Ausnahmen unmittelbar ein.

Das Verwertungsverbot nach Satz 2 wird flankiert durch die in Satz 3 enthaltene Verpflichtung, durch einen unzulässigen Eingriff erlangte Erkenntnisse unverzüglich zu löschen. Damit wird einer etwaigen Perpetuierung der Verletzung des Erhebungsverbots nach Satz 1 vorgebeugt und die Einhaltung des Verwertungsverbots nach Satz 2 abgesichert. Zur Frage, wem die Löschungspflicht obliegt, wird auf die Erläuterungen zu § 100a Abs. 4 Satz 3 StPO-E Bezug genommen.

Nach Satz 4 ist die Tatsache der Erlangung unter von Erkenntnissen, die unter das Erhebungsverbot nach Satz 1 fallen, sowie der Löschung von Aufzeichnungen über solche Er-

kenntnisse aktenkundig zu machen. Dies sichert zum einen die Einhaltung der Löschungspflicht, dient aber vor allem der späteren Nachvollziehbarkeit im Rahmen etwaiger Rechtsschutzbegehren der betroffenen Personen.

Nach Satz 5 gelten das Verwertungsverbot nach Satz 2, das Löschungsgebot nach Satz 3 und die Pflicht zur Dokumentation nach Satz 4 entsprechend für den Fall, dass durch eine Ermittlungsmaßnahme, die sich nicht gegen einen in § 53 Abs. 1 Satz 1 Nr. 1, 2 und 4 genannten Berufsgeheimnisträger richtet, gleichwohl Erkenntnisse von diesem Berufsgeheimnisträger erlangt wurden, über die dieser das Zeugnis verweigern dürfte, vgl. hierzu die obigen Erläuterungen im Anschluss an die Darlegungen zu Satz 1.

Erwogen wurde ferner eine Regelung nach dem Vorbild des § 100c Abs. 7 StPO, wonach bei Zweifeln darüber, ob nicht verwertbare Erkenntnisse erlangt wurden, unverzüglich eine Entscheidung des Gerichts über die Verwertbarkeit herbeizuführen ist. Aus der Praxis wurde indessen darauf hingewiesen, dass es der damit intendierten Hilfestellung bei der Bestimmung der Reichweite der Zeugnisverweigerungsrechte nach § 53 StPO in Anbetracht der jahrzehntelangen Erfahrung bei der Anwendung dieser Regelungen nicht bedarf. Darüber hinaus sprechen auch erhebliche systematische Gesichtspunkte dagegen, bereits im Ermittlungsverfahren abschließende Entscheidungen zur Verwertbarkeit gewonnener Erkenntnisse zu treffen. Denn die Beurteilung der Verwertbarkeit obliegt nach dem deutschen Strafprozessrecht dem – im Stadium des Ermittlungsverfahrens oftmals noch nicht bestimmbaren – erkennenden Gericht, dessen Entscheidung zudem der ober- bzw. höchstrichterlichen Kontrolle unterliegt. Dadurch kann die im Interesse der Rechtssicherheit wünschenswerte einheitliche Auslegung und Anwendung der Regelungen am besten gewährleistet werden.

Zu Absatz 2

Absatz 2 enthält ein relatives, an Verhältnismäßigkeitsgesichtspunkten orientiertes und in der Rechtsprechung im Rahmen der so genannten Abwägungslehre (vgl. Meyer-Goßner, a. a. O., Einl., Rn. 55a m. w. N.) im Grundsatz anerkanntes und angewandtes Erhebungs- und Verwertungsverbot, das im Einzelfall bei den von Absatz 1 nicht erfassten Berufsgeheimnisträgern, denen das Gesetz ein Zeugnisverweigerungsrecht zubilligt, zum Tragen kommen kann. Erfasst sind nach Satz 1 namentlich die in § 53 Abs. 1 Satz 1 Nr. 3 bis 3b StPO genannten Beratungs- und Heilberufe sowie die von § 53 Abs. 1 Satz 1 Nr. 5 StPO aufgeführten Medienmitarbeiter. Im Rahmen der von Satz 1 geforderten Verhältnismäßigkeitsprüfung ist das primär öffentliche – je nach Fallgestaltung (Opferinteressen) allerdings auch individuell begründete – Interesse an einer wirksamen, auf die Ermittlung der materiel-

len Wahrheit und die Findung einer gerechten Entscheidung gerichteten Strafrechtspflege gegen das öffentliche Interesse an den durch die zeugnisverweigerungsberechtigten Personen wahrgenommenen Aufgaben und das individuelle Interesse an der Geheimhaltung der einem Berufsgeheimnisträger anvertrauten oder bekannt gewordenen Tatsachen abzuwägen. Die besondere Berücksichtigung dieser Interessen im Rahmen der Verhältnismäßigkeitsprüfung rechtfertigt sich aus den folgenden Aspekten:

An der Tätigkeit der in § 53 Abs. 1 Satz 1 Nr. 3 bis 3b StPO bezeichneten Berufsgeheimnisträger aus dem Bereich der Beratungs- und Heilberufe besteht ein hohes öffentliches Interesse. Diese Tätigkeiten setzen ihrer Natur nach das Bestehen eines Vertrauensverhältnisses zwischen dem Berufsgeheimnisträger und demjenigen, der die Leistungen des Berufsgeheimnisträgers in Anspruch nimmt, voraus. Das in den Berufsgeheimnisträger gesetzte Vertrauen und das Recht auf informationelle Selbstbestimmung der mit dem Berufsgeheimnisträger in Kontakt tretenden Person sowie der Grundsatz, dass kein Beschuldigter verpflichtet ist, aktiv an seiner eigenen Überführung mitzuwirken, gebieten tendenziell Zurückhaltung bei der Erhebung von Erkenntnissen aus der vom Zeugnisverweigerungsrecht des Berufsgeheimnisträgers geschützten Sphäre. Da der Tätigkeit der Beratungs- und Heilberufe in einem sozialen Rechtsstaat auch gesellschaftlich ein hoher Wert zukommt, dürfen Maßnahmen der Strafverfolgung, die diese Tätigkeit beeinträchtigen können, nur unter strikter Wahrung der Verhältnismäßigkeit angewandt werden. Dies stellt Satz 1 sicher, indem er ausdrücklich bestimmt, dass diese Aspekte im Rahmen der stets erforderlichen Prüfung der Verhältnismäßigkeit einer Maßnahme besonders zu berücksichtigen sind. Je nach dem Ergebnis der Verhältnismäßigkeitsprüfung kann die im konkreten Fall in Aussicht genommene Maßnahme in vollem Umfang zulässig sein oder aber – soweit die Verhältnismäßigkeit ganz oder teilweise nicht gegeben wäre – sich die Notwendigkeit einer Beschränkung oder Unterlassung der Maßnahme ergeben; Letzteres stellt Satz 2 ausdrücklich klar.

Insbesondere bei Gesprächen mit einem Arzt wird sich oftmals die Notwendigkeit der Unterlassung oder Beschränkung der Ermittlungsmaßnahme ergeben; dies gilt regelmäßig dann, wenn diese auf eine Erhebung von Informationen aus solchen Gesprächen abzielt. Angaben des Arztes über Anamnese, Diagnose und therapeutische Maßnahmen und damit auch das Gespräch mit dem Arzt stehen nach ständiger Rechtsprechung des Bundesverfassungsgerichts als Ausfluss des allgemeinen Persönlichkeitsrechts unter dem Schutz des Grundgesetzes und derartige Informationen sind dem Zugriff der öffentlichen Gewalt grundsätzlich entzogen (vgl. nur BVerfG, 2 BvR 1349/05 vom 6. Juni 2006, Absatz Nr. 32, und BVerfG, 2 BvR 28/71 vom 25. Juni 1974, Absätze 24 f.). Vor diesem Hintergrund ist davon auszugehen, dass im Rahmen der in Satz 1 vorgesehenen Verhältnismäßigkeitsprüfung ein Über-

wiegen der schutzwürdigen Individualinteressen anzunehmen ist, das zur Unzulässigkeit einer Ermittlungsmaßnahme führt, wenn es um Informationen aus dem Kernbereich privater Lebensgestaltung oder zumindest um kernbereichsnahe besonders sensible Informationen geht, die in einem Arzt-Patienten-Gespräch ausgetauscht werden.

In dieses Regelungskonzept des Absatzes 2 werden auch die in § 53 Abs. 1 Satz 1 Nr. 5 StPO genannten Medienmitarbeiter eingebunden. Die Verfassung gewährt deren Tätigkeit wegen der hohen Bedeutung der Presse- und Rundfunkfreiheit einen besonderen, auch institutionellen Schutz (BVerfGE 20, 162, 175; 77, 65, 74; 107, 299, 332; 109, 279, 323 f.; BVerfG, 2 BvR 1112/81 vom 12. März 1982, NStZ 1982, 253 f.; BVerfG, 1 BvR 77/96 vom 22. August 2000, NStZ 2001, 43), der ebenfalls im Rahmen der Verhältnismäßigkeitsprüfung einer Maßnahme zu berücksichtigen ist. Ein genereller Vorrang der schutzwürdigen Interessen von Journalisten vor dem öffentlichen Strafverfolgungsinteresse lässt sich hingegen, wie das Bundesverfassungsgericht ausdrücklich festgestellt hat, verfassungsrechtlich nicht begründen (BVerfGE 107, 299, 332). Insbesondere weisen die Zeugnisverweigerungsrechte der Medienmitarbeiter keinen unmittelbaren Bezug zum Kernbereich privater Lebensgestaltung auf (BVerfGE 109, 279, 323).

Satz 3 macht die Verwertung von Erkenntnissen, die dem Zeugnisverweigerungsrecht der in Satz 1 in Bezug genommenen Berufsgruppen unterliegen, von einer Verhältnismäßigkeitsprüfung im Einzelfall abhängig. Grundsätzlich gelten damit für die Frage der Verwertbarkeit solcher Erkenntnisse dieselben Kriterien, die auch im Rahmen des Satzes 1 bei der Frage der Zulässigkeit der Erhebung entsprechender Erkenntnisse zu berücksichtigen sind. Dies führt zu einem weitgehenden Gleichlauf bei der Beurteilung der Erheb- und Verwertbarkeit. Zu beachten ist allerdings, dass diese Prüfungen oftmals zu unterschiedlichen Zeitpunkten vorzunehmen sind, so dass aufgrund zwischenzeitlicher Änderungen der Sachlage die Prüfung der Verwertbarkeit erlangter Erkenntnisse von der früheren Bewertung der Zulässigkeit der Ermittlungsmaßnahme abweichen kann. Erschien zum Beispiel ursprünglich die Erhebung von Erkenntnissen, die dem Zeugnisverweigerungsrecht unterliegen, in Anbetracht einer zunächst angenommenen schweren Straftat gerechtfertigt, ergibt sich aber im weiteren Verfahren, dass allenfalls eine Bagatelltat vorliegt, so kann sich ungeachtet des Umstandes, dass die Erhebung rechtmäßig war, ein Verwertungsverbot ergeben. Umgekehrt gilt Entsprechendes: War die Erhebung in Anbetracht der zunächst nur anzunehmenden geringen Schwere einer Straftat unverhältnismäßig, stellt sich dann aber später heraus, dass es sich um eine durchaus beachtliche Straftat handelt, so kann die Verwertung der – zunächst rechtswidrig – erhobenen Erkenntnisse gleichwohl zulässig sein. Auch kann sich aus einer zunächst unzulässigen Erhebung ein Verdacht gegen den Berufsgeheimnisträger ergeben,

in die aufzuklärende Straftat verstrickt zu sein, so dass – unter den Voraussetzungen des Absatzes 4 – die Schutzregelung des Absatzes 2 nicht mehr eingreift und die gewonnenen Erkenntnisse verwertbar sind; Entsprechendes gilt auch für Fallgestaltungen, die Absatz 1 unterfallen.

Zu beachten ist in diesem Zusammenhang, dass die Abwägungsregelung des Absatzes 2 ebenso wie die absolute Schutzregelung in Absatz 1 nur im Rahmen der Reichweite des jeweiligen Zeugnisverweigerungsrechts eingreift und sich hierdurch bedingt unterschiedliche Bewertungen hinsichtlich der Zulässigkeit der Erhebung und der Zulässigkeit der Verwertung der erhobenen Informationen ergeben können. Soweit etwa im Einzelfall nach einer zunächst unzulässigen Erhebung eine wirksame Entbindung von der Pflicht zur Verschwiegenheit erteilt wird (vgl. § 53 Abs. 2 Satz 1 StPO), besteht kein Zeugnisverweigerungsrecht und damit auch kein Ansatz mehr für ein etwaiges Verwertungsverbot.

Andererseits greift das Abwägungsgebot des Absatzes 2 aber auch dann ein, wenn vom Zeugnisverweigerungsrecht geschützte Erkenntnisse den Strafverfolgungsbehörden – etwa von der zeugnisverweigerungsberechtigten Person – freiwillig übermittelt werden. Denn das schutzwürdige Interesse etwa des Beschuldigten an der Geheimhaltung der von ihm dem zeugnisverweigerungsberechtigten Berufsgeheimnisträger anvertrauten Informationen wird hierdurch nicht beseitigt, was sich auch in der strafrechtlichen Wertung des § 203 StGB niederschlägt (vgl. Rudolphi, a. a. O., § 97, Rn. 18, 29).

Zu Absatz 3

Mit Absatz 3 werden die Regelungen der Absätze 1 und 2 nach dem Vorbild des § 97 Abs. 4 StPO auf die jeweiligen Berufshelfer erstreckt.

Zu Absatz 4

Entsprechend der Verstrickungsregelungen in § 97 Abs. 2 Satz 3 und § 100c Abs. 6 Satz 3 StPO endet der von den Absätzen 1 bis 3 gewährleistete besondere Schutz des Verhältnisses zu einem Berufsgeheimnisträger nach Absatz 4, soweit der Berufsgeheimnisträger der Beteiligung an der Tat oder der Begünstigung, Strafvereitelung oder Hehlerei verdächtig ist (zu dem weiteren Erfordernis der Einleitung eines Ermittlungsverfahrens s. u.). Denn der Schutz der betroffenen Vertrauensverhältnisse oder der Institutionen an sich soll nicht zur Begründung von Geheimbereichen führen, in denen kriminelles Verhalten einer staatlichen Aufklärung schlechthin entzogen ist.

Anders als bei den bisher bestehenden Verstrickungsregelungen fordert Absatz 4 Satz 1, dass aufgrund des Tatverdachts gegen den Berufgeheimnisträger bereits ein Ermittlungsverfahren eingeleitet worden ist. Dies trägt dem rechtspolitischen Willen Rechnung, die Ermittlungsbehörden noch stärker als bislang für die durch die Zeugnisverweigerungsrechte der Berufsgeheimnisträger geschützten Belange zu sensibilisieren und eine Umgehung der Schutzregelungen allein aufgrund bloßer Vermutungen auszuschließen. Dies verkennt nicht, dass die Einleitung grundsätzlich an keine Form gebunden ist und auch dann vorliegt, wenn die Staatsanwaltschaft Maßnahmen gegen einen Tatverdächtigen ergreift, die erkennbar darauf abzielen, gegen ihn wegen einer Straftat vorzugehen, wie etwa das Ersuchen um Vernehmung als Beschuldigter nach § 162 StPO.

Dieser Schutz wird – ebenfalls rechtspolitischem Willen Rechnung tragend – durch Satz 2 für Medienmitarbeiter bei Antrags- und Ermächtigungsdelikten zusätzlich dahingehend verstärkt, dass die Regelung des Satzes 1 bei Medienangehörigen, die in Verdacht stehen, in die Tat verstrickt zu sein, erst dann anzuwenden ist, wenn ein etwa erforderlicher Strafantrag vorliegt bzw. eine etwa erforderliche Ermächtigung erteilt ist.

Zu Absatz 5

Absatz 5 stellt klar, dass die spezielleren Regelungen des § 97 und des § 100c Abs. 6 StPO der Neuregelung in § 53b StPO-E vorgehen. Lediglich soweit diese speziellen Vorschriften keine Regelung treffen – wie etwa § 97 StPO hinsichtlich der (Nicht-)Verwertbarkeit von beschlagnahmefreien Gegenständen –, ist § 53b StPO-E ergänzend anzuwenden.

Zu Nummer 2 (§ 58a Abs. 2 StPO-E)

Es handelt sich um eine Folgeänderung zur Aufhebung des § 100b Abs. 6, dessen Regelungsgehalt (Löschung nicht mehr erforderlicher Daten) in § 101 Abs. 10 StPO-E eingestellt wird.

Zu Nummer 3 (§ 97 StPO-E)

Zu Buchstabe a (Absatz 2)

In Satz 1 wird klargestellt, dass mit der dort in Bezug genommenen „Gesundheitskarte“ die elektronische Gesundheitskarte gemeint ist.

Der neu gefasste Satz 3 übernimmt die in § 53b Abs. 4 Satz 1 StPO-E enthaltene Verstrickungsregelung. Dies führt dazu, dass auch die Verstrickungsregelung in § 97 Abs. 2 StPO nunmehr erst eingreift, wenn gegen den Berufsgeheimnisträger wegen des Verstrickungsverdachts bereits ein Ermittlungsverfahren eingeleitet worden ist.

Zu Buchstabe b (Absatz 5)

Die Ergänzung in Absatz 5 Satz 2 übernimmt die in § 53b Abs. 4 Satz 2 StPO-E für Medienangehörige enthaltene Regelung, wonach die Verstrickungsregelung bei Antrags- und Ermächtigungsdelikten erst dann eingreift, wenn der erforderliche Antrag vorliegt bzw. die Ermächtigung erteilt ist (vgl. die Erläuterungen zu § 53b Abs. 4 StPO-E).

Zu Nummer 4 (§ 98 StPO-E)

Die Ersetzung der Begriffe „Richter“ bzw. „richterlich“ durch die Wörter „Gericht“ bzw. „gerichtlich“ in den Absätzen 1 bis 3 dient der Gewährleistung einer geschlechtsneutralen Gesetzessprache und trägt damit § 1 Abs. 2 BGleiG Rechnung.

Die übrigen in Absatz 2 Satz 3 bis 6 enthaltenen Änderungen passen die dortigen Regelungen über die gerichtliche Zuständigkeit bei Entscheidungen über Beschlagnahmen an die Neufassung der allgemeinen Zuständigkeitsregelung in § 162 Abs. 1 StPO-E (Konzentration der Zuständigkeit des Ermittlungsgerichts am Sitz der Staatsanwaltschaft) an.

Zu Nummer 5 (§ 98b StPO-E)

In § 98b StPO werden Folge- und redaktionelle Änderungen vorgenommen:

- Absatz 1 und 2 werden redaktionell angepasst, um eine geschlechtsneutrale Sprache zu gewährleisten (§ 1 Abs. 2 BGleiG).

- Die Verwendungsregelung in Absatz 3 Satz 3 wird aufgehoben, weil ihr Regelungsgehalt nunmehr von § 477 Abs. 2 Satz 2 StPO-E mit erfasst wird. Eine inhaltliche Änderung ist damit nicht verbunden.

- Absatz 4 Satz 1 wird gestrichen. Die darin bislang durch die Bezugnahme auf § 163d Abs. 5 StPO enthaltene Benachrichtigungspflicht ergibt sich nunmehr aus § 101 Abs. 1, 4 ff. StPO-E. Zugleich begründet § 101 Abs. 3 StPO-E auch eine Kennzeichnungspflicht für die durch eine Maßnahme nach § 98a StPO erhobenen Daten. Durch diese Kennzeichnungspflicht, die die Beachtung der beschränkenden Verwendungsregelungen in § 477 Abs. 2 Satz 2 und 3 StPO-E sicherstellen soll, wird Vorgaben des Bundesverfassungsgerichts Rechnung getragen (vgl. BVerfGE 100, 313, 360 f.; 109, 279, 374, 379 f. sowie die Begründung zu § 101 Abs. 3 StPO-E).

Zu Nummer 6 (§ 100 StPO-E)

Die Vorschrift wird lediglich redaktionell überarbeitet und ergänzt:

- In den Absätzen 1 bis 4 wird durch die Ersetzung der Formulierung „der Richter“ durch „das Gericht“ und „richterlich“ durch „gerichtlich“ § 1 Abs. 2 BGleiG Rechnung getragen. In den Absätzen 3 und 4 wird durch die Ersetzung des Begriffs „Gegenstände“ durch „Postsendungen“ zudem eine redaktionelle Klarstellung vorgenommen.

- Als neue Absätze 5 und 6 werden Vorschriften eingestellt, die bisher in § 101 Abs. 2 und 3 StPO enthalten waren, systematisch aber den §§ 99, 100 StPO zuzuordnen sind (Weiterleitung von Postsendungen im Original oder in Abschrift). Dabei wird in dem neuen Absatz 5 zugleich eine redaktionelle Angleichung an den neuen Absatz 6 (bislang: § 101 Abs. 3 StPO) dahingehend vorgenommen, dass Postsendungen, deren Öffnung nicht angeordnet worden ist, an den vorgesehenen Empfänger (bislang: „Beteiligten“) unverzüglich weiter zu leiten sind.

Der in Teilen der rechtswissenschaftlichen Literatur vertretenen Auffassung, dass ein inhaltlicher Wertungswiderspruch zwischen den Regelungen der §§ 99, 100 und der §§ 100a, 100b StPO bestehe, der die Schaffung einer einheitlichen Vorschrift für die Überwachung von

„Fernkommunikation“ erfordere (vgl. Valerius, Zur Bedeutung des § 99 StPO im Zeitalter des Internets, in: Hilgendorf [Hrsg.], Informationsstrafrecht und Rechtsinformatik, 2004, S. 119, 143, 148 ff.; Böckenförde, a. a. O., S. 382 ff., 456 ff.; Bär, a. a. O., S. 295 ff.), wird nicht gefolgt. Es ist zwar zutreffend, dass sowohl das Brief- und Postgeheimnis als auch das Fernmeldegeheimnis einheitlich durch Artikel 10 GG geschützt sind und der herkömmliche Brief- und Postverkehr in weiten Teilen durch die modernen Möglichkeiten der Telekommunikation ersetzt wurde. Zwischen der Überwachung des Postverkehrs einerseits und der Telekommunikation andererseits bestehen aber grundlegende strukturelle Unterschiede, die eine unterschiedliche gesetzliche Regelung geboten erscheinen lassen. Die durch die Überwachung des Telekommunikationsverkehrs erlangten Daten sind aufgrund ihrer Unmittelbarkeit, Menge, Verfügbarkeit und der Gefahr von Vertiefungen des Ersteingriffs begründenden einfachen Duplizierbarkeit wesensmäßig von Postsendungen verschieden und bedürfen eines besonderen Schutzes. Eigenständige, auf die Maßnahme zugeschnittene Schutzvorkehrungen, die sich nicht ohne weiteres auf die Telekommunikationsüberwachung übertragen lassen, finden sich für die Postbeschlagnahme in § 100 Abs. 3 und 4 sowie in § 101 Abs. 2 und 3 StPO bzw. nunmehr in § 100 Abs. 5 und 6 StPO-E. Hinzu kommt, dass aufgrund des hohen und weiter zunehmenden Telekommunikationsaufkommens und der hieran anknüpfenden kontinuierlichen Steigerung der Anzahl von Telekommunikationsüberwachungsmaßnahmen einerseits und der vergleichsweise geringen Anwendungshäufigkeit der Postbeschlagnahme andererseits durch Maßnahmen der Telekommunikationsüberwachung in besonderem Maße die Bedingungen einer freien Telekommunikation (vgl. BVerfGE 100, 313, 359) gefährdet werden können.

Zu Nummer 7 (§§ 100a, 100b StPO-E)

Die in den §§ 100a, 100b StPO geregelte Telekommunikationsüberwachung stellt aufgrund ihres kriminalistischen Nutzens, ihrer Anwendungshäufigkeit und ihrer Eingriffsintensität den Ausgangspunkt der gesetzlichen Regelungen zu den verdeckten strafprozessualen Ermittlungsbefugnissen dar.

In absoluten Zahlen hat die Anzahl der Überwachungsanordnungen nach den §§ 100a, 100b StPO in den vergangenen Jahren jeweils deutlich zugenommen (vgl. die Berichte der Bundesregierung in BT-Drs. 14/2004, S. 5 ff.; 14/4863, S. 8 ff.; 14/7521, S. 5 ff.; 14/10001, S. 2 ff.; 15/2107, S. 11 ff.; 15/4011, S. 5 ff.; 15/6009, S. 7 ff.; 16/2812, S. 11 ff.). Unter Berücksichtigung des erheblichen Wachstums des deutschen Mobilfunkmarktes sowie der Tatsache, dass von Straftätern gezielt eine Vielzahl von Mobilfunkanschlüssen benutzt wird, um

Überwachungsmaßnahmen zu entgehen, dürfte diesen absoluten Zahlen allerdings nur eine begrenzte Aussagekraft zukommen. Die Untersuchung von Albecht, Dorsch und Krüpe weist nach, dass eingedenk des sprunghaft wachsenden Marktes und des geänderten Kommunikationsverhaltens tatsächlich ein Rückgang der Überwachungsdichte gemessen an der Zahl der überwachten zu der stetig steigenden Zahl der gemeldeten Anschlüsse besteht. Dies lässt den Schluss zu, dass die Zunahme der Telekommunikationsüberwachungen die Entwicklung des Telekommunikationsmarktes widerspiegelt.

Anliegen des Entwurfs ist es, einen gezielten Einsatz der Telekommunikationsüberwachung zu gewährleisten und für eine geringe „Streubreite“ dieser Maßnahme Sorge zu tragen. Die vorgenannte Untersuchung schlägt vor, den Straftatenkatalog des § 100a StPO durch materielle Kriterien zur abstrakten Kennzeichnung der Anlasstaten, bei denen eine Telekommunikationsüberwachung zulässig sein soll, zu ersetzen (vgl. Albrecht/Dorsch/Krüpe, a. a. O., S. 464 f.). Der Entwurf verzichtet darauf und behält den Anlasstatenkatalog in modifizierter Weise unter Überprüfung der Geeignetheit, Erforderlichkeit und Angemessenheit einer Telekommunikationsüberwachung bei. Eine solche Überprüfung aller eine Telekommunikationsüberwachung zulassenden Anlasstaten wird auch durch die Entscheidung des Bundesverfassungsgerichts vom 27. Juli 2005, 1 BvR 668/04 (Absatz-Nr. 152 ff., NJW 2005, 2603, 2610 f.), nahe gelegt, in der ein gesetzgeberisches Konzept verlangt wird, das bei jeder erfassten Anlasstat nachvollziehbar macht, weshalb diese in den Katalog eingestellt wurde. Dies vermag eine pauschale, allein an materiellen Kriterien orientierte Beschreibung der Anordnungsvoraussetzungen nicht zu gewährleisten. Insoweit erschien es geboten, die einzelnen Anlasstaten insbesondere auf die Aufklärbarkeit mittels einer Telekommunikationsüberwachung zu überprüfen.

Der Forderung des Bundesverfassungsgerichts (vgl. BVerfG, 1 BvR 668/04 vom 27. Juli 2005, Absatz-Nr. 160 ff., NJW 2005, 2603, 2611 f.), auch bei der Telekommunikationsüberwachung einfachgesetzliche Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung zu schaffen, wird durch § 100a Abs. 4 StPO-E Rechnung getragen.

Überarbeitet werden die Regelungen zur zulässigen Dauer (§ 100b Abs. 1 Satz 3 und 4 StPO-E) und zum notwendigen Inhalt einer Überwachungsanordnung (§ 100b Abs. 2 StPO-E). Ferner werden statistische Erhebungen zu Maßnahmen der Telekommunikationsüberwachung vorgesehen (§ 100b Abs. 5 und 6 StPO-E).

Verfassungsrechtlich gebotene Regelungen zu Kennzeichnungs-, Löschungs- und Benachrichtigungspflichten finden sich in der allgemeinen Vorschrift des § 101 StPO-E.

Zu § 100a Abs. 1 StPO-E

1. Am Beginn von Absatz 1 wird durch die Formulierung „Auch ohne Wissen der Betroffenen“, die – mit Ausnahme des Wortes „auch“ – bereits in § 100c Abs. 1 und § 100f Abs. 1 StPO und § 100h Abs. 1 StPO-E (bislang: § 100f Abs. 2 StPO) Verwendung findet, der Aspekt der Heimlichkeit der Maßnahme als besonderes Merkmal ihrer Eingriffsintensität hervorgehoben. Mit dem Wort „Auch“ wird klargestellt, dass die Maßnahme nicht etwa dadurch unzulässig wird, dass der oder die Betroffenen der Maßnahme gewahr werden. Andererseits entbindet das Wissen der Betroffenen von der Maßnahme auch nicht von der Einhaltung der Voraussetzungen der §§ 100a, 100b StPO. Nur wenn alle von der Überwachungsmaßnahme Betroffenen – also auch die jeweiligen Kommunikationspartner – in die Maßnahme in wirksamer Weise einwilligen, kann diese gegenüber den Einwilligenden aufgrund der allgemeinen Befugnisse nach den §§ 161, 163 StPO durchgeführt werden.

2. In Absatz 1 Nr. 1 wird durch den Begriff der „schweren Straftat“ das Verhältnis der Telekommunikationsüberwachung zu den anderen verdeckten Ermittlungsmaßnahmen in Bezug auf deren Eingriffsintensität und die damit korrespondierenden materiellen Anordnungsvoraussetzungen hervorgehoben. Während Artikel 13 Abs. 3 Satz 1 GG von „besonders schweren Straftaten“ spricht, deren Strafrahmen eine Mindesthöchststrafe von mehr als fünf Jahren Freiheitsstrafe aufweisen muss (BVerfGE 109, 279, 343 ff.), erfordern andere verdeckte Ermittlungsmaßnahmen als Anlasstat eine „Straftat von erheblicher Bedeutung“, die teilweise durch weitere Kriterien, u. a. in Bezug auf ihre Begehungsform, noch konkretisiert wird (vgl. § 98a Abs. 1 Satz 1, § 100f Abs. 1 Nr. 2, § 100g Abs. 1 Satz 1, § 100i Abs. 2 Satz 2 und 3, § 110a Abs. 1 Satz 1, § 163e Abs. 1 Satz 1, § 163f Abs. 1 Satz 1 StPO). Der Begriff der „Straftat von erheblicher Bedeutung“ ist inzwischen von Literatur und Rechsprechung weitgehend präzise erfasst worden (vgl. Rieß, GA 2004, 623 ff. m. w. N.) und vom Bundesverfassungsgericht mit diesem Verständnis anerkannt (BVerfGE 103, 21, 33 f.; 107, 299, 321 f.; 110, 33, 65; BVerfG, 2 BvR 1841/00 vom 15. März 2001, NJW 2001, 2320, 2321; BVerfG, 2 BvR 483/01 vom 20. Dezember 2001, StV 2003, 1 f.). Eine Straftat von erheblicher Bedeutung muss mindestens dem Bereich der mittleren Kriminalität zuzurechnen sein, den Rechtsfrieden empfindlich stören und dazu geeignet sein, das Gefühl der Rechtssicherheit der Bevölkerung erheblich zu beeinträchtigen (Schäfer, a. a. O., § 100g, Rn. 13 m. w. N.).

Im Vergleich zu den von Artikel 13 Abs. 3 Satz 1 GG vorausgesetzten besonders schweren Straftaten und den Straftaten von erheblicher Bedeutung nehmen die in § 100a Abs. 1 Nr. 1 StPO-E in Bezug genommenen schweren Straftaten eine Zwischenstellung ein. Hierunter können solche Straftaten verstanden werden, die eine Mindesthöchststrafe von fünf Jahren Freiheitsstrafe aufweisen, in Einzelfällen aufgrund der besonderen Bedeutung des geschützten Rechtsguts oder des besonderen öffentlichen Interesses an der Strafverfolgung aber auch eine geringere Freiheitsstrafe. Eine Höchststrafe von einem Jahr Freiheitsstrafe entspricht dem Begriff der schweren Straftat nicht mehr. Gesetzliche Strafmilderungen für minder schwere Fälle bleiben bei dieser Strafrahmenbetrachtung unberücksichtigt (vgl. BVerfGE 109, 279, 349).

Entsprechend dem bisherigen Recht muss – selbstverständlich – noch nicht feststehen, dass eine schwere Straftat vorliegt; eine solche Feststellung kann vielmehr erst am Ende des gerichtlichen Hauptverfahrens getroffen werden. Hinreichend – aber auch erforderlich – für die Anordnung einer Telekommunikationsüberwachung ist weiterhin der auf bestimmte Tatsachen gründende Verdacht, dass eine schwere Straftat begangen, in strafbarer Weise versucht oder durch eine andere Straftat vorbereitet wurde.

3. In Absatz 1 Nr. 2 wird klargestellt, dass die – begangene, in strafbarer Weise versuchte oder durch eine andere – ihrerseits nicht notwendig schwere – Straftat vorbereitete – Anlasstat nicht nur abstrakt, sondern auch im Einzelfall schwer wiegen muss. Hierdurch wird den Ausführungen des Bundesverfassungsgerichts 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 2006, 2603, 2611 (zum im Nds. SOG verwendeten Begriff der Straftat von erheblicher Bedeutung), Rechnung getragen, wonach eine besonders schwere Straftat bzw. eine Straftat von erheblicher Bedeutung auch im konkreten Fall besonders schwer wiegen bzw. von erheblicher Bedeutung sein muss, um einen Eingriff in das jeweilige Grundrecht zu rechtfertigen. Damit sollen die Fälle ausgeschieden werden, die zwar eine Katalogstraftat zum Gegenstand haben, aber mangels hinreichender Schwere im konkreten Einzelfall den mit einer Telekommunikationsüberwachung verbundenen Eingriff in das Fernmeldegeheimnis nicht zu rechtfertigen vermögen. Bei dieser Einzelfallprüfung sind allerdings die im Gesetz als Strafmilderungsgründe benannten minder schweren Fälle nicht von vornherein auszuschließen. Zum einen wird sich im Stadium des Ermittlungsverfahrens meist noch nicht absehen lassen, ob die Voraussetzungen eines – erst die Strafzumessung berührenden – minder

schweren Falles vorliegen. Zum anderen kann auch ein minder schwerer Fall insbesondere in Anbetracht der Auswirkungen der Straftat auf das Opfer im Einzelfall so schwer wiegen, dass die mit einer Telekommunikationsüberwachung verbundenen Eingriffe verhältnismäßig erscheinen.

4. Absatz 1 Nr. 3 enthält eine qualifizierte Subsidiaritätsklausel, die dem bisherigen § 100a Satz 1 StPO entspricht.

Zu § 100a Abs. 2 StPO-E

Der Anlasstatenkatalog wird unter Berücksichtigung des Urteils des Bundesverfassungsgerichts vom 27. Juli 2005, 1 BvR 668/04, Absatz-Nr. 152 ff. (vgl. NJW 2005, 2603, 2610 f.), und rechtstatsächlicher Erkenntnisse (vgl. Albrecht/Dorsch/Krüpe, a. a. O., S. 12 ff., 462 ff.) sowie von Erfordernissen der Strafverfolgungspraxis überarbeitet und mit dem Anlasstatenkatalog in § 100c Abs. 2 StPO harmonisiert.

Über die bislang in der Strafprozessordnung enthaltenen Kategorien der Straftaten von erheblicher Bedeutung und der besonders schweren Straftaten wird eine weitere Kategorie geschaffen, die eine Zwischenstellung zu den vorgenannten einnimmt. Einem Stufenmodell folgend werden so für eingriffsintensivere Maßnahmen entsprechend höhere Anordnungsvoraussetzungen gefordert. Der Entwurf streicht daher solche Straftaten aus dem Anlasstatenkatalog, die keine schweren Straftaten im oben dargelegten Sinne darstellen oder für deren Beibehaltung kein rechtstatsächliches Bedürfnis erkennbar ist. Neu hinzukommen bislang nicht erfasste Straftaten der Transaktions- und Wirtschaftskriminalität sowie der organisierten Kriminalität, weil die Telekommunikationsüberwachung sich gerade in diesen Bereichen als effektives und effizientes Aufklärungsmittel erwiesen hat (vgl. Albrecht/Dorsch/Krüpe, a. a. O., S. 355 ff.), ferner solche Straftatbestände, deren Nichtberücksichtigung gegenüber dem Anlasstatenkatalog der akustischen Wohnraumüberwachung (§ 100c Abs. 2 StPO) einen Wertungswiderspruch darstellen würde. Dieser ergibt sich daraus, dass die Telekommunikationsüberwachung als weniger eingriffsintensiver Grundrechtseingriff bislang teilweise für Taten nicht zugelassen ist, die eine Wohnraumüberwachung rechtfertigen können. Insgesamt verfolgt der Entwurf bei der Gestaltung des Anlasstatenkatalogs das Ziel, den Strafverfolgungsbehörden durch die grundsätzliche Ermöglichung der Maßnahme die notwendigen Mittel bei der Verfolgung schwerer und schwer ermittelbarer Kriminalität an die Hand zu geben, zugleich aber die Telekommunikationsüberwachung, die regelmäßig einen erheblichen Eingriff in Rechte Betroffener darstellt, in solchen Fällen auszuschließen, in denen die Bedeutung des zu schützenden Rechtsguts und das öffentliche Interesse an der Strafverfol-

gung nicht so gewichtig erscheinen, dass der von der Maßnahme zu erwartende Nutzen die mit ihr verbundenen Beeinträchtigungen überwiegen würde. Dies trägt dem Grundsatz Rechnung, dass auch im Strafverfahren die Wahrheit nicht „um jeden Preis“ erforscht werden darf (BGHSt 14, 358, 365; 17, 337, 348; 31, 304, 309).

Der Straftatenkatalog wird zudem neu und übersichtlicher gefasst. Im Einzelnen:

- In Absatz 2 Nr. 1 Buchstabe a werden die bisher in § 100a Satz 1 Nr. 1a StPO enthaltenen Straftaten übernommen; ausgenommen hiervon werden § 86 StGB und § 20 Abs. 1 Nr. 1 bis 4 VereinsG, die keine schweren Straftaten im oben genannten Sinne darstellen.

- In Absatz 2 Nr. 1 Buchstaben b, q und s werden zur Gewährleistung einer effektiven Bekämpfung der zunehmend an Bedeutung erlangenden Korruptionsdelikte als Anlasstaten aufgenommen:

  - Abgeordnetenbestechung nach § 108e StGB;

  - Wettbewerbsbeschränkende Absprachen bei Ausschreibungen nach § 298 StGB;

  - Besonders schwere Fälle der Bestechlichkeit und Bestechung im geschäftlichen Verkehr nach § 299 unter den in § 300 Satz 2 StGB genannten Voraussetzungen;

  - Bestechlichkeit und Bestechung nach den §§ 332 und 334 StGB.

  Dies trägt zum einen dem Umstand Rechnung, dass schon für den intensiveren Eingriff der akustischen Wohnraumüberwachung die besonders schweren Fälle der Bestechlichkeit und Bestechung nach § 335 Abs. 1 unter den in § 335 Abs. 2 Nr. 1 bis 3 StGB genannten Voraussetzungen vorgesehen sind. Zum anderen sind die jetzt darüber hinaus aufgenommenen Korruptionsdelikte jeweils dadurch gekennzeichnet, dass sie typischerweise heimlich zwischen den Tatbeteiligten begangen werden und nach außen nicht in Erscheinung treten, so dass regelmäßig auch keine Zeugen vorhanden sind, die das Tatgeschehen beobachten und zur Anzeige bringen können. Zur Aufklärung solcher Kriminalitätsformen ist der Einsatz verdeckter Ermittlungsmaßnamen auch in Form der Telekommunikationsüberwachung erforderlich und wird aus der Praxis seit langem gefordert.

  Keine Aufnahme in den Anlasstatenkatalog finden hingegen die Delikte der Vorteilsannahme nach § 331 und der Vorteilsgewährung nach § 333 StGB, weil diese keine schwe-

ren Straftaten im oben genannten Sinne darstellen und auch bei ihren qualifizierten Begehungsformen (§ 331 Abs. 2, § 333 Abs. 2 StGB) ein Bedürfnis für eine Telekommunikationsüberwachung fraglich erscheint.

- In § 100a Abs. 2 Nr. 1 Buchstabe d StPO-E werden die bislang in § 100a Satz 1 Nr. 1 Buchstabe c StPO enthaltenen Straftaten gegen die öffentliche Ordnung nach den §§ 129 bis 130 StGB übernommen. Nicht übernommen wird die Bezugnahme auf die Straftat nach § 95 Abs. 1 Nr. 8 AufenthaltsG, die mit einer Strafandrohung von einem Jahr Freiheitsstrafe oder Geldstrafe den Mindestanforderungen an eine schwere Straftat nicht genügt.

- § 100a Satz 1 Nr. 1 Buchstabe d StPO wird gestrichen, weil die Telekommunikationsüberwachung für die Aufklärung der dort in Bezug genommenen Straftatbestände (Anstiftung oder Beihilfe zur Fahnenflucht oder Anstiftung zum Ungehorsam, jeweils begangen durch Nichtsoldaten) keine praktische Relevanz hat (vgl. Albrecht/Dorsch/Krüpe, a. a. O., S. 463). Darüber hinaus haben diese unter Würdigung des vom Gesetz vorgesehenen Strafrahmens nicht die für eine Aufnahme in den Anlassstraftatenkatalog erforderliche Schwere: Die angedrohte Höchststrafe beträgt zwar für Soldaten fünf (§ 16 WStG) bzw. drei (§ 19 WStG) Jahre Freiheitsstrafe. Für die allein in Bezug genommenen Nichtsoldaten verschiebt sich jedoch nach § 28 i. V. m. § 49 Abs. 1 StGB der Strafrahmen hinsichtlich der Höchststrafe auf 4 Jahre und 3 Monate bzw. 2 Jahre und 4 Monate, wobei beim Gehilfen gemäß § 27 Abs. 2 i. V. m. § 49 Abs. 1 StGB eine weitere Strafrahmenverschiebung nach unten vorzunehmen ist.

- § 100a Satz 1 Nr. 1 Buchstabe e StPO wird gestrichen, weil der Telekommunikationsüberwachung für die in Bezug genommenen Straftaten gegen NATO-Truppen keine praktische Relevanz zukommt. Die Zahl der Verfahren in den Jahren 1998 bis 2005 ist mit Ausnahme der Jahre 2001 und 2005 gleich Null (vgl. BT-Drs. 16/2812, S. 11 ff., 15/6009, S. 7 ff.; 15/4011, S. 5 ff.; 15/2107, S. 11 ff.;14/10001, S. 2 ff.; 14/7521, S. 5 ff., 14/4863, S. 8 ff.; 14/2004, S. 5 ff.) Eine Beibehaltung dieser Vorschrift ist auch nicht aufgrund der in Art. 29 Abs. 1 und 2 des Zusatzabkommens zu dem Abkommen zwischen den Parteien des Nordatlantikvertrages über die Rechtsstellung ihrer Truppen hinsichtlich der in der Bundesrepublik Deutschland stationierten ausländischen Truppen vom 3. August 1959 (im folgenden: Zusatzabkommen) bestehenden völkerrechtliche Verpflichtung erforderlich. Danach haben die Entsendestaaten einen Anspruch darauf, dass die im Zusatzabkommen aufgeführten Handlungen – gemäß dem Bundeswehrstandard – mit Strafe bedroht und grundsätzlich verfolgt werden. Entsprechende Regelungen, die von der vorliegend

vorgesehenen Streichung nicht berührt werden, sind mit dem Vierten Strafrechtsänderungsgesetz vom 11. Juni 1957 (BGBl. I S. 597) geschaffen worden.

- In Absatz 2 Nr. 1 Buchstabe e werden aus dem Bereich der Geld- und Wertzeichenfälschung – entsprechend dem Anlasstatenkatalog des § 100c Abs. 2 StPO – die gewerbs- oder bandenmäßige Fälschung von Zahlungskarten, Schecks und Wechseln nach § 152a Abs. 3 StGB und die Fälschung von Zahlungskarten mit Garantiefunktion und Vordrucken von Euroschecks nach § 152b Abs. 1 bis 4 StGB neu aufgenommen. Es handelt sich jeweils um Straftaten, die dem Bereich der organisierten Kriminalität zuzurechnen sind und für die ein hohes öffentliches Aufklärungsinteresse besteht (vgl. auch BR-Drs. 163/04, S. 9).

- In Absatz 2 Nr. 1 Buchstabe f werden als Anlassstraftat auch die minder schweren Fälle des schweren sexuellen Missbrauchs von Kindern nach § 176a Abs. 4 StGB einbezogen. Eine Ausklammerung dieser Taten, die mit Freiheitsstrafe von drei Monaten bis zu fünf Jahren bzw. von einem Jahr bis zu zehn Jahren bedroht sind, erscheint angesichts der erheblichen Schwere dieser Delikte und der damit verbundenen weit reichenden negativen Folgen für das Opfer nicht zu rechtfertigen. Ziel gesetzgeberischer Bemühungen muss es daher sein, den Schutz von Kindern vor sexuellen Übergriffen auch durch eine effektive Strafverfolgung zu stärken. Hierzu trägt die Ermöglichung der Telekommunikationsüberwachung bei diesen Straftaten bei.

  In Harmonisierung mit dem Anlasstatenkatalog des § 100c StPO werden ferner § 177 Abs. 2 Nr. 2 und § 179 Abs. 5 Nr. 2 StGB aufgenommen. Dies vermeidet Wertungswidersprüche und trägt Verhältnismäßigkeitsgesichtspunkten Rechnung: Eine Telekommunikationsüberwachung kann in geeigneten Fallgestaltungen den Einsatz der – bei generalisierender Betrachtung – eingriffsintensiveren akustischen Wohnraumüberwachung entbehrlich machen.

- In Absatz 2 Nr. 1 Buchstabe g werden neben dem bislang schon von § 100a StPO erfassten gewerbs- oder bandenmäßigen Verbreiten, Erwerben und Besitzen kinderpornographischer Schriften nach § 184b Abs. 3 StGB auch die nicht qualifizierten Fälle des Verbreitens, des Erwerbs und des Besitzes kinderpornographischer Schriften nach § 184b Abs. 1 und 2 StGB einbezogen. Auch bei diesen Straftaten handelt es sich um schwere und – in Anbetracht der weit verbreiteten Nutzung des Internets – inzwischen telekommunikationstypische Delikte. Der Großteil kinderpornografischer Schriften wird heute über elektronische Kommunikationsmedien verbreitet und auf elektronischen Datenträgern

(Festplatten, Servern) gespeichert. Dies zeigen die Auswertungen der im Rahmen von Ermittlungsverfahren wegen Straftaten nach §§ 184 ff. StGB sichergestellten Beweismittel.

- In Absatz 2 Nr. 1 Buchstabe i werden neben den schon bislang aus dem Bereich der Straftaten gegen die persönliche Freiheit einbezogenen Straftaten auch aufgenommen die Fälle

  − des Menschenhandels zum Zweck der sexuellen Ausbeutung nach § 232 Abs. 1 und 2 StGB,

  − des Menschenhandels zum Zweck der Ausbeutung der Arbeitskraft nach § 233 Abs. 1 und 2 StGB und

  − der Förderung des Menschenhandels nach § 233a StGB.

  Damit sind die Menschenhandelsdelikte künftig insgesamt erfasst. Dies ist angesichts der Schwere dieser Delikte – es handelt sich durchgehend um zumindest schwere, zum Teil auch besonders schwere Straftaten – gerechtfertigt und entspricht Forderungen aus der Praxis, die zur Aufklärung dieser Delikte aus dem Bereich der organisierten Kriminalität gerade auf die Telekommunikationsüberwachung angewiesen ist, um in die konspirativ und abgeschottet agierenden Täterkreise eindringen zu können.

- In Absatz 2 Nr. 1 Buchstabe k wird auch der räuberische Diebstahl nach § 252 StGB einbezogen, um Wertungswidersprüche und Abgrenzungsprobleme zu den bislang schon im Anlasstatenkatalog erfassten Raub- und Erpressungsdelikten zu vermeiden.

- In Absatz 2 Nr. 1 Buchstaben n, o und q wird mit der Aufnahme besonders schwerer Fälle sowie der Qualifikationstatbestände des Betrugs, des Computerbetrugs, des Subventionsbetrugs und des Bankrotts dem Bedürfnis nach einer effektiveren Verfolgung von Straftaten aus dem Bereich der Wirtschaftskriminalität Rechnung getragen. Es handelt sich um Delikte, die typischerweise von in organisierten Strukturen handelnden Personen unter Nutzung entsprechender Organisations- und Kommunikationsstrukturen begangen werden und daher regelmäßig nur unter Einsatz verdeckter Ermittlungsmaßnahmen aufgeklärt werden können. Die Ausdehnung der Telekommunikationsüberwachung auf diese Deliktsbereiche wird insbesondere die Möglichkeit bieten, in diese organisierten und meist abgeschotteten Strukturen einzudringen. Die Erweiterung ist jedoch vor dem Hintergrund,

dass eine Vielzahl von Betrugsdelikten Gegenstand von Ermittlungsverfahren ist, auf die besonders schweren Fälle und die Qualifikationstatbestände begrenzt.

- In Absatz 2 Nr. 1 Buchstabe p werden die besonders schweren Fälle sowie die banden- und/oder gewerbsmäßig begangenen Urkundenfälschungsdelikte neu aufgenommen. Diese Delikte sind dem Kernbereich der Organisierten Kriminalität zuzurechnen und werden typischerweise in organisierten, abgeschottet agierenden Strukturen als Begleitdelikte – namentlich bei so genannten Schleusungsdelikten und beim organisierten Kfz-Diebstahl, darüber hinaus aber auch von sonstigen Tätergruppierungen – begangen (vgl. Kinzig, die Rechtliche Bewältigung von Erscheinungsformen der organisierten Kriminalität, 2004, S. 417). Die Erweiterung bleibt aus den o. g. Gründen auf die besonders schweren Fälle sowie die banden- und/oder gewerbsmäßige Begehungsweise begrenzt.

- In Absatz 2 Nr. 2 werden schwere Straftatbestände nach der Abgabenordnung neu aufgenommen.

  - Durch die Einbeziehung des besonders schweren Falls der Steuerhinterziehung nach § 370 Abs. 3 Satz 2 Nr. 5 AO (in der Fassung, die diese Vorschrift durch Artikel 3 dieses Gesetzentwurfs erhält: bandenmäßige fortgesetzte Hinterziehung von Umsatz- oder Verbrauchssteuern) wird insbesondere die Verfolgung so genannter Umsatzsteuerkarusselle verbessert werden, wofür ein erhebliches praktisches Bedürfnis besteht. Diese Form der Wirtschafts- und Transaktionskriminalität setzt Organisationsstrukturen voraus, die von außen in offen ermittelnder Form nicht zugänglich sind.

  - Die Einbeziehung des gewerbsmäßigen, gewaltsamen und bandenmäßigen Schmuggels nach § 373 AO zielt auf ein effektives Vorgehen gegen den organisierten Schmuggel (z. B. Zigarettenschmuggel), der in weiten Teilen unter Einsatz von Telekommunikationsmitteln durchgeführt wird.

  - Der organisierten Kriminalität zuzurechnen ist auch der Straftatbestand der gewerbsmäßigen oder bandenmäßigen Steuerhehlerei nach § 374 Abs. 2 AO (in der Fassung, die diese Vorschrift durch Artikel 3 dieses Gesetzentwurfs erhält), deren Einbeziehung als Anlasstat eine notwendige Ergänzung darstellt, um der Nutzziehung aus den in § 374 Abs. 1 AO genannten Steuerdelikten und damit auch der Finanzierung organisierter Kriminalität den Boden zu entziehen.

- In Absatz 2 Nr. 3 werden besonders schwere Fälle einer Dopingstraftat nach § 95 Abs. 1 Nr. 2a des Arzneimittelgesetzes (AMG) neu aufgenommen. Durch die Einbeziehung des gewerbs- oder bandenmäßigen Inverkehrbringens, Verschreibens oder Anwendens von Dopingmitteln nach § 95 Abs. 3 Satz 2 Nr. 2 Buchstabe b AMG (in der Fassung, die diese Vorschrift im parallelen Gesetzgebungsvorhaben zur Verbesserung der Bekämpfung des Dopings im Sport erhält) soll die Verfolgung der gewerbs- oder bandenmäßig organisierten Dopingkriminalität sowie der Schutz der Volksgesundheit verbessert werden. Die Einbeziehung zielt damit auf ein effektiveres Vorgehen gegen organisierte Dopingnetzwerke.

- In Absatz 2 Nr. 4 bis 8 sind die schon bislang im Straftatenkatalog des § 100a StPO enthaltenen Straftaten nach dem Asylverfahrensgesetz, dem Aufenthaltsgesetz, dem Außenwirtschaftsgesetz, dem Betäubungsmittelgesetz und dem Gesetz über die Kontrolle von Kriegswaffen (KrWaffKontrG) übernommen worden. Neu aufgenommen wurde in Nr. 8 die als Verbrechen ausgestaltete Strafvorschrift des § 20a Abs. 1 bis 3 KrWaffKontrG (Antipersonenminen). Die Aufnahme rechtfertigt sich aus der Schwere dieser Straftat sowie dem Umstand, dass der illegale Umgang mit Antipersonenminen regelmäßig in abgeschottet organisierter Weise stattfindet, so dass das Instrument der Telekommunikationsüberwachung in besonderer Weise zur Aufklärung dieses Verbrechens geeignet erscheint.

- In Absatz 2 Nr. 9 sind in Angleichung an § 100c Abs. 2 Nr. 6 StPO die Verbrechensstraftaten nach den §§ 7 bis 12 VStGB (Verbrechen gegen die Menschlichkeit, Kriegsverbrechen gegen Personen, Kriegsverbrechen gegen Eigentum und sonstige Rechte, Kriegsverbrechen gegen humanitäre Organisationen und Embleme, Kriegsverbrechen des Einsatzes verbotener Methoden der Kriegsführung) neu eingestellt worden. § 6 VStGB (Völkermord), der ebenfalls in Bezug genommen wird, ist auch bislang schon Anlasstat nach § 100a Satz 1 Nr. 2 StPO.

- In Absatz 2 Nr. 10 ist bei den Straftaten nach dem Waffengesetz die Bezugnahme auf den Fahrlässigkeitsstraftatbestand des § 51 Abs. 4 WaffG gestrichen worden, da es sich nicht um eine schwere Straftat handelt (das Gesetz droht insoweit Freiheitsstrafe von maximal zwei Jahren oder Geldstrafe an).

Zu § 100a Abs. 3 StPO-E

Die Vorschrift entspricht dem bisherigen § 100a Satz 2 StPO.

Zu § 100a Abs. 4 StPO-E

Absatz 4 trifft Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung bei Telekommunikationsüberwachungsmaßnahmen.

Das Bundesverfassungsgericht hat mehrfach einen Kernbereich privater Lebensgestaltung anerkannt, der dem staatlichen Zugriff schlechthin entzogen ist (BVerfGE 6, 32, 41; 27, 1, 6; 32, 373, 379; 34, 238, 245; 80, 367, 373; 109, 279; BVerfG, 1 BvR 668/04 vom 27. Juli 2005, Absatz-Nr. 160 ff. NJW 2005, 2603, 2611 f.). In seiner Entscheidung zur akustischen Wohnraumüberwachung (BVerfGE 109, 279 ff.) hat das Bundesverfassungsgericht erstmals einfachgesetzliche Vorkehrungen zum Schutz dieses Kernbereichs für Maßnahmen nach § 100c StPO gefordert. Dieser Forderung ist der Gesetzgeber durch das Gesetz vom 24. Juni 2005 (BGBl. I S. 1841) nachgekommen. In zeitlicher Nachfolge zu dieser Rechtsprechung ist die Anzahl von Maßnahmen nach § 100c StPO (akustische Wohnraumüberwachung) von vorher durchschnittlich knapp30 auf deutlich unter 10 zurückgegangen.

In seinem Urteil vom 27. Juli 2005 (1 BvR 668/04, NJW 2005, 2603 ff.) hat das Bundesverfassungsgericht darüber hinausgehend auch einfachgesetzliche Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung bei Maßnahmen der (gefahrenabwehrrechtlichen) Telekommunikationsüberwachung gefordert, gleichzeitig aber anerkannt, dass hier andere Maßstäbe anzulegen sind (mit beachtlichen Erwägungen kritisch zu diesen verfassungsgerichtlichen Vorgaben Löffelmann, ZStW 118 [2006], 358, 375 ff.).

Eine besondere Regelung, insbesondere eine solche, die die Strafverfolgungsbehörden verpflichten würde, prognostisch eine mögliche Kernbereichsrelevanz der Gespräche vor der Beantragung, Anordnung und Durchführung der Maßnahme im Sinne präventiven Rechtsschutzes zu prüfen, ist – anders als bei der akustischen Wohnraumüberwachung (vgl. § 100c Abs. 4 und 5 StPO) – bei der Telekommunikationsüberwachung hiernach nicht erforderlich und wäre auch nicht praktikabel. Bei der Nutzung eines Mediums, das auf die Entfernung der Kommunizierenden voneinander angelegt ist und typischerweise nicht in vergleichbarer Weise wie bei der Nutzung einer Wohnung den Rahmen für den Austausch höchstpersönlicher Informationen bietet, dessen Nutzung nicht nur die Inanspruchnahme der Dienste Dritter – der Telekommunikationsdiensteanbieter – erfordert, sondern auch im Bereich des Mobilfunks vielfach in der Öffentlichkeit stattfindet, besteht in ungleich geringerem Maße als bei der akustischen Wohnraumüberwachung, durch die unmittelbar in den „letzten Rückzugsbereich“ (BVerfGE 109, 279, 314) des Bürgers eingegriffen wird, die Gefahr der Erfassung von Ge-

sprächen, die dem Kernbereich privater Lebensgestaltung zuzuordnen und daher am unantastbaren Schutz der Menschenwürde des Betroffenen teilhaben. Ein vorbeugender Schutz für jegliche denkbare Gefährdung dieses Kernbereichs durch eine Telekommunikationsüberwachung wäre auch praktisch nicht umsetzbar, da sich – worauf auch das Bundesverfassungsgericht hinweist (BVerfG, 1 BvR 668/04 vom 27. Juli 2005, Absatz-Nr. 164, NJW 2005, 2603, 2612) – Anhaltspunkte für die Kernbereichsrelevanz eines Gesprächs in aller Regel erst aus dem Gespräch selbst ergeben.

Das Ermittlungsinstrument der Telekommunikationsüberwachung wird zudem sowohl in Deutschland als auch im internationalen Bereich als sehr bedeutsam eingeschätzt. Der Untersuchung von Albecht, Dorsch und Krüpe ist zu entnehmen, dass es als ein wichtiges und unabdingbares Ermittlungsinstrument anzusehen ist (a. a. O., S. 463). Mit Blick auf den verfassungsrechtlichen Strafverfolgungsauftrag des Staates ist es deshalb notwendig, dass für unverzichtbare Ermittlungsinstrumente, wie sie die Telekommunikationsüberwachung darstellt, ein praktikabler Anwendungsbereich verbleibt.

§ 100a Abs. 4 StPO-E stellt deshalb klar, dass eine Telekommunikationsüberwachung unzulässig ist, wenn tatsächliche Anhaltspunkte vorliegen, dass durch die Überwachung allein Erkenntnisse aus diesem Kernbereich erlangt würden. Soweit dies erkennbar ist, hat die Überwachung zu unterbleiben. Absatz 4 knüpft damit an die Regelung zum Schutz des Kernbereichs privater Lebensgestaltung bei der akustischen Wohnraumüberwachung nach § 100c Abs. 4 StPO an, unterscheidet sich davon aber in wesentlichen Punkten. Nach § 100c Abs. 4 StPO darf die akustische Wohnraumüberwachung nur dann angeordnet werden, wenn prognostiziert werden kann, dass eine Verletzung des Kernbereichs nicht zu besorgen ist; hierzu sind vor Anordnung der Maßnahme Abklärungen vorzunehmen, etwa zur Art der überwachten Räumlichkeit und zu den sich dort voraussichtlich aufhaltenden Personen. Demgegenüber ist eine Telekommunikationsüberwachung – bei Vorliegen der sonstigen Voraussetzungen – grundsätzlich zulässig und hat nur dann zu unterblieben, wenn die anhand vorliegender tatsächlicher Anhaltspunkte zu erstellende Prognose ergibt, dass allein Erkenntnisse aus dem Kerbereich privater Lebensgestaltung zu erwarten sind. Für die Erstellung dieser Prognose brauchen – anders als bei der akustischen Wohnraumüberwachung – keine besonderen vorausgehenden Ermittlungen getätigt zu werden.

Erwogen worden ist, den Anforderungen des Bundesverfassungsgerichts in der Entscheidung 1 BvR 668/04 vom 27. Juli 2005 (NJW 2005, 2603 ff.) dadurch Rechnung zu tragen, dass lediglich ein Beweisverwertungsverbot für Erkenntnisse aus dem Kernbereich persönlicher Lebensgestaltung vorgesehen wird (so z. B. für den Bereich der Polizeigesetze: Si-

cherheits- und Ordnungsgesetz des Landes Mecklenburg-Vorpommern, GVOBl. M-V 2006, S. 551). Auch in der Literatur wird teilweise vertreten, dass die Anforderungen in der vorgenannten Entscheidung des Bundesverfassungsgerichts nicht das „Ob“ der Maßnahme, sondern lediglich das „Wie“ betreffe; die unterschiedlichen Schutzbereiche und Schutzrichtungen von Artikel 10 GG einerseits und Artikel 13 GG andererseits ließen für den Bereich der Überwachung der Telekommunikation ein Beweisverwertungsverbot ausreichend erscheinen (vgl. Gusy, Nds.VBl. 2006, 65, 69).

Die Vereinbarkeit dieser Auffassung mit den Vorgaben des Bundesverfassungsgerichts ist indessen zumindest zweifelhaft. Nach den Darlegungen des Bundesverfassungsgerichts hat bereits die Maßnahme zu unterbleiben, wenn der Kernbereich privater Lebensgestaltung betroffen wird. Dem trägt das Erhebungsverbot in § 100a Abs. 4 Satz 1 StPO-E Rechnung. Anders als bei einer akustischen Wohnraumüberwachung, bei der Anhaltspunkte anhand der Art der zu überwachenden Räumlichkeit und dem Verhältnis der zu überwachenden Personen zueinander gewonnen werden können, ist bei einer Telekommunikationsüberwachungsmaßnahme – worauf auch das Bundesverfassungsgericht hinweist – kaum je vorhersehbar, ob kernbereichsrelevante Inhalte anfallen. Soll etwa ein privater Anschluss abgehört werden, so wird sich regelmäßig nicht ausschließen lassen, dass private Gespräche – bis hin zum Austausch intimster Kommunikationsinhalte – erfasst würden. Aber auch von primär geschäftlich oder dienstlich genutzten Festnetzanschlüssen werden erfahrungsgemäß auch private Gespräche geführt, die kernbereichsrelevante Inhalte aufweisen können. Die Erfassung kernbereichsrelevanter Inhalte lässt sich damit – wie auch das Bundesverfassungsgericht ausführt – bei einer Telekommunikationsüberwachung regelmäßig nicht ausschließen.

Theoretisch könnte die Erfassung kernbereichsrelevanter Kommunikation bei einer Telekommunikationsüberwachung allerdings durch ein Mithören in Echtzeit weitgehend abgewendet werden. Sobald ein zu überwachendes Gespräch kernbereichsrelevant wird, wäre das Abhören und Aufzeichnen der Telekommunikation zu unterbrechen oder gar endgültig zu beenden. Ein solches Vorgehen ist indessen weder praktisch durchführbar noch mit vertretbarem – auch zusätzlichem – personellen und sonstigen Aufwand zu leisten. Ein Großteil der derzeit zu Zwecken der Strafverfolgung überwachten Telekommunikation wird beispielsweise in fremden, zum Teil nicht ohne weiteres identifizierbaren Sprachen und Dialekten und darüber hinaus unter Benutzung von Geheimcodes geführt. Selbst bei ständigem parallelem Mithören durch einen Dolmetscher könnte hierbei nicht gewährleistet werden, dass der Inhalt der Gespräche sofort zutreffend erfasst und übersetzt wird. Oftmals ist hierfür vielmehr das wiederholte Abspielen und Anhören der aufgezeichneten Kommunikation unter Einbeziehung der bisherigen Erkenntnisse des Verfahrens unabdingbar. Darüber hinaus sind manche Ge-

spräche aus sonstigen, der Nutzung des Mediums geschuldeten Gründen (z. B. Hintergrundrauschen, schlechter Empfang) kaum ohne technische Aufbereitung beim ersten Hören zu verstehen. Hinzu kommt, dass Betroffene mitunter eine Vielzahl von Telekommunikationsmitteln besitzen und teilweise parallel nutzen, etwa telefonische Absprachen über die parallel im Internet vorzunehmenden Aktivitäten treffen (während vielleicht auch noch parallel ein Telefax eingeht). Die in der Praxis zur Erfassung aller ermittlungsrelevanten Kommunikation regelmäßig notwendige Rund-um-die-Uhr-Überwachung könnte bei dem Erfordernis eines Mithörens in Echtzeit selbst bei einer deutlichen Aufstockung der Personalkapazitäten nicht geleistet werden. Dies gilt erst recht und gerade im Bereich der für eine Telekommunikationsüberwachung primär in Betracht kommenden organisierten Kriminalität, die regelmäßig die parallele Überwachung mehrerer Personen mit teilweise zahlreichen Telekommunikationsanschlüssen notwendig macht.

Auch das Bundesverfassungsgericht hat – wohl eingedenk dieser tatsächlichen Gegebenheiten – kein Mithören in Echtzeit bei der Telekommunikationsüberwachung gefordert, sondern ausgeführt, dass insoweit nicht dieselben strengen Maßstäbe wie bei einer akustischen Wohnraumüberwachung anzulegen sind, die zudem ebenfalls nicht stets ein Mithören in Echtzeit erfordert.

Die Regelung in § 100a Abs. 4 Satz 1 StPO-E trägt diesen Erkenntnissen Rechnung. Die Regelung ermöglicht weiterhin eine zur Verfolgung von schweren Straftaten notwendige effektive Durchführung von Telekommunikationsüberwachungsmaßnahmen und gewährleistet zugleich in praktikabler Weise den Schutz des Kernbereichs privater Lebensgestaltung. Einerseits trifft sie zum Schutz des Kernbereichs privater Lebensgestaltung bereits auf der Anordnungsebene ein Erhebungsverbot für den Fall, dass von vornherein allein – ohnehin nicht verwertbare (vgl. Absatz 4 Satz 2) – Erkenntnisse aus dem Kernbereich privater Lebensgestaltung zu erwarten sind. Andererseits begrenzt sie dieses Erhebungsverbot auf Fallgestaltungen, in denen die Maßnahme ausschließlich Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erwarten lässt. Solche Fallgestaltung werden außerhalb des Anwendungsbereichs des § 53b Abs. 1 StPO-E selten anzutreffen sein. Ein Beispiel dürfte die Kommunikation mit der durch die katholische und evangelische Kirche angebotene Telefonseelsorge sein, die meist nicht von Geistlichen im Sinne des § 53 Abs. 1 Satz 1 Nr. 1 StPO sondern von besonders geschulten haupt- und ehrenamtlichen Mitarbeitern im Auftrag der Kirchen durchgeführt wird.

Nach Absatz 4 Satz 2 dürfen Erkenntnisse aus dem Kernbereich privater Lebensgestaltung nicht verwertet werden. Dies entspricht den vom Bundesverfassungsgerichts aufgestellten

Vorgaben wie auch der gefestigten fachgerichtlichen Rechtsprechung (vgl. 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, 2 BJs 112/97-2 – StB 10 u 11/99 vom 13. Oktober 1999, NStZ 2000, 383), die von dem Gedanken ausgeht, dass durch eine derartige Verwertung der unzulässige Eingriff in den Kernbereich noch vertieft würde. Aus diesem Verwertungsverbot kann sich in besonderen Einzelfällen unter Anwendung des Grundsatzes der Verhältnismäßigkeit die Verpflichtung ergeben, die Überwachung und Aufzeichnung der Telekommunikation zu unterbrechen. Wird etwa – wozu die Regelungen des § 100a Abs. 4 StPO-E nicht verpflichten und was in der Praxis den Ausnahmefall darstellen dürfte – im Zuge einer Telekommunikationsüberwachungsmaßnahme eine Telekommunikation ausnahmsweise in Echtzeit („live“) mitgehört und dabei zweifelsfrei erkannt, dass kernbereichsrelevante Inhalte Gegenstand der Kommunikation sind, so ist deren weitere Erhebung schon deshalb unzulässig, weil sie in Ansehung des Verwertungsverbotes in Satz 2 nicht geeignet ist, die Erreichung des mit der Maßnahme verfolgten Zwecks zu fördern. In solchen Ausnahmefallgestaltungen ist die Überwachung und Aufzeichnung der Telekommunikation daher vorübergehend zu unterbrechen.

Mit dem Verwertungsverbot korrespondiert in Absatz 4 Satz 3 die Pflicht, durch einen Eingriff in den Kernbereich erlangte Erkenntnisse unverzüglich zu löschen. Dieses Gebot zur unverzüglichen Löschung verpflichtet grundsätzlich diejenige Person, die dazu am ehesten in der Lage ist, in der Regel also die mit der Auswertung von Überwachungsaufzeichnungen betrauten Ermittlungspersonen. Diese kann – und wird in zweifelhaften Fällen – vor einer Löschung die Entscheidung der Staatsanwaltschaft einholen. Auch ist es der Staatsanwaltschaft als „Herrin des Ermittlungsverfahrens“ unbenommen, sich im Einzelfall oder auch generell die Entscheidung über die Löschung vorzubehalten. Stets muss die Entscheidung über eine Löschung aber unverzüglich, also ohne schuldhaftes Zögern, herbeigeführt werden, damit – soweit geboten – auch die Löschung unverzüglich erfolgen kann.

Um die Erlangung von Rechtsschutz gegen den Eingriff zu sichern, ist nach Absatz 4 Satz 4 die Tatsache der Erfassung solcher Erkenntnisse und der Löschung von Aufzeichnungen hierüber aktenkundig zu machen.

Erwogen wurde ferner eine Regelung nach dem Vorbild des § 100c Abs. 7 StPO, wonach bei Zweifeln darüber, ob nicht verwertbare Erkenntnisse erlangt wurden, unverzüglich eine Entscheidung des Gerichts über die Verwertbarkeit herbeizuführen ist. Aus den bereits zu § 53b Abs. 1 StPO-E (vor den Erläuterungen zu § 53b Abs. 2 StPO-E) dargelegten Gründen wurde von einer entsprechenden Regelung abgesehen.

Zu § 100b StPO-E

In § 100b StPO-E sind – wie bislang – die für die Anordnung und Durchführung einer Telekommunikationsüberwachung maßgeblichen Verfahrensregelungen zusammengefasst, soweit diese nicht in allgemeinen Vorschriften, insbesondere in § 101 StPO-E bzw. – hinsichtlich der bislang in § 100b Abs. 5 StPO enthaltenen Verwendungsregelung – in § 477 Abs. 2 StPO-E eingestellt werden.

Zu § 100b Abs. 1 StPO-E

Absatz 1 stellt die Telekommunikationsüberwachung weiterhin unter den Vorbehalt der gerichtlichen Anordnung und enthält die jeweils zu beachtenden Anordnungsfristen.

Satz 1 bestimmt, dass Maßnahmen nach § 100a StPO-E stets eines Antrags der Staatsanwaltschaft bedürfen und – wie bislang – dem Vorbehalt der gerichtlichen Anordnung unterliegen. Zuständiges Gericht ist im Ermittlungsverfahren das Amtsgericht am Sitz der Staatsanwaltschaft, § 162 Abs. 1 StPO-E.

Nach Satz 2 kann die Staatsanwaltschaft entsprechend dem geltenden Recht bei Gefahr im Verzug die Anordnung auch selbst treffen (Eilanordnung).

Ebenfalls entsprechend dem geltenden Recht bestimmt Satz 3 Halbsatz 1, dass die Eilanordnung der Staatsanwaltschaft außer Kraft tritt, wenn sie nicht binnen drei Werktagen von dem Gericht bestätigt wird. Neu ist die in Satz 3 Halbsatz 2 aufgenommene und einer möglichen Umgehung des Richtervorbehalts vorbeugende Regelung, nach der die aufgrund der Eilanordnung erlangten personenbezogenen Daten nur dann zu Beweiszwecken im Strafverfahren verwertbar sind, wenn die für die Eilanordnung der Staatsanwaltschaft vorausgesetzte Gefahr im Verzug bestand. Das erkennende Gericht hat daher bei einer beweismäßigen Verwertung von Erkenntnissen, die aufgrund einer Eilanordnung der Staatsanwaltschaft erlangt wurden, auch zu prüfen, ob die für die Eilanordnung erforderliche Gefahr im Verzug bestand.

Nach Satz 4 ist die Maßnahme auf maximal zwei Monate zu befristen. Die damit verbundene Verkürzung der Anordnungsdauer von bislang drei auf nunmehr zwei Monate berücksichtigt die rechtstatsächlichen Erkenntnisse aus der Untersuchung von Albrecht/Dorsch/Krüpe

(a. a. O., S. 166 ff., 170 f.), wonach etwa drei Viertel der Telekommunikationsmaßnahmen über einen Zeitraum von bis zu zwei Monaten geführt und nur etwa 9 % der Anschlüsse tatsächlich über die Dauer von drei Monaten überwacht werden. Damit erscheint für den Großteil der Maßnahmen eine Anordnungsdauer von maximal zwei Monaten ausreichend. Aufgrund dieser Verkürzung der Anordnungsdauer dürfte allerdings ein Anstieg der Anzahl der Verlängerungsanordnungen und damit auch der Gesamtzahl der jährlichen Telekommunikationsanordnungen zu erwarten sein.

Nach Satz 5 kann die Anordnung wie schon bislang – auch mehrfach – verlängert werden, soweit dies im Einzelfall erforderlich ist. Neu ist, dass die Verlängerung jeweils auf maximal zwei Monate zu befristen ist; dies trägt den vorgenannten rechtstatsächlichen Erkenntnissen Rechnung. Ferner ist ausdrücklich klargestellt, dass eine Verlängerung nur zulässig ist, wenn die Anordnungsvoraussetzungen unter Berücksichtigung der gewonnenen Ermittlungsergebnisse fortbestehen. Dies setzt in der Praxis voraus, dass das Gericht von den Strafverfolgungsbehörden über die zwischenzeitlich gewonnenen Ermittlungsergebnisse – nicht nur aus der Telekommunikationsüberwachung, sondern auch aus etwaigen anderen zwischenzeitlichen Ermittlungsmaßnahmen – hinreichend in Kenntnis gesetzt wird.

Für die Berechnung der Anordnungs- wie auch der Verlängerungsfristen gelten die allgemeinen Regelungen der §§ 42 ff. StPO (vgl. eingehend zur Berechnung der Fristen im Rahmen des geltenden § 100b StPO: Günther, Kriminalistik 2006, S. 683 ff.). Der Fristbeginn wird dabei bereits durch den Erlass der gerichtlichen Erst- bzw. Verlängerungsanordnung ausgelöst. Nur so ist gewährleistet, dass die Anordnung der Maßnahme die jeweils aktuellen Erkenntnisse zugrunde gelegt und in die gerichtliche Prüfung der Anordnungsvoraussetzungen einbezogen werden können. Dies gilt auch dann, wenn eine Verlängerungsanordnung deutlich vor Ablauf der Erstanordnung erlassen wird, so dass die in der Erstanordnung enthaltene Frist faktisch nicht voll ausgeschöpft wird. Dies schließt den Erlass „vorsorglicher“ Verlängerungsanordnungen aus. Hiermit wird eine jeweils zeitnahe gerichtliche Kontrolle der Telekommunikationsüberwachungsmaßnahme im Sinne eines möglichst effektiven Grundrechtsschutzes der von der Maßnahme betroffenen Personen gewährleistet. Zur Bestimmung des Fristendes vgl. auch die Neuregelung in Absatz 2 Satz 2 Nr. 3 (Benennung des Endzeitpunktes).

Satz 6 ergänzt dieses Kontrollsystem, indem Anordnungen über sechs Monate hinaus nur durch das im Rechtszug übergeordnete Gericht – regelmäßig also das Landgericht – angeordnet werden dürfen. Dies gilt allerdings nur vorbehaltlich des § 169 StPO: In Sachen, die in die Zuständigkeit des Ermittlungsrichters beim Oberlandesgericht oder beim Bundesge-

richtshof gehören, bleibt dieser auch für Verlängerungen über sechs Monate hinaus zuständig.

Zu § 100b Abs. 2 StPO-E

Die Vorschrift enthält in Modifizierung von § 100b Abs. 2 Satz 1 bis 3 StPO und in Anlehnung an § 100d Abs. 2 StPO qualifizierte Pflichten für Form und Inhalt eines Anordnungsbeschlusses. Qualifizierte Begründungspflichten werden allerdings – anders als bei der akustischen Wohnraumüberwachung (§ 100d Abs. 3 StPO) – nicht vorgesehen, da die Anordnungsvoraussetzungen für die Telekommunikationsüberwachung, insbesondere mit Blick auf die bei der akustischen Wohnraumüberwachung erforderliche qualifizierte Kernbereichsprognose, insgesamt geringer sind. Zudem ist die gefestigte Rechtsprechung zu den notwendigen Begründungsinhalten von Durchsuchungsbeschlüssen, die auch hier Anwendung findet, ohnehin zu beachten (BVerfGE 96, 44, 52; 103, 142, 151; 107, 299 ff.; BVerfG, 2 BvR 27/04 vom 8. März 2004, NJW 2004, 1517 ff.). Die Aufnahme einer qualifizierten Begründungspflicht bei Telekommunikationsüberwachungsanordnungen würde die besonderen Anforderungen, die an die Begründung der Anordnung einer akustischen Wohnraumüberwachung zu stellen sind, relativieren und im Umkehrschluss die Frage aufwerfen, ob an die Begründung der Anordnung anderer verdeckter und offener Ermittlungsmaßnahmen geringere Anforderungen zu stellen sind. Eine allgemeine Pflicht zur angemessenen, die Nachvollziehbarkeit und Überprüfung der Entscheidung ermöglichenden Begründung einer Anordnung ergibt sich bereits aus § 34 StPO.

- Nach Absatz 2 Satz 1 hat die Anordnung einer Telekommunikationsüberwachung schriftlich zu ergehen. Dies entspricht dem geltenden Recht und bezieht sich sowohl auf die gerichtliche Anordnung als auch auf die staatsanwaltschaftliche Eilanordnung und etwaige Verlängerungsanordnungen.

- Nach Absatz 2 Satz 2 Nr. 1 sind der Name und die Anschrift der betroffenen Person, gegen die sich die Maßnahme richtet, anzugeben, soweit diese Angaben möglich sind. Die Einschränkung „soweit möglich“ trägt dem Umstand Rechnung, dass nicht stets vollständige Angaben zur Person des Betroffenen bekannt sind, z. B. weil diese unter einem Alias- oder Decknamen auftritt oder ihr Name noch gar nicht bekannt ist.

- Erwogen wurde, entsprechend den oben genannten, durch die Rechtsprechung festgelegten Anforderungen an den notwendigen Inhalt einer Anordnung in Anlehnung an § 100d Abs. 2 Nr. 2 StPO festzulegen, dass die Entscheidungsformel auch den Tatvorwurf, auf-

grund dessen die Maßnahme angeordnet wird, anzugeben hat. Davon wurde vor dem Hintergrund, dass der Beschluss in den Fällen des Absatzes 3 – also regelmäßig – an das Telekommunikationsunternehmen zu übermitteln ist, aus Verhältnismäßigkeitsgesichtspunkten (Datenschutz) abgesehen.

- Nach Absatz 2 Satz 2 Nr. 2 muss die Anordnung ferner die Rufnummer oder eine andere Kennung (z. B. die IMSI − International Mobile Subscriber Identity) des zu überwachenden Anschlusses oder des Endgerätes enthalten.

  Die Möglichkeit der Angabe einer Kennung des zu überwachenden Endgerätes steht unter der – vom Gesetzgeber auch in § 23b Abs. 4 Satz 2 Nr. 2 ZFdG vorgesehenen – Einschränkung, dass die anzugebende Endgerätekennung auch allein dem zu überwachenden Endgerät zugeordnet ist. Die damit künftig auch strafprozessual mögliche so genannte „IMEI-gestützte“ Überwachung eines Mobiltelefons trägt den Schwierigkeiten Rechnung, die sich derzeit bei der Überwachung polizei- und ermittlungserfahrener Täter ergeben. Diese verfügen teilweise über zahlreiche (mitunter über 100) verschiedene Mobiltelefonkarten (SIM-Karten), die sie abwechselnd in dem zumeist selben Mobilfunkgerät einsetzen (so genannte „Kartenspieler“). Dadurch ändert sich die zu überwachende Kennung des Mobilfunkabschlusses fortwährend, so dass bislang die jeweils neue Kennung des Anschlusses zunächst ermittelt und sodann ein auch auf diese Kennung bezogener gerichtlicher Überwachungsbeschluss herbeigeführt werden muss. Durch diese Taktik können die Beschuldigten der Überwachung für gewisse Zeiträume und teilweise auch ganz entgehen. Aus den dadurch entstehenden Überwachungslücken ergibt sich ein Bedürfnis der Praxis, über die Gerätekennung (IMEI) des dauerhaft genutzten Mobiltelefons eine möglichst unterbrechungsfreie Überwachung der Telekommunikation herbeizuführen. Dem trägt die Neuregelung in Absatz 2 Satz 2 Nr. 2 Rechnung.

  Die Voraussetzung, dass die zu überwachende Endgerätekennung allein dem zu überwachenden Endgerät zugeordnet ist, wird in der Praxis dadurch sicherzustellen sein, dass die nach Absatz 3 zur Mitwirkung und Auskunftserteilung verpflichteten Telekommunikationsdienstleister vor der Schaltung der Überwachungsmaßnahme überprüfen, ob die betreffende Gerätekennung mehrfach in das Mobilfunknetz eingebucht ist.

- Absatz 2 Satz 2 Nr. 3 übernimmt aus § 100b Abs. 2 Satz 3 StPO das Erfordernis der Angabe von Art, Umfang und Dauer der Maßnahme. Durch entsprechende Konkretisierungen, die auch die Art des technischen Zugriffs auf die zu überwachende Telekommunikation betreffen, wird erreicht, dass die Maßnahme zielgerichtet eingesetzt und der Richter-

vorbehalt im Sinne einer umfassenden Prüfung aller eingriffsrelevanten Aspekte ausgeübt wird. Neu ist, dass hinsichtlich der Dauer der Maßnahme in den Anordnungen jeweils auch der Endzeitpunkt der Maßnahme anzugeben ist. Damit sind die erforderlichen Fristberechnungen von der anordnenden Stelle mit Verbindlichkeit insbesondere auch für die nach Absatz 3 zur Mitwirkung verpflichteten Telekommunikationsdienstleister vorzunehmen. Dies vermeidet Ungewissheiten und daraus in der Vergangenheit gelegentlich resultierte Streitigkeiten, bis zu welchem genauen Tag eine angeordnete Maßnahme auszuführen ist.

Zu § 100b Abs. 3 StPO-E

Absatz 3 statuiert – entsprechend dem bisherigen Recht – eine Mitwirkungspflicht der Telekommunikationsdienstleister zur Ermöglichung der Telekommunikationsüberwachung. Diese haben die Durchführung der Überwachungsmaßnahme zu ermöglichen und – was nunmehr im Gesetzestext auch im Hinblick auf den in § 100g Abs. 2 StPO-E eingestellten Verweis auf § 100b Abs. 3 ausdrücklich klargestellt wird – die erforderlichen Auskünfte zu erteilen.

Die Notwendigkeit für diese Inpflichtnahme ergibt sich daraus, dass sich Telekommunikationsüberwachungsmaßnahmen in effizienter Weise regelmäßig nur unter Mitwirkung der Telekommunikationsdienstleister umsetzen lassen, indem diese eine Kopie der heute durchgehend digitalisierten Telekommunikationssignale an die Strafverfolgungsbehörden ausleiten. Eine Obliegenheit der Strafverfolgungsbehörden, Telekommunikationsüberwachungsmaßnahmen stets unter Mitwirkung eines Telekommunikationsdienstleisters durchzuführen, wird damit allerdings nicht begründet. Vielmehr enthält § 100a Abs. 1 Satz 1 StPO-E eine nicht durch die Mitwirkung der Telekommunikationsdienstleister bedingte Befugnis, Telekommunikation zu überwachen und aufzuzeichnen. Beschränkt wird diese Befugnis lediglich durch die in der gerichtlichen Anordnungsentscheidung näher zu bestimmende Art der Überwachung (vgl. § 100b Abs. 2 Satz 2 Nr. 3 StPO-E). Nach Maßgabe der gerichtlichen Anordnungsentscheidung sind die Strafverfolgungsbehörden daher auch berechtigt, Überwachungsmaßnahmen ausschließlich mit eigenen Mitteln durchzuführen. Dass hierbei auch technische Mittel eingesetzt werden dürfen, ergibt sich ebenfalls bereits aus § 100a Abs.1 Satz 1 StPO-E, da das dort ausdrücklich erlaubte Überwachen und Aufzeichnen von Telekommunikation regelmäßig nur unter Einsatz technischer Mittel erfolgen kann. Im Einzelfall ist allerdings bei der Umsetzung einer Überwachungsmaßnahme strikt zu beachten, dass nur diejenige Telekommunikation erfasst wird, deren Überwachung durch die gerichtliche Anordnung legitimiert ist.

Notwendig ist mit Blick auf die Umsetzung von Artikel 17 i. V. m. Artikel 16 des Übereinkommens über Computerkriminalität, die keine dem bisherigen Absatz 3 entsprechende Beschränkung von Mitwirkungspflichten auf Telekommunikationsdiensteanbieter vorsehen, die ihre Dienste *geschäftsmäßig* erbringen, die Ausweitung der Vorschrift auch auf solche Personen und Stellen, die Telekommunikationsdienste erbringen oder daran mitwirken, ohne geschäftsmäßig zu handeln. „Geschäftsmäßiges Erbringen von Telekommunikationsdiensten“ ist das nachhaltige Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht (§ 3 Nr. 10 TKG). Nicht erfasst sind hiervon solche Telekommunikationsdienste, die innerhalb eines geschlossenen Systems anfallen, z. B. zwischen nur für den „Eigenbedarf“ betriebenen Nebenstellen, wie in Hotels, Krankenhäusern, Betrieben oder bei Haustelefonanlagen (Nack, a. a. O., § 100a, Rn. 18). Artikel 16 und 17 des Übereinkommens über Computerkriminalität sehen eine Beschränkung der Mitwirkungspflicht auf Stellen und Personen, die Telekommunikationsdienste geschäftsmäßig anbieten, nur unter der Vorbehaltsmöglichkeit von Artikel 16 Abs. 4 i. V. m. Artikel 14 Abs. 3 Buchstabe b des Übereinkommens vor. Diese erstreckt sich jedoch nur auf Maßnahmen nach den Artikeln 20 und 21 des Übereinkommens, im Falle von Verkehrsdaten also auf deren Echtzeiterhebung.

Aufgrund der zunehmenden Verbreitung geschlossener Telekommunikationssysteme kommt einer entsprechenden Ausdehnung der Mitwirkungspflicht auch auf nicht geschäftsmäßig handelnde Anbieter große kriminalistische Bedeutung zu. Werden etwa aus einem Unternehmen oder aus einer Behörde heraus kriminelle Handlungen begangen, so können auch Erkenntnisse über die unternehmensinterne Telekommunikation zur Tataufklärung beitragen. Diese Überlegungen gelten auch für die Echtzeiterhebung von Verkehrsdaten, die daher – ohne von der Vorbehaltsmöglichkeit des Artikel 16 Abs. 4 i. V. m. Artikel 14 Abs. 3 Buchstabe b des Übereinkommens Gebrauch zu machen – entsprechend geregelt werden soll. Um nicht geschäftsmäßig tätig werdenden Stellen keine unverhältnismäßigen Kosten aufzubürden, bleibt die in der Telekommunikations-Überwachungsverordnung (TKÜV) vorgesehene Verpflichtung, Vorkehrungen für die Umsetzung von Überwachungsmaßnahmen zu treffen, auf „öffentliche“ Anbieter beschränkt. Der entsprechende Verweis in Absatz 3 Satz 2 wird allgemeiner gefasst, um durch Änderungen des in Bezug genommenen Telekommunikationsgesetzes häufig veranlasste Folgeänderungen zu vermeiden.

Zu § 100b Abs. 4 StPO-E

Satz 1 entspricht inhaltlich der bisherigen Regelung in § 100b Abs. 4 Satz 1 StPO und stellt damit klar, dass die aufgrund der Überwachungsanordnung ergriffenen Maßnahmen unverzüglich zu beenden sind, wenn die Voraussetzungen der Anordnung nicht mehr vorliegen.

Die im bisherigen Satz 2 enthaltene Regelung zur Mitteilung der Beendigung der Maßnahme an das Gericht und den nach § 100b Abs. 3 StPO verpflichteten Telekommunikationsdiensteanbieter ist nicht übernommen worden, ohne dass damit eine inhaltliche Änderung verbunden ist. Denn die Pflicht zur Unterrichtung des Telekommunikationsdiensteanbieters folgt bereits aus Satz 1, wonach die aufgrund der Anordnung ergriffenen Maßnahmen unverzüglich zu beenden sind. Dies setzt hinsichtlich der Ausleitung der überwachten Telekommunikation vom Telekommunikationsdiensteanbieter an die Strafverfolgungsbehörde bereits eine entsprechende Unterrichtung des Telekommunikationsdiensteanbieters durch die Strafverfolgungsbehörde voraus und bedarf daher keiner gesonderten gesetzlichen Regelung.

Der neue Satz 2 weitet die bislang bestehende Pflicht zur Unterrichtung des Gerichts von der Beendigung der Maßnahme dahingehend aus, dass dieses nunmehr auch über den Verlauf und die Ergebnisse der Überwachung zu unterrichten ist. Die in Anlehnung an § 100d Abs. 4 StPO geregelte Unterrichtungspflicht dient der Stärkung der mit dem Richtervorbehalt bezweckten rechtsstaatlichen Kontrolle. Sie soll dem Gericht, das bislang in vielen Fällen keine Rückmeldung erhält, so es nicht mit weiteren Entscheidungen (etwa Verlängerungsanordnungen) betraut wird, eine Erfolgskontrolle ermöglichen, um die daraus resultierenden Erfahrungen bei künftigen Entscheidungen berücksichtigen zu können.

Zu § 100b Abs. 5 und 6 StPO-E

Die Absätze 5 und 6 werden mit anderen Regelungsinhalten neu gefasst; der Gehalt des bisherigen Absatzes 5 (Verwendungsbeschränkung) findet sich nunmehr in § 477 Abs. 2 Satz 2 StPO-E, derjenige des bisherigen Absatzes 6 (Vernichtungsregelung) in § 101 Abs. 10 StPO-E.

Mit den neu gefassten Absätzen 5 und 6 wird eine einheitliche Bestimmung für statistische Erhebungen zu Telekommunikationsüberwachungsmaßnahmen nach § 100a Abs. 1 StPO-E geschaffen, die § 110 Abs. 8 TKG sowie die korrespondierende Regelung in § 25 TKÜV ablöst und für die schon bislang erfolgenden statistischen Mitteilungen der Landesjustizverwaltungen und des Generalbundesanwalts beim Bundesgerichtshof eine ausdrückliche gesetzliche Verpflichtung trifft.

Absatz 5 Satz 1 bestimmt, dass die Länder sowie der Generalbundesanwalt dem (künftigen) Bundesamt für Justiz kalenderjährlich über in ihrem jeweiligen Zuständigkeitsbereich angeordnete Maßnahmen nach § 100a StPO-E berichten. Bei diesen Berichten handelt es sich,

wie sich aus Absatz 6 ergibt, um reine statistische Angaben. Die Übermittlung personenbezogener Daten ist damit nicht verbunden. Die Berichte sind, um eine zeitnahe Kenntnisnahme der aktuellen Entwicklung bei Telekommunikationsüberwachungsmaßnahmen zu gewährleisten, jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres zu übermitteln. Es bleibt den Ländern sowie dem Generalbundesanwalt überlassen, in welcher Weise dort für die Erstellung und rechtzeitige Übermittlung der Berichte Sorge getragen wird. Die Länder werden, entsprechend ihrer Handhabung in der Vergangenheit, voraussichtlich durch die Landesjustizverwaltungen entsprechende Berichte aufgrund von Mitteilungen der Staatsanwaltschaften erstellen.

Absatz 5 Satz 2 verpflichtet das Bundesamt für Justiz, anhand der von den Ländern und vom Generalbundesanwalt mitgeteilten Daten eine bundesweite Übersicht zu erstellen und diese im Internet zu veröffentlichen. Hierdurch wird ein hohes Maß an Transparenz hinsichtlich der Entwicklung von repressiv veranlassten Telekommunikationsüberwachungsmaßnahmen erreicht.

Absatz 6 führt die in den Berichten nach Absatz 5 im Einzelnen anzugebenden Daten konkret auf:

- Die Nummern 1 bis 3 beziehen sich auf aus den Anordnungs- oder Verlängerungsbeschlüssen ohne weiteres ablesbare Daten (Anzahl der Verfahren, in denen Anordnungen ergangen sind; Anzahl der Anordnungen, unterschieden nach erstmaliger und Verlängerungsanordnung sowie nach Art der zu überwachenden Kommunikation; zugrunde liegende Anlasstat).

- Nummer 4 verlangt die Angabe der Anzahl der überwachten Telekommunikationsvorgänge, und zwar aufgeschlüsselt nach Festnetz-, Mobilfunk- und Internettelekommunikation. Die Angabe soll Erkenntnisse darüber erbringen, in welchem Ausmaß durch Maßnahme nach § 100a StPO Telekommunikation überwacht und dadurch Personen in ihren Grundrechten beschränkt werden. Anzugeben sind damit etwa die Anzahl der überwachten Insoweit war zunächst erwogen worden, die Anzahl der Beteiligten an der überwachten Telekommunikation erheben zu lassen. Dies stößt indessen auf praktische Probleme. So könnte beispielsweise bei unbekannten Gesprächsteilnehmern von Telefonaten allenfalls mit ganz erheblichem zusätzlichen und unverhältnismäßigen Aufwand bestimmt werden, ob es sich um die jeweils selbe oder andere Personen handelt. Verlässliche Zahlen über die Anzahl der Beteiligten lassen sich daher nicht gewinnen. Wohl aber entspricht des der üblichen Vorgehensweise bei Telekommunikationsüberwachungsmaßnahmen, die Auf-

zeichnung jedes Telekommunikationsvorgangs gesondert auszuwerten, so dass ein Zählung der erfassten Telekommunikationsvorgänge ohne weiteres und ohne hohen zusätzlichen Aufwand möglich ist.

Zu Nummer 8 (§ 100c StPO-E)

Die vorgesehenen Änderungen in den Absätzen 1 und 6 sind im Wesentlichen redaktioneller Art:

- Die Voranstellung des Wortes „Auch“ in Satz 1 stellt klar, dass die Maßnahme nicht dadurch unzulässig wird, dass ein Betroffener der Maßnahme gewahr wird (vgl. im Einzelnen die Ausführungen zu der entsprechenden Änderung in § 100a Abs. 1 StPO-E).

- Die Einfügung der Wörter „als Täter oder Teilnehmer“, die ebenfalls in der redaktionell entsprechenden Regelung des § 100a Abs. 1 Nr. 1 StPO(-E) enthalten sind, dient der Klarstellung, dass die akustische Wohnraumüberwachung auch gegen einen der Teilnahme Beschuldigten angeordnet werden darf.

- Die Ersetzung des Wortes „oder“ durch „sowie“ in Absatz 1 Nr. 1 Buchstabe b trägt dem Umstand Rechnung, dass es sich um eine kumulative Aufzählung handelt.

- Mit der stringenteren Fassung von Absatz 1 Nr. 1 Buchstabe c sind keine inhaltlichen Änderungen verbunden.

- Die Ersetzung des bisherigen Absatzes 6 Satz 3 durch einen Verweis auf § 53b Abs. 4 StPO-E passt die bisherige Verstrickungsregelung an die allgemeine und – im Hinblick auf das neue Erfordernis, dass der Verstrickungsverdacht bereits zur Einleitung eines Ermittlungsverfahrens gegen den Berufsgeheimnisträger geführt haben muss – engere Verstrickungsregelung in § 53b Abs. 4 StPO-E an.

Zu Nummer 9 (§100d StPO-E)

Auch in § 100d StPO werden lediglich redaktionelle Änderungen vorgenommen:

- Absatz 2 Satz 2 Nr. 1 wird durch die Ersetzung des Wortes „bekannt“ durch das Wort „möglich“ an § 100b Abs. 2 Satz 2 Nr. 2 StPO-E angepasst, ohne dass damit eine inhaltliche Änderung verbunden ist.

- Der bisherige Absatz 5 entfällt, da die darin enthaltene Vernichtungsregelung nun in der allgemeinen Vorschrift des § 101 Abs. 10 StPO-E enthalten ist.

- Der bisherige Absatz 6, der zu Absatz 5 wird, wird an einzelnen Detailstellen im Hinblick auf die im Datenschutzrecht gefestigten Begrifflichkeiten terminologisch überarbeitet, ohne dass damit inhaltliche Veränderungen verbunden sind.

- Die bisherigen Absätze 7 bis 10 entfallen, weil ihr Regelungsgehalt (Kennzeichnung, Benachrichtigung, nachträglicher Rechtsschutz) nunmehr in der für alle verdeckten Ermittlungsmaßnahmen geltenden Vorschrift des § 101 Abs. 3, 4 bis 9 StPO-E enthalten ist.

Zu Nummer 10 (§100e StPO-E)

Die Regelung zur Erstellung von (statistischen) Berichten über Anordnungen zur akustischen Wohnraumüberwachung in Absatz 1 wird durch die Bezugnahme in Satz 1 auf den neuen § 100b Abs. 5 StPO-E kürzer gefasst. Satz 2 stellt klar, dass die Bundesregierung zur Erfüllung ihrer Berichtspflicht nach Artikel 13 Abs. 6 GG dem Deutschen Bundestag weiterhin jährlich über nach § 100c StPO angeordnete Maßnahmen berichtet. Der Bericht an den Deutschen Bundestag hat, wie eingangs des Satzes 2 ausdrücklich klargestellt ist, zeitlich vor der vom Bundesamt für Justiz nach § 100b Abs. 5 Satz 2 StPO-E vorzunehmenden Veröffentlichung der Übersicht im Internet zu erfolgen. Er findet, der bisherigen Handhabung entsprechend, Eingang in eine Bundestagsdrucksache. Die Veröffentlichung der Übersicht durch das Bundesamt für Justiz kann daher, soweit sich dies als praktisch erweist, auch durch eine Verlinkung auf die Internetseite des Deutschen Bundestages, auf der die Bundestagsdrucksachen eingestellt werden, erfolgen.

In Absatz 2 Nr. 8 wird lediglich eine redaktionelle Folgeänderung vorgenommen, die daraus resultiert, dass die in Bezug genommenen Regelungen über die Benachrichtigung bei der akustischen Wohnraumüberwachung künftig nicht mehr in § 100d Abs. 8 StPO enthalten sind, sondern sich aus der allgemeinen Vorschrift des § 101 Abs. 4 ff. StPO-E ergeben.

Zu Nummer 11 (§§ 100f bis 101 StPO-E)

Zu § 100f StPO-E

Den Vorschriften zur akustischen Wohnraumüberwachung in §§ 100c bis 100e StPO nachfolgend regelt § 100f StPO-E künftig nur noch die akustische Überwachung außerhalb von Wohnungen. Die in § 100f StPO bislang enthaltenen Regelungen zu Bildaufnahmen und technischen Observationsmitteln werden in § 100h StPO-E eingestellt.

- Der bisherige Absatz 1 entfällt, da sein Regelungsgehalt in § 100h StPO-E eingeht.

- Der bisherige Absatz 2 Satz 1 wird daher zu Absatz 1 Satz 1 und im Eingangswortlaut („Auch ohne“) redaktionell an § 100a Abs. 1 und § 100c StPO-E angepasst (vgl. die dortigen Erläuterungen).

- Die bisher in § 100f Abs. 2 Satz 2 und 3 StPO enthaltenen Verfahrensregelungen werden durch einen Verweis im neuen Absatz 4 auf § 100b Abs. 1, 4 Satz1 und § 100d Abs. 2 StPO-E ersetzt. Damit werden die hinsichtlich ihrer Eingriffstiefe vergleichbaren Maßnahmen der Telekommunikationsüberwachung und der Überwachung des gesprochenen Worts außerhalb von Wohnungen verfahrensmäßig einander angeglichen:

  − Die Regelung der Anordnungskompetenz im bisherigen Absatz 2 Satz 2 (bislang: Richtervorbehalt; in Eilfällen Anordnung durch Staatsanwaltschaft oder Ermittlungspersonen) wird durch einen generellen Verweis in Absatz 4 auf § 100b Abs. 1 StPO-E ersetzt, was in der Gesamtschau der verdeckten Ermittlungsmaßnahmen der Eingriffsintensität der Überwachung des nicht öffentlich gesprochenen Wortes angemessener erscheint. Die Ermittlungspersonen der Staatsanwaltschaft (§ 152 GVG) haben danach auch bei Gefahr in Verzug künftig keine Anordnungskompetenz mehr.

  − Der bisherige Verweis in § 100f Abs. 2 Satz 3 auf § 98b Abs. 1 Satz 2 StPO entfällt, weil er systematisch unpassend und unklar erscheint und neben dem – nunmehr in Absatz 4 eingestellten – Verweis auf § 100b Abs. 1 Satz 3 StPO-E keine eigenständige Bedeutung hat.

  − Hinsichtlich der formellen Anforderungen an die Anordnung wird nicht mehr auf § 100b Abs. 2 StPO, sondern auf den insofern sachnäheren § 100d Abs. 2 StPO verwiesen.

- Der Verweis auf § 100b Abs. 4 Satz 1 StPO-E (Abbruch der Maßnahme bei Wegfall der Anordnungsvoraussetzungen) wird beibehalten.

- Die in § 100f Abs. 2 StPO durch Verweis auf § 100b Abs. 6 StPO geregelte Löschungspflicht wird künftig durch den Verweis auf die Regelungen des § 101 StPO-E sichergestellt, der die Maßnahme nach § 100f StPO-E zudem den dortigen Kennzeichnungs- und Benachrichtigungspflichten unterstellt (vgl. Begründung zu § 101 StPO-E).

- Der bisherige Absatz 3 Satz 1 findet sich im neuen Absatz 2 Satz 1.

- Der bisherige Absatz 3 Satz 2 entfällt, da sein Regelungsgehalt die nunmehr in § 100h StPO-E geregelten Bildaufnahmen betrifft.

- Der bisherige Absatz 3 Satz 3 findet sich in redaktionell angepasster Weise im neuen Absatz 2 Satz 2.

- Der bisherige Absatz 4 findet sich im neuen Absatz 3, der hinsichtlich mitbetroffener Personen die Formulierung des § 163f Abs. 2 StPO übernimmt („Dritte“ statt „andere Personen“).

- Der bisherige Absatz 5 entfällt, weil sein Regelungsgehalt (Verwendungsregelung) sich nunmehr in § 477 Abs. 2 Satz 2 StPO-E findet.

Zu § 100g StPO-E

§ 100g StPO wird umfassend neu gefasst, um den Vorgaben und Konsequenzen aus der Richtlinie zur so genannten „Vorratsdatenspeicherung“ vom 15. März 2006 (2006/24/EG), des Übereinkommens des Europarats über Computerkriminalität vom 23. November 2001 (SEV Nr. 185) und verfassungsrechtlichen Vorgaben Rechnung zu tragen.

Zu § 100g Abs. 1 StPO-E

Absatz 1 wird in Anlehnung an § 100a Abs. 1 StPO-E als allgemeine Befugnis zur Erhebung von Verkehrsdaten ausgestaltet und schafft damit die von Artikel 20 des Übereinkommens über Computerkriminalität geforderte Möglichkeit einer Echtzeiterhebung von Verkehrsdaten.

1. Nach bisheriger Rechtslage enthält die Vorschrift lediglich eine Befugnis der Strafverfolgungsbehörden, Auskunft über gespeicherte Verbindungsdaten (zu den Begriffen der Verbindungsdaten und der Verkehrsdaten vgl. unten 2.) von denjenigen zu verlangen, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken. Die Erhebung von Verkehrsdaten in Echtzeit ist hingegen bisher nur unter den Voraussetzungen der §§ 100a, 100b StPO zulässig, während die nicht in Echtzeit erfolgende Auskunft sowohl über in der Vergangenheit angefallene als auch künftig anfallende Verkehrsdaten nach § 100g Abs. 1 StPO angeordnet werden darf. Diese unterschiedliche Behandlung der Erlangung von beim Diensteanbieter gespeicherten Verkehrsdaten, deren Echtzeiterhebung und der Auskunft über zukünftig anfallende Verkehrsdaten erscheint unnötig schwierig und in der Sache nicht gerechtfertigt. Maßgeblich für die Beurteilung der Eingriffsintensität von Ermittlungsmaßnahmen im Zusammenhang mit Telekommunikationsvorgängen ist die Qualität der erlangten Daten, also der Umstand, ob diese Auskunft über Inhalte der überwachten Kommunikation geben oder lediglich über deren äußere Umstände oder gar nur über Umstände, die keinen konkreten Telekommunikationsvorgang betreffen, wie dies etwa bei der Erhebung von Standortdaten eines lediglich betriebsbereiten aber nicht genutzten Mobiltelefons der Fall ist. An diese Differenzierung knüpft auch die Rechtsprechung des Bundesverfassungsgerichts an (vgl. BVerfGE 67, 157, 172; 100, 313, 358 f.; 107, 299, 312 f.; 110, 33, 52 f., 68 f.; BVerfG, 1 BvR 668/04 vom 27. Juli 2005, Absatz-Nr. 81, und 2 BvR 1345/03). § 100g StPO wird daher nicht mehr allein als Regelung eines Auskunftsanspruchs gegenüber Telekommunikationsdiensteanbietern sondern als umfassende Erhebungsbefugnis für Verkehrsdaten ausgestaltet. Damit wird zugleich Artikel 20 Abs. 1 Buchstabe a des Übereinkommens über Computerkriminalität Rechnung getragen, der die Ermöglichung einer Erhebung von Verkehrsdaten in Echtzeit verlangt.

   Eine Beschränkung dieser Möglichkeit auf bestimmte Straftaten ist dort nicht vorgesehen, wäre aber aufgrund der Vorbehaltsmöglichkeit nach Artikel 20 Abs. 4 i. V. m. Artikel 14 Abs. 3 Buchstabe a des Übereinkommens grundsätzlich möglich. Die bisherige deutsche Regelung einer Gleichbehandlung der Echtzeiterhebung von Verkehrsdaten und Daten über den Inhalt einer Telekommunikation nach Maßgabe des § 100a StPO würde zugleich die äußerste Grenze eines nach Artikel 14 Abs. 3 Buchstabe b des Übereinkommens zulässigen Vorbehalts darstellen. Allerdings haben sich die Vertragsparteien in Artikel 14 Abs. 2 Satz 5 des Übereinkommens verpflichtet, die Möglichkeit zu prüfen, einen solchen Vorbehalt zu beschränken, damit die Erhebung von Verkehrsdaten in Echtzeit im weitest möglichen Umfang angewendet werden kann.

Eine im Sinne dieser Vorbehaltsoption mögliche Beschränkung der Echtzeiterhebung von Verkehrsdaten entsprechend den Regelungen zur Erhebung von Inhaltsdaten im Sinne des § 100a StPO ist nach deutschem Recht aufgrund der unterschiedlichen Eingriffsintensität beider Maßnahmen verfassungsrechtlich nicht geboten. Die bereits bisher in § 100g Abs. 1 StPO enthaltenen – und zumal die aufgrund des gegenständlichen Entwurfs hinzukommenden – materiellen Beschränkungen der Auskunftserlangung über Verkehrsdaten gewährleisten vielmehr auch hinsichtlich der Erhebung von Verkehrsdaten in Echtzeit eine ausreichende Begrenzung der Maßnahme. Hinzu kommt, dass durch die Harmonisierung des § 100g StPO-E mit den Verfahrensregelungen in den §§ 100b, 101 StPO-E auch bei der Erhebung von Verkehrsdaten der Rechtsschutz Betroffener gegenüber der bisherigen Rechtslage deutlich verbessert wird. Zu den vorgesehenen Beschränkungen des § 100g StPO im Hinblick auf die Regelungen zur so genannten „Vorratsdatenspeicherung“ vgl. die nachfolgenden Erläuterungen unter Punkt 5.

Mit der Ausgestaltung des § 100g Abs. 1 Satz 1 StPO-E als umfassende Befugnis zur Erhebung von Verkehrsdaten entfällt nicht die bislang ausdrücklich in § 100g Abs. 1 StPO enthaltene Auskunftsverpflichtung der Diensteanbieter. Deren Pflicht zur Mitwirkung an einer Ausleitung der Verkehrsdaten in Echtzeit oder zur Auskunftserteilung über gespeicherte Verkehrsdaten folgt vielmehr aus dem Verweis in § 100g Abs. 2 Satz 1 auf § 100b Abs. 3 StPO-E. Hiernach kann über gespeicherte Verkehrsdaten, die Telekommunikationsvorgänge aus der Vergangenheit betreffen, (im Rahmen des Erforderlichen) unbeschränkt Auskunft verlangt werden. Auch kann hiernach weiterhin Auskunft über zukünftig anfallende Verkehrsdaten verlangt werden; insoweit sind allerdings die nach § 100g Abs. 2 Satz 1 i. V. m. § 100b Abs. 1 StPO-E geltenden Anordnungsfristen zu beachten. Für zukünftig anfallende Verkehrsdaten sieht die Regelung daher zwei Möglichkeiten der Erhebung durch die Strafverfolgungsbehörden vor: Zum einen ist es zulässig, diese Daten in Echtzeit zu erheben, d. h. „live“ vom Telekommunikationsdienstleister an die Strafverfolgungsbehörden ausleiten zu lassen; zum anderen kann die Erhebung auch weiterhin in der Weise erfolgen, dass die nach dem Zeitpunkt der Anordnung anfallenden Verkehrsdaten in bestimmten Zeitabständen gebündelt an die Strafverfolgungsbehörde beauskunftet werden.

§ 100g Abs. 1 Satz 1 StPO-E gilt darüber hinaus aus den bereits zu § 100b Abs. 3 StPO-E dargelegten Gründen nicht nur für Verkehrsdaten, die bei Personen oder Stellen gespeichert sind, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken, sondern auch für solche Personen und Stellen, die diese Dienste

nicht geschäftsmäßig erbringen. Denn die Erforderlichkeit der Erhebung von Verkehrsdaten für Strafverfolgungszwecke wird nicht dadurch beseitigt, dass die Telekommunikationsdienste nicht geschäftsmäßig erbracht werden. Entscheidend ist, dass die Daten, die sich im Herrschaftsbereich eines Telekommunikationsdiensteanbieters befinden, dem von Artikel 10 GG geschützten Telekommunikationsvorgang zuzurechnen sind und § 100g StPO-E daher eine verfassungskonforme Rechtsgrundlage für die Erhebung dieser Daten schafft. Ob und ggf. welche Vorkehrungen der jeweilige Telekommunikationsdiensteerbringer dafür zu treffen hat, dass bei einer Anforderung durch die Strafverfolgungsbehörden die Beauskunftung von Verkehrsdaten auch tatsächlich möglich ist, regelt § 100g StPO-E nicht; diese Frage bestimmt sich vielmehr nach den telekommunikationsrechtlichen Vorschriften, wie etwa dem Telekommunikationsgesetz (z. B. § 113a TKG-E) oder – dem künftigen – Inhalt der Telekommunikations-Überwachungsverordnung.

2. Entsprechend den Vorgaben des Übereinkommens über Computerkriminalität und dem im modernen Telekommunikationsrecht üblichen Sprachgebrauch wird der bislang in § 100g StPO verwandte Begriff der „Telekommunikationsverbindungsdaten“ durch den in § 96 Abs. 1 TKG verwendeten und in § 3 Nr. 30 TKG gesetzlich definierten, umfassenderen Begriff „Verkehrsdaten“ (Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden) ersetzt. Da Absatz 1 Satz 1 hinsichtlich der Daten, deren Erhebung zulässig ist, allgemein auf § 96 Abs. 1 TKG verweist, kann zudem die bisherige Definition der Verkehrsdaten in § 100g Abs. 3 StPO entfallen. Dieser Vereinfachung liegt der allgemeine Gedanke zugrunde, dass Verkehrsdaten, die der Diensteanbieter für seine Zwecke erheben darf, auch – unter den vorgesehenen engen Voraussetzungen – von den Strafverfolgungsbehörden erhoben werden dürfen. Der Verweis auf § 96 Abs. 1 TKG geht insofern über § 100g Abs. 3 StPO hinaus, als dort personenbezogene Berechtigungskennungen (§ 96 Abs. 1 Nr. 1 TKG), abrechnungsrelevante übermittelte Datenmengen (§ 96 Abs. 1 Nr. 2 und 4 TKG) und sonstige, zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendige Verkehrsdaten (§ 96 Abs. 1 Nr. 5 TKG) nicht erwähnt sind. Eine weitreichende Ausweitung der Erhebungsbefugnis ist hiermit nicht verbunden:

   - Personenbezogene Berechtigungskennungen (§ 96 Abs. 1 Nr. 1 TKG) können bereits nach der insoweit speziellen Vorschrift des § 113 Abs. 1 Satz 2 TKG unter den dortigen – weiter gefassten Voraussetzungen – erhoben werden.

- Abrechnungsrelevante übermittelte Datenmengen (§ 96 Abs.1 Nr. 2 und 4 TKG) lassen einen Rückschluss auf die Kommunikationsinhalte nur in ähnlicher Weise zu, wie dies auch aufgrund der Kenntnis der Verbindungsdauer möglich ist.

- Die Einbeziehung der sonstigen, zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendigen Verkehrsdaten (§ 96 Abs. 1 Nr. 5 TKG), ist zur Aufklärung von Straftaten erforderlich. Bei dem Verdacht einer in betrügerischer Weise manipulierten Entgeltabrechnung kann sich andernfalls die Situation ergeben, dass dieser Verdacht nicht hinreichend aufgeklärt werden kann, weil es an einer Befugnis zur Erhebung der sonstigen zur Entgeltabrechnung notwendigen Verkehrsdaten fehlt. Darüber hinaus ist der Bereich der Telekommunikation von einem rasanten technischen Fortschritt gekennzeichnet, so dass es sich schon aus diesem Grunde empfiehlt, die Erhebungsbefugnis in § 100g Abs. 1 StPO-E durch die Einbeziehung der in § 96 Abs. 1 Nr. 5 TKG genannten „sonstigen Verkehrsdaten“ technikoffen zu gestalten, um der fortschreitenden Entwicklung im Bereich der Telekommunikation folgen zu können.

3. Die Erhebungsbefugnis nach § 100g StPO-E setzt ferner nicht mehr, wie § 100g Abs. 3 StPO durch die Formulierung „im Falle einer Verbindung“ kenntlich gemacht hat, eine bestehende Kommunikationsverbindung voraus. Die Neuregelung kann damit im Falle der Erhebung von Standortdaten die – rechtlich umstrittene – Übersendung einer so genannten „stillen SMS“ („Stealth-Ping-Verfahren“) entbehrlich machen, so dass – z. B. zur Ermöglichung oder Erleichterung von Observationsmaßnahmen – die Standortdaten eines eingeschalteten Mobiltelefons auch dann in Echtzeit erhoben werden können, wenn dieses aktuell nicht genutzt wird. Eine solche die Strafverfolgung erheblich effektivierende Möglichkeit wird aus Gründen der Verhältnismäßigkeit allerdings nur bei Straftaten von erheblicher Bedeutung im Sinne des Absatzes 1 Satz 1 Nr. 1 StPO-E eröffnet; dies wird durch Absatz 1 Satz 3 ausdrücklich klargestellt. Zur Vereinbarkeit dieser Beschränkung mit den Vorgaben des Übereinkommens des Europarats über Computerkriminalität vgl. im Einzelnen oben unter V. letzter Absatz.

4. Die bislang in § 100g StPO enthaltene Voraussetzung, dass die Maßnahme für die Untersuchung erforderlich sein muss, wird entsprechend den Formulierungen in anderen speziellen Befugnisnormen (z. B. in § 100a Abs. 1 StPO-E) dahin präzisiert, dass die Erhebung der Verkehrsdaten für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich sein muss.

5. § 100g Abs. 1 StPO-E beinhaltet auch künftig zwei Kategorien von Straftaten, die die Erhebung von Verkehrsdaten rechtfertigen: Straftaten von erheblicher Bedeutung und mittels Telekommunikation begangene Straftaten.

   a) Zur Fallgruppe der Straftaten von erheblicher Bedeutung (Absatz 1 Satz 1 Nr. 1) wird entsprechend den Vorgaben des Bundesverfassungsgerichts im neuen Wortlaut klargestellt, dass die Straftat nicht nur abstrakt – etwa unter Berücksichtigung des gesetzlichen Strafrahmens – sondern auch im Einzelfall von erheblicher Bedeutung sein muss (vgl. BVerfGE 107, 299, 322; sowie die obigen Erläuterungen zu § 100a Abs. 1 Nr. 2 StPO-E).

   b) Die Beschreibung der bisherigen Fallgruppe der „mittels einer Endeinrichtung“ begangenen Straftaten – bei wortlautgetreuem Verständnis wäre darunter auch der Einsatz des Endgerätes zur Begehung von Körperverletzungen zu subsumieren – wird sprachlich dahingehend präzisiert, dass die Straftat „mittels Telekommunikation“ begangenen sein muss (Absatz 1 Satz 1 Nr. 2). Dass der Gesetzgeber im Falle einer mittels Telekommunikation begangenen Straftat die Erhebung von Verkehrsdaten auch dann vorsieht, wenn die Straftat nicht von erheblicher Bedeutung ist, begegnet keinen verfassungsrechtlichen Bedenken (so ausdrücklich: BVerfG, 2 BvR 1085/05 vom 17.6.2006, Absatz-Nr. 17).

      Auch unter Berücksichtigung dieser verfassungsgerichtlichen Rechtsprechung empfiehlt sich jedoch für diese Fallgruppe, für die bislang außer dem allgemeinen Verhältnismäßigkeitsgrundsatz keine einschränkenden Merkmale im Hinblick auf die Schwere oder Erheblichkeit der Anlassstraftat geregelt sind, zur Gewährleistung einer in der Gesamtschau mit den Regelungen zur so genannten „Vorratsdatenspeicherung“ (Artikel 2, §§ 113a, 113b TKG-E) verhältnismäßigen Befugnisnorm eine Modifizierung in mehrfacher Weise:

      - Zum einen findet diese Fallgruppe künftig nur noch Anwendung, wenn die mittels Telekommunikation begangene Straftat vollendet ist. Straftaten mittels Telekommunikation, die lediglich in das Versuchsstadium gelangen oder gar nur in strafbarer Weise vorbereitet werden, werden damit von dieser Fallgruppe nicht mehr erfasst. Sofern es sich jedoch bei der aufzuklärenden Straftat um eine solche von erheblicher Bedeutung handelt, kann sie als solche eine Verkehrsdatenerhebung nach Satz 1 Nr. 1 rechtfertigen.

- Ferner wird die Erhebung von Verkehrsdaten bei mittels Telekommunikation begangenen Straftaten nach § 100g Abs. 1 Satz 2 StPO-E künftig nur noch dann zulässig sein, wenn ohne die Erhebung der Verkehrsdaten die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten aussichtslos wäre. Durch diese strenge Subsidiaritätsklausel wird dem Verhältnismäßigkeitsgrundsatz in besonderer Weise Rechnung getragen. Dies ist angezeigt, weil die Verkehrsdatenerhebung durch die Ausweitung des mit der „Vorratsdatenspeicherung“ einhergehenden Datenvolumens insgesamt an Eingriffsintensität gewinnt und daher in der vorliegenden Fallgruppe nur gerechtfertigt erscheint, wenn andere – zulässige – Ermittlungsmöglichkeiten fehlen oder mit hoher Wahrscheinlichkeit keinen Erfolg versprechen (vgl. zum Begriff der Aussichtslosigkeit und zum Verhältnis unterschiedlicher Subsidiaritätsklauseln zueinander Schäfer, a. a. O., § 110a, Rn. 30 f.). Es bedarf daher künftig einer Einzelfallprüfung, ob alternative Ermittlungsmaßnahmen in Betracht kommen oder eine Verkehrsdatenerhebung das einzig zielführende und zugleich verhältnismäßige Mittel ist. Für eine Vielzahl der Fälle, z. B. bei einer telefonischen Bedrohung, werden gleich geeignete, aber weniger belastende Ermittlungsmaßnahmen oftmals nicht zur Verfügung stehen, wenn außer dem Zeitpunkt des Anrufs keine weiteren Ermittlungsansätze gegeben sind. Für diese Fälle, die etwa dem Bereich des so genannten „Stalking“ entstammen, ist die Verkehrsdatenerhebung ein unverzichtbares – weil regelmäßig alternativloses – Ermittlungsinstrument.

- Zusätzlich wird – ebenfalls als Ausprägung des Verhältnismäßigkeitsgrundsatzes – diese Fallgruppe dahingehend eingeschränkt, dass eine Erhebung von Verkehrsdaten nur dann zulässig ist, wenn sie in einem angemessenen Verhältnis zur Bedeutung der Sache steht. Im Hinblick auf die Schwere des mit der „Vorratsdatenspeicherung“ verbundenen Grundrechtseingriffs soll damit der Bereich der leichteren Kriminalität aus dem Anwendungsbereich der Erhebungsbefugnis auch für den Fall ausgenommen werden, dass die Tat auf andere Weise nicht aufklärbar ist. Dies erlangt etwa Bedeutung für einzelne mittels Telekommunikation begangene geringfügige Beleidigungstaten.

Diese aus Verhältnismäßigkeitsgründen vorgesehenen Beschränkungen erlauben es, in beiden Fallgruppen des § 100g Abs. 1 eine Erhebung der nach § 113a TKG(-E) gespeicherten so genannten „Vorratsdaten“ zuzulassen. Dies wird durch

die Bezugnahme in dem Klammerzusatz in Satz 1 auch auf § 113a TKG(-E) klargestellt.

Diese Ausgestaltung der Erhebungsbefugnis in § 100g Abs. 1 StPO-E steht auch in Einklang mit Artikel 1 Abs. 1 der Richtlinie zur „Vorratsdatenspeicherung“. Nach dieser Regelung haben die Mitgliedstaaten sicherzustellen, dass die „auf Vorrat“ zu speichernden Verkehrsdaten zum Zwecke der Ermittlung, Feststellung und Verfolgung von „schweren Straftaten“ („serious crime“) im Sinne des einzelstaatlichen Rechts jedes Mitgliedstaates zur Verfügung stehen. Nach der hierzu vom Ministerrat für Justiz und Inneres am 21. Februar 2006 angenommenen Erklärung zu Artikel 1 Abs. 1 der Richtlinie haben die Mitgliedstaaten bei der Definition des Begriffs „schwere Straftat“ im einzelstaatlichen Recht die in Artikel 2 Abs. 2 des Rahmenbeschlusses des Rates über den Europäischen Haftbefehl genannten Straftaten (das sind Straftaten, die mit einer Freiheitsstrafe oder einer freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens drei Jahren bedroht sind) sowie Straftaten unter Einsatz von Telekommunikationseinrichtungen angemessen zu berücksichtigen. Diesen Vorgaben wird in § 100g Abs. 1 StPO-E durch die Anknüpfung an eine Straftat von erheblicher Bedeutung bzw. an eine mittels Telekommunikation begangene Straftat Rechnung getragen. Hierbei ist zu berücksichtigen, dass der Begriff „serious crime“, der sich in der englischen Textfassung von Artikel 1 der Richtlinie 2006/24/EG findet, in der deutschen Textfassung zwar – wenig glücklich – mit „schwere Straftat“ übersetzt worden ist, im europäischen Kontext aber nicht dieselbe Bedeutung hat, wie der nunmehr in § 100a StPO-E verwandte Begriff der „schweren Straftat“. Während bei § 100a StPO-E eine schwere Straftat im Hinblick auf den Strafrahmen regelmäßig eine Mindesthöchststrafe von fünf Jahren Freiheitsstrafe voraussetzt (vgl. die Erläuterungen zu § 100a Abs. 1 StPO-E), dient dieser Begriff in europäischen Rechtsinstrumenten regelmäßig dazu, Tatbestände auszugrenzen, die lediglich die Schwere von Ordnungswidrigkeiten oder von Bagatellkriminalität erreichen. Dies ist vor dem Hintergrund zu sehen, dass nicht alle Mitgliedstaaten die im deutschen Recht stattgehabte Herabstufung von ehedem strafbaren Verhalten zu Ordnungswidrigkeiten vollzogen haben. Der Begriff „serious crime“ ist daher im europäischen Rechtskontext eher im Sinne einer „ernsthaften Straftat“ zu übersetzen als mit schwerer Kriminalität zu assoziieren.

Dies zeigt auch ein Vergleich mit anderen Rechtsakten im europäischen Rechtsraum:

So macht beispielsweise Artikel 99 Abs. 2 Buchstabe a des Schengener Durchführungsübereinkommens (SDÜ) eine Ausschreibung zur Strafverfolgung von dem Vorlie-

gen „extremely serious criminal offences“ abhängig, was in der deutschen Textfassung zwar mit „außergewöhnlich schweren Straftat“ übersetzt wird, dabei aber unstreitig nicht als „besonders schweren Straftat“ etwa im Sinne des Artikels 13 Abs. 3 GG bzw. des § 100c StPO zu verstehen ist. Der deutsche Gesetzgeber hat, wie die Regelung in § 163e StPO zeigt, „extremely serious criminal offences“ im deutschen Rechtssystem den Straftaten von erheblicher Bedeutung zugeordnet.

Die Europäische Kommission geht von einer im Sinne des Europäischen Rechts schweren Straftat dann aus, wenn für ihre Begehung eine Freiheitsstrafe von im Höchstmaß mindestens einem Jahr angedroht ist. Dies zeigen etwa die Erläuterungen der Kommission zum Europäischen Haftbefehl, wonach Letzterer bei schweren Straftaten erlassen werden kann: „Ziel des Europäischen Haftbefehls ist es, langwierige Auslieferungsverfahren durch eine neue und effiziente Art der Rückführung von Personen zu ersetzen, die entweder einer schweren Straftat verdächtig sind oder bereits für eine schwere Straftat verurteilt wurden und sich ins Ausland abgesetzt haben.“ (vgl. http://ec.europa.eu/justice_home/fsj/criminal/extradition/fsj_criminal_extradition_de.htm). Nach Artikel 2 Abs. 1 des Rahmenbeschlusses des Rates vom 13. Juni 2002 über den Europäischen Haftbefehl und die Übergabeverfahren zwischen den Mitgliedstaaten – 2002/584/JI (ABl. EU Nr. L 190 S. 1) – kann ein Europäischer Haftbefehl bei Handlungen erlassen werden, die nach den Rechtsvorschriften des Ausstellungsmitgliedstaats mit einer Freiheitsstrafe oder einer freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens zwölf Monaten bedroht sind, oder im Falle einer Verurteilung zu einer Strafe oder der Anordnung einer Maßregel der Sicherung, deren Maß mindestens vier Monate beträgt.

Im Ergebnis sieht § 100g Abs. 1 StPO-E unter Würdigung der vorstehenden Hinweise jedenfalls keine Schwelle unterhalb von „serious crime“ vor. Im Übrigen ist zu bedenken, dass Artikel 1 der Richtlinie 2006/24/EG keine Schwelle für den Zugriff auf die zu speichernden Daten vorgibt, sondern lediglich den Zweck der Richtlinie umschreibt. Dem Zugang zu den zu speichernden Daten gewidmet ist vielmehr Artikel 4 der Richtlinie, der die Regelung des Zugangs dem Recht der Mitgliedstaaten überlässt und lediglich sichergestellt wissen will, dass dabei die einschlägigen Bestimmungen der Europäischen Union und des Völkerrechts sowie den Anforderungen der Notwendigkeit und der Verhältnismäßigkeit einzuhalten sind. Dem trägt die in besonderer Weise am Verhältnismäßigkeitsgrundsatz orientierte Ausgestaltung der Erhebungsbefugnisse nach § 100g Abs. 1 StPO-E Rechnung. Sie steht auch nicht in Widerspruch zu den Vorgaben des Übereinkommens über Computerkriminalität; denn eine am Verhältnis-

mäßigkeitsgrundsatz orientierte Ausgestaltung des innerstaatlichen Rechts ist von Artikel 15 Abs. 1 dieses Übereinkommens ausdrücklich gefordert.

6. Nicht aufgenommen wurde in § 100g Abs. 1 StPO-E die von Artikel 16 Abs. 2 des Übereinkommens über Computerkriminalität geforderte Möglichkeit des „Einfrierens“ von Verkehrsdaten bei den speichernden Personen und Stellen (so genanntes „Quick Freezing“). Denn eine solche Regelung ist vor allem aufgrund der zugleich umzusetzenden Richtlinie zur „Vorratsdatenspeicherung“ entbehrlich geworden: Die Daten, die aufgrund einer solchen Speicherungsanordnung „einzufrieren“ wären, werden – soweit sie für die Strafverfolgung regelmäßig von Relevanz sind – künftig bereits aufgrund der in § 113a TKG-E (Artikel 2 dieses Gesetzes) vorgesehenen Speicherungspflichten aufbewahrt. Darüber hinaus besteht aufgrund der Eilfallkompetenz der Staatsanwaltschaft (§ 100g Abs. 2 i. V. m. § 100b Abs. 1 Satz 2 StPO-E) die Möglichkeit, sehr kurzfristig auf vorhandene Verkehrsdaten zuzugreifen und so deren Löschung durch die Diensteanbieter vorzubeugen.

   Würde allerdings, wie dies in der rechtspolitischen Diskussion zum Teil erwogen wird, was der Entwurf aber aus den vorstehend zu Nummer 5 sowie aus den nachfolgend dargelegten praktischen Gründen nicht vorsieht, die Erhebung von Verkehrsdaten, die ausschließlich nach Maßgabe der Richtlinie 2006/24/EG „auf Vorrat“ gespeichert werden, nur noch bei Straftaten von erheblicher Bedeutung oder gar nur bei schweren Straftaten i. S. v. § 100a Abs. 1 Nr. 2, Abs. 2 StPO-E vorgesehen, müsste für die übrigen Straftaten – insbesondere also diejenigen, die mittels Telekommunikation begangen wurden, die geforderte Erheblichkeitsschwelle aber nicht überschreiten – die Möglichkeit einer Speicherungsanordnung aufgrund von Artikel 16 des Übereinkommens über Computerkriminalität geschaffen werden. Denn nach Artikel 14 Abs. 2 Buchstabe b des Übereinkommens sind die darin vorgesehenen Befugnisse und Verfahren – mithin auch die in Artikel 16 vorgesehene Speicherungsanordnung nebst der in Artikel 17 vorgegebenen Erhebungsbefugnis für die zuständigen Behörden – insbesondere auch hinsichtlich solcher Straftaten vorzusehen, die in den Artikeln 2 bis 11 des Übereinkommens umschrieben sind (dazu zählen z. B. Straftaten im Zusammenhang mit der Verletzung des Urheberrechts und verwandter Schutzrechte, Artikel 10 des Übereinkommens) oder die mittels eines Computersystems (und damit regelmäßig mittels Telekommunikation) begangen wurden. Eine Beschränkung der Erhebung von „auf Vorrat“ gespeicherten Verkehrsdaten auf Straftaten von erheblicher Bedeutung würde damit – je nach konkreter gesetzlicher Ausgestaltung – zu einem (technisch ggf. aufwändigen) Nebeneinander (z. B. infolge getrennter Speicherungssysteme) oder zu ei-

nem nicht unkomplizierten Ineinandergreifen von „Vorratsdatenspeicherung“ und Speicherungsanordnung führen. Es erscheint sachgerecht, dieses – auch in der praktischen Umsetzung durch die Diensteanbieter voraussichtlich aufwändigere – Nebeneinander oder Ineinandergreifen zu vermeiden, indem zwar auch bei mittels Telekommunikation begangenen Straftaten ein Zugriff auf die „auf Vorrat“ gespeicherten Verkehrsdaten im Grundsatz erlaubt wird, die Erhebungsbefugnis insoweit aber enger als bislang gefasst wird. Dem tragen die oben dargestellten Modifizierungen (Subsidiaritäts- und besondere Verhältnismäßigkeitsklausel, Ausschluss von Versuchs- und Vorbereitungsstraftaten) Rechnung.

Zu § 100g Abs. 2 StPO-E

Die bisher in § 100g Abs. 2 StPO ausdrücklich getroffene Regelung zur so genannten Zielwahlsuche, mit der durch Abgleich aller in einem bestimmten Zeitraum bei den Diensteanbietern angefallenen Verkehrsdatensätze ermittelt wird, von welchem – unbekannten – Anschluss aus eine Verbindung zu einem bestimmten – bekannten – Anschluss hergestellt worden ist, entfällt:

- Zum einen werden von den Diensteanbietern, die Telekommunikationsdienste für die Öffentlichkeit erbringen, künftig auch die Rufnummern der anrufenden Anschlüsse zu speichern sein, wenn diese von ihnen verarbeitet werden (vgl. Artikel 2 Nummer 5 − § 113a Abs. 2 Nr. 1 TKG-E), so dass diese künftig regelmäßig ohne Zielwahlsuche ermittelt werden können.

- Zum anderen ist in den wenigen Fällen, in denen eine Zielwahlsuche möglicherweise künftig noch erforderlich sein könnte, diese aufgrund der allgemeinen Erhebungsbefugnis für Verkehrsdaten nach § 100g Abs. 1 StPO-E, die auch die Anordnung einer Zielwahlsuche erlaubt, weiterhin möglich. Einer besonderen Regelung im Sinne des bisherigen § 100g Abs. 2 StPO mit höheren Zulässigkeitsvoraussetzungen bedarf es für diese seltenen Fallgestaltungen nicht mehr, zumal das Bundesverfassungsgericht zwischenzeitlich entschieden hat, dass der Verkehrsdatenabgleich im Zuge einer Zielwahlsuche nur in das Fernmeldegeheimnis derjenigen eingreift, die als „Treffer“ den Strafverfolgungsbehörden mitgeteilt werden; hinsichtlich des übrigen Personenkreises erfolgt eine Beeinträchtigung subjektiver Rechte durch die Zielwahlsuche nicht (vgl. BVerfGE 100, 313, 366; 107, 299, 328).

Der neu gefasste Absatz 2 enthält einen umfassenden Verweis auf § 100a Abs. 3 und § 100b Abs. 1 bis 4 Satz 1 StPO-E und harmonisiert damit die Verfahrensregelungen bei der Ermittlung von Verkehrs- und Inhaltsdaten. Dies trägt auch dem Umstand Rechnung, dass die Echtzeiterhebung von Verkehrsdaten nunmehr unter § 100g Abs. 1 StPO-E fällt. Ferner wird durch diese Harmonisierung der Verfahrensregelungen zu §§ 100a, 100b und 100g Abs. 1 StPO-E der Regelungsgehalt dieser Vorschriften klarer strukturiert und regelungstechnisch deutlich vereinfacht, was der Rechtssicherheit und damit auch dem Rechtsschutz Betroffener zugute kommt.

Im Einzelnen regelt Satz 1:

- Der Verweis auf § 100a Abs. 3 StPO-E ersetzt den Regelungsgehalt des bisherigen § 100g Abs. 1 Satz 2 StPO (Zielpersonen der Maßnahme).

- Der Verweis auf § 100b Abs. 1 StPO-E ersetzt den Verweis auf § 100b Abs. 1 StPO in § 100h Abs. 1 Satz 3 Halbsatz 1 StPO (Anordnungskompetenz) und auf § 100b Abs. 2 Satz 4 und 5 StPO in § 100h Abs. 1 Satz 3 Halbsatz 2 StPO (Dauer der Maßnahme). Ebenso wie bei der Telekommunikationsüberwachung verkürzt sich damit die Dauer für die Anordnung einer in die Zukunft gerichteten Verkehrsdatenerhebung auf zwei Monate (§ 100b Abs. 1 Satz 4 StPO-E). Wird hingegen Auskunft über in der Vergangenheit angefallene Verkehrsdaten verlangt, so sind – wie im bisherigen Recht auch – sämtliche beim Diensteanbieter vorhandenen Verkehrsdaten zu beauskunften, ohne dass insoweit eine zeitliche Beschränkung eingreift. Dies gilt, wie der Klammerverweis in Absatz 1 Satz 1 auch auf § 113a TKG-E klarstellt, auch für die nach dem Telekommunikationsgesetz „auf Vorrat“ zu speichernden Daten.

- Der Verweis auf § 100b Abs. 2 StPO-E ersetzt den Verweis auf § 100b Abs. 2 Satz 1 und 3 StPO in § 100h Abs. 1 Satz 1 und 3 Halbsatz 1 StPO (Form und Inhalt der Anordnung).

- Der Verweis auf § 100b Abs. 3 StPO-E ist notwendig, weil § 100g Abs. 1 StPO-E nicht mehr als Auskunftsverpflichtung ausgestaltet ist, mithin die in § 100b Abs. 3 StPO-E geregelte Mitwirkungspflicht der Diensteanbieter in Bezug genommen werden muss. Zugleich wird damit der Verweis auf § 95 Abs. 2 StPO in § 100h Abs. 1 Satz 3 Halbsatz 1 StPO (Ordnungs- und Zwangsmittel bei Verweigerung der Mitwirkung) entbehrlich, weil dies bereits durch den Verweis auf § 100b Abs. 3, der seinerseits auf § 95 Abs. 2 verweist, erfasst ist.

- Der Verweis auf § 100b Abs. 4 Satz 1 StPO-E ersetzt den Verweis auf § 100b Abs. 4 Satz 1 StPO in § 100h Abs. 1 Satz 3 Halbsatz 2 StPO (Beendigung der Maßnahme bei Wegfall der Anordnungsvoraussetzungen). Die bislang für die Auskunft über zukünftige Telekommunikationsverbindungen in § 100h Abs. 1 Satz 3 Halbsatz 2 StPO i. V. m. § 100b Abs. 4 Satz 2 StPO geregelte ausdrückliche Verpflichtung, die Beendigung der Maßnahme dem Gericht und dem zur Auskunft verpflichteten Telekommunikationsdiensteanbieter mitzuteilen, entfällt. Die Pflicht zur Unterrichtung des Telekommunikationsdiensteanbieters folgt bereits aus § 100b Abs. 4 Satz 1 StPO(-E), weil die unverzügliche Beendigung der Maßnahme voraussetzt, dass die Strafverfolgungsbehörden den Telekommunikationsdiensteanbieter auffordern, keine weiteren Verkehrsdaten mehr zu übermitteln. Eine besondere Mitteilung über die Beendigung der Maßnahme an das Gericht, wie sie im geltenden Recht vorgesehen ist, erscheint nicht erforderlich, weil sie für das Gericht keine erhellenden Erkenntnisse verspricht. Die für die Telekommunikationsüberwachung insoweit vorgesehene Ausweitung der Unterrichtung des Gerichts über den Verlauf und die Ergebnisse einer Telekommunikationsüberwachungsmaßnahme (§ 100b Abs. 4 Satz 2 StPO-E) ist jedenfalls für die Verkehrsdatenerhebung nicht geboten und wäre mit ganz erheblichen zusätzlichen Belastungen für die Praxis verbunden.

- Die bislang durch Verweis in § 100h Abs. 1 Satz 3 Halbsatz 1 StPO auf § 100b Abs. 6 StPO eingreifende Vernichtungsregelung findet sich nunmehr in § 101 Abs. 10 StPO-E.

§ 100g Abs. 2 Satz 2 StPO-E übernimmt die bislang in § 100h Abs. 1 Satz 2 StPO enthaltene Regelung zur so genannten „Funkzellenabfrage“, nach der im Falle einer Straftat von erheblicher Bedeutung eine räumlich und zeitlich hinreichend bestimmte Bezeichnung der Telekommunikation genügt, wenn andernfalls die Erforschung des Sachverhalts aussichtslos oder wesentlich erschwert wäre. Hierdurch wird die Verweisung in Absatz 2 Satz 1 auf § 100b Abs. 2 Satz 2 Nr. 2 StPO-E modifiziert.

Eine im Jahr 2005 im Land Schleswig-Holstein zur Aufklärung von Brandstiftungsdelikten durchgeführte Funkzellenabfrage, die zu kontroversen Diskussion geführt hat (vgl. etwa Bizer, DuD 2005, 578), gibt Anlass zu folgenden Hinweisen:

In der Sache entbindet die Regelung zur Funkzellenabfrage (lediglich) von dem andernfalls nach § 100g Abs. 2 Satz 1 StPO-E i. V. m. § 100b Abs. 2 Satz 2 Nr. 2 StPO-E bestehenden Erfordernis, bei der Erhebung von Verkehrsdaten die Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses oder des Endgerätes anzugeben, nicht aber von der

nach § 100g Abs. 2 Satz 1 StPO-E i. V. m. § 100a Abs. 3 StPO-E zu beachtenden Voraussetzung, dass sich die Anordnung zur Verkehrsdatenerhebung nur gegen den Beschuldigten oder dessen Nachrichtenmittler richten darf. Zwar werden durch eine Funkzellenabfrage in regelmäßig unvermeidbarer Weise auch Verkehrsdaten Dritter erhoben, namentlich solcher Personen, die – ohne Beschuldigte oder Nachrichtenmittler des Beschuldigten zu sein – in der Funkzelle zu der anzugebenden Zeit mittels eines Mobiltelefons kommuniziert haben. Die Funkzellenabfrage darf aber nach der eindeutigen Regelung in § 100g Abs. 2 Satz 1 StPO-E i. V. m. § 100a Abs. 3 StPO-E nicht mit der Zielrichtung erfolgen, gerade die Verkehrsdaten dieser Personen zu erheben. Sie ist vielmehr ausgeschlossen, wenn sie allein der Ermittlung etwa von – im konkreten Fall auch nicht als Nachrichtenmittler in Betracht kommenden – Zeugen dienen soll. Ist das Ziel hingegen die Erhebung von Verkehrsdaten des – wenn auch noch unbekannten – Beschuldigten oder dessen Nachrichtenmittlers, so ist die Maßnahme – soweit die übrigen Voraussetzungen vorliegen, insbesondere die Aufklärung einer Straftat von erheblicher Bedeutung Anlass der Maßnahme ist – grundsätzlich zulässig. Im Rahmen der Verhältnismäßigkeitsprüfung ist aber insbesondere zu berücksichtigen, inwieweit dritte Personen von der Maßnahme mit betroffen werden. Die Maßnahme kann daher im Einzelfall aus Verhältnismäßigkeitsgründen zeitlich und örtlich weiter zu begrenzen sein oder muss unterbleiben, wenn eine solche Begrenzung nicht möglich ist und das Ausmaß der Betroffenheit Dritter als unangemessen erscheint. Ist die Maßnahme hingegen in rechtmäßiger Weise angeordnet und durchgeführt worden, können die mit ihr erlangten Daten auch insoweit, als sie dritte Personen betreffen, sowohl als Ermittlungsansatz als auch als Beweismittel verwertet werden.

Zu § 100g Abs. 3 StPO-E

Der Regelungsgehalt des bisherigen Absatzes 3 (Aufzählung der Verbindungsdaten im Sinne des § 100g StPO) entfällt, da § 100g Abs. 1 Satz 1 StPO-E hinsichtlich der Daten, deren Erhebung die Vorschrift regelt, auf die in § 96 Abs. 1 TKG aufgezählten Verkehrsdaten Bezug nimmt (vgl. im Einzelnen die Erläuterungen zu Absatz 1).

Die neue Regelung in Absatz 3 stellt klar, dass sich die Erhebung von Verkehrsdaten nach den allgemeinen Vorschriften, also insbesondere nach den §§ 94 ff. StPO richtet, wenn sie – etwa durch Sicherstellung von Gegenständen (z. B. elektronische Datenträger, aber auch Verbindungsnachweise in Papierform), die Aufschluss über Verkehrsdaten geben können – nach Abschluss des Kommunikationsvorgangs in anderer Weise als durch eine Auskunftsanordnung an den Diensteanbieter erfolgt. § 100g Abs. 1 und 2 StPO-E ist insoweit nicht anzuwenden. Mit dieser Klarstellung wird die durch den Kammerbeschluss des Bundesver-

fassungsgerichts vom 4. Februar 2005, 2 BvR 308/04, zeitweise hervorgerufene Unsicherheit bei der Frage beseitigt, welche Normen für die Beschlagnahme von nicht im Gewahrsam des Telekommunikationsdienstleisters befindlichen Datenträgern Anwendung finden, auf denen Verkehrsdaten gespeichert sind. Eine insoweit klare und anwendungsfreundliche Regelung ist unerlässlich, um der Strafverfolgungspraxis eine eindeutige und praktikable Befugnisnorm an die Hand zu geben, aber auch, um den – durch die §§ 94 ff. StPO nicht in minderer, sondern anderer Weise gewährleisteten – Rechtsschutz Betroffener sicherzustellen. Dies entspricht auch den verfassungsrechtlichen Vorgaben, wonach die nach Abschluss des Übertragungsvorgangs im Herrschaftsbereich des Kommunikationsteilnehmers gespeicherten Kommunikationsverbindungsdaten nicht durch Artikel 10 GG geschützt werden (so ausdrücklich: BVerfG, 2 BvR 2099/04 vom 2. März 2006, Absatz-Nr. 72 = BVerfGE 115, 166 ff.).

Zu § 100g Abs. 4 StPO-E

In § 100g Abs. 4 StPO-E sind in Umsetzung von Artikel 10 der Richtlinie 2006/24/EG Regelungen zu statistischen Berichten über die Erhebung von Verkehrsdaten nach § 100g Abs. 1 StPO-E aufgenommen worden, die systematisch an § 100b Abs. 5, 6 und § 100e StPO anknüpfen (vgl. im Einzelnen die Erläuterungen zu § 100b Abs. 5 und 6 StPO-E).

Zu § 100h StPO-E

Der bisherige Regelungsgehalt des § 100h StPO wird durch andere Vorschriften ersetzt (vgl. auch die obigen Erläuterungen zu § 100g Abs. 2 Satz 1 StPO-E):

- § 100h Abs. 1 Satz 1 StPO wird ersetzt durch den Verweis auf § 100b Abs. 2 in § 100g Abs. 2 Satz 1 StPO-E (Inhalt der Anordnung).

- § 100h Abs. 1 Satz 2 StPO, der den Inhalt der Anordnung im Falle der so genannten Funkzellenabfrage regelt, wird ersetzt durch die Regelung in § 100g Abs. 2 Satz 2 StPO-E.

- Die Verweisungen in § 100h Abs. 1 Satz 3 StPO werden ersetzt durch die Verweisungen auf § 100b Abs. 1 bis 4 Satz 1 in § 100g Abs. 2 Satz 1 StPO-E. Der Verweis auf § 100b Abs. 4 Satz 2 StPO-E entfällt (s. dazu die obigen Erläuterungen zu § 100g Abs. 2 StPO-

E). Die durch die Verweisung auf § 100b Abs. 6 StPO bislang in Bezug genommene Vernichtungsregelung findet sich nunmehr in § 101 Abs. 10 StPO-E.

- § 100h Abs. 2 StPO entfällt aufgrund der allgemeinen und umfassend geltenden Regelungen zum Schutz von Berufsgeheimnisträgern bei Ermittlungsmaßnahmen in § 53b StPO-E.

- Die Verwendungsregelung in § 100h Abs. 3 StPO entfällt aufgrund der allgemeinen Regelung in § 477 Abs. 2 Satz 2 und 3 StPO-E.

Der neue Regelungsgehalt des § 100h StPO-E enthält – in redaktionell überarbeiteter Weise – die bislang in § 100f Abs. 1, 3 und 4 StPO enthaltenen Bestimmungen zum Einsatz technischer Mittel, soweit sich diese auf Bildaufnahmen und Observationsmittel beziehen:

- § 100h Abs. 1 StPO-E entspricht inhaltlich dem bisherigen § 100f Abs. 1 StPO. Zur redaktionellen Anpassung der Eingangswörter („Auch ohne“) vgl. die Begründung zu § 100a Abs. 1 StPO-E.

- § 100h Abs. 2 Satz 1 StPO-E entspricht inhaltlich dem bisherigen § 100f Abs. 3 Satz 1 StPO.

- § 100h Abs. 2 Satz 2 Nr. 1 StPO-E entspricht inhaltlich dem bisherigen § 100f Abs. 3 Satz 2 StPO.

- § 100h Abs. 2 Satz 2 Nr. 2 StPO-E entspricht inhaltlich dem bisherigen § 100f Abs. 3 Satz 3 StPO.

- § 100h Abs. 3 StPO-E entspricht inhaltlich dem bisherigen § 100f Abs. 4 StPO und übernimmt hinsichtlich mitbetroffener Personen die Formulierung des § 163f Abs. 2 StPO („Dritte“ statt „andere Personen“).

Zu § 100i StPO-E

Die vom Bundesverfassungsgericht mit Beschluss vom 22. August 2006 (2 BvR 1345/03) als verfassungsgemäß beurteilte Regelung des § 100i StPO zum so genannten „IMSI[1]-Catcher“-

[1] IMSI = International Mobile Subscriber Identity.

Einsatz wird unter Angleichung an § 100g Abs. 1 Satz 1 Nr. 1 StPO-E neu gefasst. Damit wird die schon bislang für technische Observationsmittel in § 100f Abs. 1 Nr. 2 StPO (jetzt: § 100h Abs. 1 Satz 1 Nr. 1, Satz 2 StPO-E) sowie für die längerfristige Observation in § 163f Abs. 1 StPO enthaltene materielle Schwelle des Erfordernisses einer Straftat von erheblicher Bedeutung auch in § 100i StPO-E integriert. Zugleich wird es dadurch möglich, den „IMSI-Catcher“ auch zur Unterstützung einer Observationsmaßnahme sowie zur Vorbereitung einer Verkehrsdatenerhebung nach § 100g StPO-E einzusetzen. Ferner führt die Neufassung der Vorschrift zu einer deutlichen redaktionellen Straffung des Regelungstextes. Dies trägt auch Stellungnahmen aus der Praxis Rechnung, die die Lesbarkeit des bisherigen § 100i StPO bemängelten (vgl. Albrecht, Dorsch und Krüpe, a. a. O., S. 204).

Absatz 1 enthält die materiellen Voraussetzungen für den Einsatz des „IMSI-Catchers“: Erforderlich ist – wie im Falle des § 100g Abs. 1 Satz 1 Nr. 1 StPO-E – zum einen der auf bestimmte Tatsachen gründende Verdacht einer – vollendeten, in strafbarer Weise versuchten oder durch eine Straftat vorbereiteten – Straftat von erheblicher Bedeutung. Zum anderen muss die mittels IMSI-Catcher bezweckte Ermittlung der Geräte- oder Kartennummer oder des Standortes eines Mobilfunkgerätes erforderlich sein zur Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsortes des Beschuldigten.

Absatz 2 entspricht dem bisherigen Absatz 3.

Absatz 3 Satz 1 enthält mit der Verweisung auf § 100a Abs. 3 und weite Teile des § 100b StPO-E die für die Anordnung und Durchführung des IMSI-Catcher-Einsatzes vorgesehenen Verfahrensregelungen:

- Mit dem Verweis auf § 100a Abs. 3 StPO-E wird geregelt, dass der Einsatz sich nur gegen den Beschuldigten und die so genannter Nachrichtenmittler richten darf.

- Mit dem Verweis auf § 100b Abs. 1 Satz 1 bis 3 wird entsprechend dem bisherigen Recht der Richtervorbehalt nebst Eilkompetenz der Staatsanwaltschaft vorgesehen und darüber hinaus die in § 100b Abs. 1 Satz 3 Halbsatz 2 StPO-E neu aufgenommene Verwertungsregelung übernommen.

- Aus dem Verweis auf § 100b Abs. 2 Satz 1 und Abs. 4 Satz 1 folgt, dass die Anordnung des IMSI-Catcher-Einsatzes schriftlich zu erfolgen hat und der der Einsatz zu beenden ist, wenn die Voraussetzungen der Anordnung entfallen.

Absatz 3 Satz 1 und 2 übernimmt in redaktionell angepasster Weise die bisherige Regelung in § 100i Abs. 4 Satz 2 und 3 zu den Anordnungsfristen.

Nicht mehr ausdrücklich erwähnt wird in dem neu gefassten § 100i StPO-E die im geltenden § 100i Abs. 2 Satz 3 ausdrücklich vorgesehene Zulässigkeit der Maßnahme zur Eigensicherung der mit einer Festnahme betrauten Beamten des Polizeidienstes. Gleichwohl bleibt auch diese Einsatzmöglichkeit erhalten: Der IMSI-Catcher-Einsatz im Rahmen einer Eigensicherung dient dazu, den aktuellen Aufenthaltsort des Beschuldigten zu ermitteln. Dieser Einsatzzweck wird in Absatz 1 letzter Halbsatz ausdrücklich erwähnt.

Ebenfalls nicht mehr ausdrücklich in § 100i StPO-E geregelt ist die bislang in § 100i Abs. 5 Satz 4 enthaltene Auskunftsverpflichtung von geschäftsmäßig tätigen Telekommunikationsdiensten, die Geräte- und Kartennummer mitzuteilen. Die Befugnis zur Erhebung dieser Angaben ergibt sich bereits aus den allgemeinen Befugnisnormen (§§ 94 ff., 161, 163 StPO) in Verbindung mit den in §§ 111 ff. TKG geregelten Verpflichtung der Telekommunikationsdienstleister zur Erteilung der entsprechenden Auskünfte.

Soweit aus der Strafverfolgungspraxis die Forderung erhoben wird, zwecks Vorbereitung des IMSI-Catcher-Einsatzes eine Befugnis zur Erhebung von Standortkennungen (Funkzellenangaben) bei den Telekommunikationsdienstleistern zu schaffen, ist diesem Petitum bereits durch die Neuregelung des § 100g StPO-E Rechnung getragen.

§ 100i StPO-E wird durch die für alle verdeckten Ermittlungsmaßnahmen geltenden Regelungen in § 101 StPO-E ergänzt. Der Rechtsschutz Betroffener wird hierdurch insofern gestärkt, als die grundrechtssichernden Regelungen des § 101 StPO-E in vollem Umfang auch auf den Einsatz des „IMSI-Catchers“ Anwendung finden und damit auch eine Benachrichtigungspflicht gegenüber der in ihrem Recht auf informationelle Selbstbestimmung betroffenen Zielperson der Maßnahme eingeführt wird. Soweit durch den Einsatz des „IMSI-Catchers“ funktionsbedingt vorübergehend auch Daten von Mobiltelefonen dritter Personen erfasst werden, die technisch verarbeitet und durch Bildung einer Schnittmenge aus den Daten mehrerer Messungen wieder ausgeschieden werden, ist bereits fraglich, ob insoweit ein Eingriff in die Rechte dieser Dritten gegeben ist (vgl. BVerfGE 100, 313, 366; 107, 299, 328). Jedenfalls begegnet es keinen verfassungsrechtlichen Bedenken, dass das Gesetz eine (Ermittlung und) Benachrichtigung mitbetroffener dritter Personen nicht vorsieht (vgl. BVerfG, 2 BvR 1345/03 vom 22. August 2006, Absatz-Nr. 77).

Zu § 101 StPO-E

§ 101 StPO-E fasst für die Ermittlungsbefugnisse nach den §§ 98a, 99, 100a, 100c, 100f bis 100i, 110a und 163d ff. StPO-E all jene Verfahrensvorschriften zusammen, die bislang jeweils gesondert – und daher mitunter abweichend voneinander – geregelt waren oder – etwa aufgrund verfassungsgerichtlicher Vorgaben – zusätzlich vorzusehen sind. Die Vorschrift regelt so im Lichte der Rechtsprechung des Bundesverfassungsgerichts einheitlich für alle speziellen verdeckten Maßnahmen Kennzeichnungspflichten (Absatz 3), Benachrichtigungspflichten (Absatz 4) und deren Zurückstellung nebst gerichtlicher Überprüfung (Absatz 5 bis 8). Zur Stärkung des Grundrechts auf rechtliches Gehör nach Artikel 103 Abs. 1 GG und des Gebots der Gewährleistung eines effektiven Rechtsschutzes nach Artikel 19 Abs. 4 GG wird unabhängig von der Stellung des Betroffenen im Verfahren nachträglicher Rechtsschutz gewährt (Absatz 9). Eine allgemeine Regelung zur Löschung nicht mehr benötigter personenbezogener Daten, die aus verdeckten Maßnahmen gewonnen wurden, findet sich in Absatz 10.

- Der Inhalt des bisherigen § 101 Abs. 1 StPO sowie des bisherigen § 100d Abs. 8 und 9 (Benachrichtigungspflichten) geht so ein in die neuen Abätze 4 bis 8.

- Der Inhalt des bisherigen § 101 Abs. 2 und 3 StPO ist systematisch den Regelungen zur Postbeschlagnahme zuzuordnen und daher in § 100 Abs. 5 und 6 StPO-E eingestellt worden.

- Die bisherige Regelung zur getrennten Aktenführung in § 101 Abs. 4 findet sich nunmehr in § 101 Abs. 2 StPO-E.

Zu § 101 Abs. 1 StPO-E

Absatz 1 erstreckt den Anwendungsbereich der nachfolgenden Absätze für alle verdeckten Maßnahmen, soweit nicht bereichsspezifisch etwas anderes geregelt ist. Namentlich sind damit von den Regelungen des § 101 StPO erfasst:

- die Rasterfahndung nach § 98a StPO-E,

- die Postbeschlagnahme nach § 99 StPO-E,

- die Telekommunikationsüberwachung nach § 100a StPO-E,

- die akustische Wohnraumüberwachung nach § 100c StPO-E,
- die akustische Überwachung außerhalb von Wohnungen nach § 100f StPO-E,
- die Verkehrsdatenerhebung nach § 100g StPO-E,
- der Einsatz besonderer technischer Mittel nach § 100h StPO-E,
- der „IMSI-Catcher"-Einsatz nach 100i StPO-E,
- der Einsatz Verdeckter Ermittler nach § 110a StPO-E,
- die Schleppnetzfahndung nach § 163d StPO-E,
- die Ausschreibung nach § 163e StPO und
- die längerfristige Observation nach § 163f StPO-E.

Nicht einbezogen ist hingegen die DNA-Analyse im Fall des § 81e StPO, für die bislang § 101 Abs. 1 StPO eine Benachrichtigungspflicht vorsieht (zur Kritik hieran vgl. Löffelmann, ZStW 118 [2006], S. 358, 367; ders. in: Krekeler/Löffelmann, Anwaltskommentar zur StPO, § 101 Rn. 1):

- Im Fall des § 81e Abs. 1 (molekulargenetische Untersuchung der einer Person entnommenen Körperzellen) handelt es sich um keine verdeckte Ermittlungsmaßnahme. Denn bei Anordnung einer Körperzellenentnahme für Zwecke der DNA-Analyse wird die Maßnahme der betroffenen Person zwangsläufig bekannt. Es besteht daher kein Anlass, auf diese Fallgestaltung die Regelungen zu verdeckten Ermittlungsmaßnahmen anzuwenden, insbesondere Benachrichtigungspflichten nach den Absätzen 4 ff. vorzusehen.

- Und in der in § 81e Abs. 2 StPO geregelten Fallgestaltung der molekulargenetischen Untersuchung einer anonymen Spur ist die betroffene Person – jedenfalls zunächst – nicht bekannt, so dass etwa eine Benachrichtigung nicht in Betracht kommt. Wird diese Person aufgrund des DNA-Abgleichs bekannt, wird das Untersuchungsergebnis der Person ohnehin im Rahmen des Ermittlungsverfahrens mitgeteilt, da hieran weitere Ermittlungsmaßnahmen, u. a. die Vernehmung der Person, anknüpfen.

Zu § 101 Abs. 2 StPO-E

In Absatz 2 werden die bislang 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. § 100f Abs. 1 Nr. 2 StPO und
- den Einsatz Verdeckter Ermittler in § 110d Abs. 2 StPO

enthaltenen Regelungen zur getrennten Aktenführung unverändert übernommen. Von einer – im Sinne einer harmonischen Gesamtregelung erwogenen – Ausweitung der getrennten Aktenführung auch auf andere verdeckte Ermittlungsmaßnahmen wird abgesehen. Die getrennte Aktenführung führt – insbesondere nach Anklageerhebung – zu einer nicht unerheblichen Beschränkung der Akteneinsichtsrechte. Für die Notwendigkeit einer solchen Beschränkung auch bei anderen verdeckten Ermittlungsmaßnahmen ist bislang aus der Praxis kein Bedarf bekundet oder gar belegt worden.

Zu § 101 Abs. 3 StPO-E

Absatz 3 bestimmt, dass die aus den in Absatz 1 aufgeführten Maßnahmen resultierenden personenbezogenen Daten als solche zu kennzeichnen sind. Dies entspricht der bereits zur akustischen Wohnraumüberwachung getroffenen Regelung in § 100d Abs. 7 StPO, die in Folge der Neuregelung in Absatz 3 entfällt. Die Kennzeichnungspflichten sind entsprechend den Vorgaben des Bundesverfassungsgerichts (BVerfGE 100, 313, 360; 109, 279, 374, 379 f.) für die Sicherstellung einer ordnungsgemäßen Datenverwendung erforderlich und werden daher konsequent auf alle speziell geregelten verdeckten Ermittlungsmaßnahmen erstreckt. Denn alle diese Maßnahmen sind – von der Postbeschlagnahme abgesehen – vom Verdacht bestimmter, in den jeweiligen Regelungen näher umschriebener Straftaten abhängig und lösen damit das Eingreifen der Verwendungsbeschränkungen in § 477 Abs. 2 StPO-E aus.

Zu § 101 Abs. 4 StPO-E

In Absatz 4 werden die bisher in § 101 Abs. 1 Satz 1 StPO und weiteren Vorschriften (z. B. § 100d Abs. 8 und 9 StPO) enthaltenen Benachrichtigungspflichten an zentraler Stelle zusammengefasst, maßnahmebezogen konkretisiert und unter Berücksichtigung der Vorgaben des Bundesverfassungsgerichts (BVerfGE 109, 279, 366 f.) überarbeitet.

Satz 1 bestimmt, dass die von den in Absatz 1 genannten verdeckten Ermittlungsmaßnahmen Betroffenen von der Maßnahme zu benachrichtigen sind und führt die zu benachrichtigenden Personen maßnahmespezifisch auf. Damit wird den Unsicherheiten Rechnung getragen, die nach der Untersuchung von Albrecht/Dorsch/Krüpe (a. a. O., S. 470) 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, insbesondere der Praxis keine hinreichende Hilfestellung zur Bestimmung der zu benachrichtigenden Personen geben. Dem soll durch die Aufzählung in Satz 1 entgegengewirkt werden.

- Die bislang in § 101 Abs. 1 StPO vorgesehene Benachrichtigungspflicht bei Maßnahmen nach § 81e StPO (DNA-Analyse) entfällt, vgl. hierzu die obigen Ausführungen zu Absatz 1.

- Bei der Rasterfahndung nach § 98a StPO-E sind die von der Rasterfahndung betroffenen Personen, gegen die nach Auswertung der Daten weitere Ermittlungen geführt wurden, zu benachrichtigen. Dies entspricht der bisherigen Bestimmung des zu benachrichtigenden Personenkreises in § 98b Abs. 4 Satz 1 i. V. m. § 163d Abs. 5 StPO.

- Bei der Postbeschlagnahme nach § 99 StPO-E sind der Absender und der Adressat der beschlagnahmten Postsendung zu benachrichtigen. Der Begriff „Adressat“ anstelle des auch in Betracht kommenden Begriffs „Empfänger“ wurde gewählt, um dem Umstand Rechnung zu tragen, dass die zu benachrichtigende Person, an die die Postsendung gerichtet war, diese im Fall der Postbeschlagnahme gerade nicht empfangen hat.

- Bei einer Telekommunikationsüberwachung nach § 100a StPO-E sind die Beteiligten der überwachten Telekommunikation zu benachrichtigen, also diejenigen Personen, die telekommuniziert haben. Dies trägt dem Umstand Rechnung, dass bei diesen Personen in das ihnen von Artikel 10 GG gewährleistete Fernmeldegeheimnis eingegriffen wurde. Ein solcher Eingriff wird regelmäßig – aber nicht ausnahmslos – bezüglich des Inhabers des

überwachten Anschlusses und des Beschuldigten vorliegen; sind diese Personen aber im konkreten Fall an der überwachten Telekommunikation nicht beteiligt gewesen, etwa weil der Inhaber des Anschlusses diesen einer anderen Person überlassen hat oder lediglich ein Telefonat des Nachrichtenmittlers mit einer dritten Person überwacht wurde, so besteht eine Benachrichtigungspflicht weder gegenüber dem Inhaber des überwachten Anschlusses noch gegenüber dem Beschuldigten. Etwaige Akteneinsichtsrechte, bei deren Wahrnehmung der Beschuldigte bzw. dessen Verteidiger Kenntnis von der Maßnahme erlangen können, bleiben davon unberührt.

- Bei der akustischen Wohnraumüberwachung mit technischen Mitteln nach § 100c StPO-E ist der bislang in § 100d Abs. 8 Satz 3 StPO beschriebene Kreis der zu benachrichtigenden Personen (Beschuldigter, sonstige überwachte Personen sowie Inhaber und Inhaberinnen und Bewohner und Bewohnerinnen der überwachten Wohnung) – bis auf eine Klarstellung in Buchstabe c – unverändert übernommen worden. Die – schon in § 100d Abs. 8 Satz 3 StPO enthaltene – Unterscheidung zwischen Inhabern und Bewohnern einer Wohnung geht auf das Urteil des Bundesverfassungsgerichts zur akustischen Wohnraumüberwachung zurück (BVerfG, 1 BvR 2378/98 vom 3.3.2004, Absatz-Nr. 295). Sinngebend ist diese Differenzierung, wenn man berücksichtigt, dass Inhaber einer Wohnung auch ein Mieter sein kann, der die Wohnung nicht oder – etwa während des Laufs der akustischen Wohnraumüberwachung – zeitweise nicht selbst bewohnt, ohne hierbei seine Rechte hinsichtlich der Wohnung aufgegeben zu haben. Auch wenn die Kommunikation eines solcher Inhabers im Rahmen der akustischen Wohnraumüberwachung nicht abgehört und aufgezeichnet worden ist, so sind seine Rechte doch durch die – regelmäßig heimliche – Einbringung der Überwachungstechnik in die Wohnung betroffen worden.

- Bei der akustischen Überwachung mit technischen Mitteln außerhalb von Wohnungen nach § 100f StPO-E sind die Zielperson – also diejenige, die mittels der akustischen Überwachung überwacht werden soll – sowie die von der Maßnahme erheblich mitbetroffenen Personen zu benachrichtigen. Die Formulierung „erheblich mitbetroffenen Personen“ trägt dem Umstand Rechnung, dass durch die Streubreite einer solchen Maßnahme eine Vielzahl von Personen in jedoch jeweils vergleichsweise unerheblicher Weise mitbetroffen sein kann. Wird etwa in einer Parkanlage ein Gespräch zwischen verdächtigen Personen (Beschuldigten) abgehört und werden hierbei auch einzelne „Wortfetzen“ zufällig vorübergehender Personen mit erfasst, so erscheint es weder sachgerecht noch aus verfassungsrechtlichen Gründen geboten, diese „vorbeispazierenden“ Personen von der Maßnahme zu benachrichtigen. Gesellen sich hingegen zu den verdächtigen Personen weitere Personen für einige Zeit hinzu, so dass deren Kommunikationsbeiträge in erheblichem

Umfang mit erfasst werden, so greift die Maßnahme auch in deren Grundrechte in nicht unerheblicher Weise ein und lässt damit die Benachrichtigungspflicht auch diesen gegenüber zur Entstehung gelangen.

- Bei der Verkehrsdatenerhebung nach § 100g StPO-E sind – ebenso wie bei Maßnahmen nach § 100a StPO-E – die Beteiligten der betroffenen Telekommunikation zu benachrichtigen. Die obigen Ausführungen betreffend § 100a StPO-E gelten entsprechend. Damit wird der Kreis der zu benachrichtigenden Personen dem Grunde nach bei Maßnahmen, die das Fernmeldegeheimnis beschränken, zwar – aufgrund verfassungsrechtlicher Vorgaben – zunächst recht groß. In der Praxis dürften jedoch die in Absatz 4 Satz 3 bis 5 enthaltenen Ausschlussgründe hier besondere Relevanz erlangen.

- Bei dem Einsatz besonderer technischer Mittel nach § 100h StPO-E (Bildaufnahmen, technische Observationsmittel) sind die Zielperson sowie die erheblich mitbetroffenen Personen zu benachrichtigen. Die obigen Ausführungen zu Maßnahmen nach § 100f StPO-E gelten entsprechend. Die damit gegenüber § 101 Abs. 1 Satz 1 StPO verbundene Ausdehnung der Benachrichtigung bei Bildaufnahmen (§ 100f Abs. 1 Nr. 1 StPO bzw. § 100h Abs. 1 Nr. 1 StPO-E) ist wegen des damit verbundenen Eingriffs in das Rechts am eigenen Bild grundrechtlich geboten.

- Bei dem Einsatz des „IMSI-Catchers“ nach 100i StPO-E ist die Zielperson zu benachrichtigen. Damit wird für diese Maßnahme die Benachrichtigungspflicht neu eingeführt. Dies ist grundrechtlich geboten, weil die Maßnahme nach § 100i StPO-E in nicht ganz unerheblicher Weise in das Recht auf informationelle Selbstbestimmung der Zielperson eingreift. Die Nichteinbeziehung der sonstigen von der Maßnahme betroffenen Personen trägt dem Umstand Rechnung, 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.

- Bei dem Einsatz eines Verdeckten Ermittlers nach § 110a StPO-E sind die Zielperson sowie diejenige Person, deren nicht allgemein zugängliche Wohnung der Verdeckte Ermittler betreten hat, zu benachrichtigen. Hinsichtlich des Wohnungsinhabers entspricht dies der bisherigen Regelung der Benachrichtigungspflicht beim Einsatz eines Verdeckten Ermittlers in § 110d Abs. 1 StPO. Es ist aber darüber hinaus auch geboten, die Benach-

richtigung der Zielperson vorzusehen, weil der Einsatz des verdeckten Ermittlers insoweit eine erhebliche Eingriffsintensität haben kann.

- Bei der Schleppnetzfahndung nach § 163d StPO-E sind die betroffenen Personen, gegen die nach Auswertung der Daten weitere Ermittlungen geführt wurden, zu benachrichtigen. Dies entspricht der bisherigen Bestimmung des zu benachrichtigenden Personenkreises in § 163d Abs. 5 StPO.

- Bei der Ausschreibung zur polizeilichen Beobachtung nach § 163e StPO(-E) sind die Zielperson der Maßnahme und die Personen, deren personenbezogene Daten gemeldet worden sind, zu benachrichtigen. Damit wird für diese Maßnahme erstmals eine Benachrichtigungspflicht eingeführt. Dies erscheint in Anbetracht der mit der Maßnahme im Einzelfall verbundenen Überwachungsintensität (Erstellung von Bewegungsprofilen) geboten. „Zielperson“ ist diejenige Person, gegen die die Maßnahme nach § 163e Abs. 1 StPO angeordnet werden darf, also der Beschuldigte und dessen Nachrichtenmittler. Soweit nach § 163e Abs. 2 StPO auch das Kennzeichen eines Kraftfahrzeuges ausgeschrieben werden kann, kommt die Regelung dem eingetragenen Halter oder Nutzer des Kraftfahrzeugs zugute. Soweit die in § 163e Abs. 2 StPO genannten Begleiter betroffen sind, weil ihre personenbezogene Daten gemeldet worden sind, sind auch sie zu benachrichtigen.

- Bei der längerfristigen Observation nach § 163f StPO-E sind die Zielperson sowie die erheblich mitbetroffenen Personen zu benachrichtigen. Für die Maßnahme der längerfristigen Observation wird damit erstmals eine Benachrichtigungspflicht begründet. Dies ist in Anbetracht der Grundrechtsrelevanz dieser Maßnahme geboten. Zur Umschreibung des zu benachrichtigenden Personenkreises wird auf die entsprechend geltenden obigen Ausführungen zu Maßnahmen nach § 100f StPO-E verwiesen.

Satz 2 bestimmt, dass im Rahmen der Benachrichtigung auf die Möglichkeit nachträglichen Rechtsschutzes nach Absatz 9 und die dafür vorgesehene Frist hinzuweisen ist. Die Regelung ist § 100d Abs. 8 Satz 2 StPO nachgebildet, entspricht aber auch der in § 98 Abs. 2 Satz 7 StPO statuierten Rechtsmittelbelehrung und gestaltet die Rechtsschutzmöglichkeiten der Betroffenen damit effektiv aus.

Nach Satz 3 hat die Benachrichtigung zu unterblieben, wenn durch sie überwiegende schutzwürdige Interessen anderer Betroffener (z. B. des Nachrichtenmittlers oder auch des Beschuldigten, wenn etwa dessen Gespräche mit einem an der Straftat unbeteiligten Geschäftspartner erfasst wurde) der Benachrichtigung entgegenstehen. Dies erfordert eine Ab-

wägung der widerstreitenden Interessen im Einzelfall, die einer weitergehenden gesetzlichen Regelung nicht zugänglich ist.

Satz 4 bestimmt, dass in den Fällen des Satzes 1 Nr. 2 (Postbeschlagnahme), 3 (Telekommunikationsüberwachung) und 6 (Verkehrsdatenerhebung) die Benachrichtigung unterbleiben kann, wenn eine der dort genannten Personen, gegen die sich die Maßnahme nicht gerichtet hat, von der Maßnahme in nur unerheblicher Weise betroffen wurde und anzunehmen ist, dass kein Interesse an einer Benachrichtigung besteht. Diese Regelung trägt dem Umstand Rechnung, dass von den in Bezug genommenen Maßnahmen zwar regelmäßig viele Personen in ihrem Grundrecht aus Artikel 10 GG betroffen werden, dies aber im Einzelfall in einer vergleichsweise so geringfügigen Weise, dass ein Interesse an einer Benachrichtigung oftmals nicht anzunehmen ist. Bei Postbeschlagnahmen (Satz 1 Nr. 2) kann dies etwa der Fall sein, wenn vorsorglich oder versehentlich auch Werbebriefsendungen, die massenhaft versandt werden, einbezogen wurden. Bei Telekommunikationsüberwachungsmaßnahmen (Satz 1 Nr. 3) wird dies beispielsweise dann der Fall sein, wenn für die Strafverfolgung irrelevante Gespräche zur Besorgung von Alltagsgeschäften mit erfasst wurden (z. B. Terminvereinbarungen mit Handwerkern; telefonische Bestellungen etwa bei Bringdiensten; Reklamationen, die über so genannte Callcenter bearbeitet werden). Entsprechendes gilt bei Verkehrsdatenerhebungen (Satz 1 Nr. 6). In solchen Fallgestaltungen wird regelmäßig davon auszugehen, dass der Kommunikationspartner aufgrund seiner regelmäßig nur zufälligen und nur geringfügigen Betroffenheit kein Interesse an einer Benachrichtigung und der dadurch ermöglichten Geltendmachung nachträglichen Rechtsschutzes nach Absatz 9 hat. Die Ausrichtung der Benachrichtigungspflichten an dieser Interessenlage der Betroffenen trägt – im Hinblick auf den mit Benachrichtigungspflichten verbundenen Aufwand an Personal-, Sach- und Finanzmitteln – zugleich dem Gebot des wirtschaftlichen Haushaltens mit öffentlichen Mitteln Rechnung und wirkt einer Überbürokratisierung entgegen.

Die Regelung in Satz 4 ist nicht als zwingende Regelung sondern als Ermessensvorschrift ausgestaltet. Dies trägt zwei Aspekten Rechnung: Zum einen ist, auch wenn eine Person in nur unerheblicher Weise von der Maßnahme betroffen wurde und anzunehmen ist, dass kein Interesse an der Benachrichtigung besteht, kein Grund gegeben, die Benachrichtigung gesetzlich zu verbieten. Zum anderen kann es in Einzelfällen für die Strafverfolgungsbehörden effizienter sein, eine Benachrichtigung durchzuführen, als eingehende Überlegungen dazu anzustellen, ob das Maß der Betroffenheit bereits die Unerheblichkeitsschwelle überschritten hat bzw. welche Punkte für oder gegen ein Interesse an der Benachrichtigung sprechen. Die Kann-Regelung in Satz 4 kommt damit den Bedürfnissen der Praxis entgegen.

Satz 5 befasst sich mit der Fallgestaltung, dass die Identität einer in Satz 1 in Bezug genommenen Person nicht bekannt ist, so dass eine Benachrichtigung praktisch nur erfolgen kann, wenn zuvor mittels entsprechender Nachforschungen die Identität der Person festgestellt wird. Das Bundesverfassungsgericht hat für solche Fallgestaltungen darauf hingewiesen, dass Nachforschungen zur Feststellung der Identität den Grundrechtseingriff sowohl für die Zielperson wie für sonstige Beteiligte vertiefen können und deshalb das Bestehen von Benachrichtigungspflichten unter diesen Umständen von einer Abwägung abhängt. Für diese ist zum einen die Intensität des Eingriffs bedeutsam und zum anderen, welchen Aufwand die Feststellung der Identität des Betroffenen fordert und welche Beeinträchtigungen mit ihr für die Zielperson und sonstige Beteiligte verbunden sein können (BVerfGE 109, 279, 364 f). Satz 5 nimmt diese Vorgaben des Bundesverfassungsgerichts auf, indem er bestimmt, dass Nachforschungen zur Feststellung der Identität nur vorzunehmen sind, wenn dies unter Berücksichtigung der Eingriffsintensität der Maßnahme gegenüber dieser Person, des Aufwands für die Feststellung ihrer Identität sowie der daraus für diese oder andere Personen folgenden Beeinträchtigungen geboten ist. Ergibt diese im Einzelfall erforderliche Abwägung, dass Nachforschungen nicht geboten sind, so haben diese ebenso wie die Benachrichtigung zu unterbleiben.

Zu § 101 Abs. 5 StPO-E

Absatz 5 enthält eine Regelung zur zeitweisen Zurückstellung einer Benachrichtigung, die der – aufzuhebenden – Regelung in § 100d Abs. 8 Satz 5 StPO nachgebildet ist.

Nach Satz 1 muss die Benachrichtigung erst erfolgen, sobald dies ohne Gefährdung des Untersuchungszwecks, des Lebens, der körperlichen Unversehrtheit und der persönlichen Freiheit einer Person und von bedeutenden Vermögenswerten geschehen kann.

Ein Zurückstellen der Benachrichtigung wegen Gefährdung der öffentlichen Sicherheit und der Möglichkeit der weiteren Verwendung eines eingesetzten nicht offen ermittelnden Beamten wurde aufgrund der Vorgaben des Bundesverfassungsgerichts gestrichen (vgl. hierzu BVerfGE 109, 279, 366 f.; BT-Drs. 15/4533, S. 19).

Hinsichtlich des Einsatzes eines Verdeckten Ermittlers wurde jedoch aus dem geltenden Recht (§ 110d Abs. 1 StPO) der Zurückstellungsgrund der Gefährdung der Möglichkeit der weiteren Verwendung des Verdeckten Ermittlers übernommen. Die Ausführungen des Bundesverfassungsgerichts im Urteil zur akustischen Wohnraumüberwachung (BVerfG 109, 279 ff., Abs. 302 f.) stehen dem nicht entgegen. Dort hat das Bundesverfassungsgericht ausge-

führt, dass die Gefährdung der weiteren Verwendung „eines nicht offen ermittelnden Beamten …die Zurückstellung einer Benachrichtigung im Falle der akustischen Wohnraumüberwachung nicht zu rechtfertigen“ vermag. Vorliegend geht es aber weder um die Zurückstellung der Benachrichtigung im Falle einer akustischen Wohnraumüberwachung noch um den Zurückstellungsgrund der Gefährdung der weiteren Verwendung eines nicht offen ermittelnden (Polizei-)Beamten (so genannter „NoeP“), sondern um die Zurückstellung der Benachrichtigung über den Einsatz eines Verdeckten Ermittlers („VE“), um dessen weiteren Verwendung nicht zu gefährden.

Dieser Zurückstellungsgrund ist unverzichtbar und hinreichend gewichtig, um eine Beschränkung der Benachrichtigungspflicht zu rechtfertigen. Die Ausbildung Verdeckter Ermittler, die Schaffung der erforderlichen Legende und das – nicht ohne weiteres reproduzierbare – Heranführen und Einschleusen eines Verdeckten Ermittlers in Kreise etwa der organisierten Kriminalität sind mit einem ganz erheblichen zeitlichen, organisatorischen und finanziellen Aufwand verbunden. Dieser spezifischen Ausgangssituation hat der Gesetzgeber Rechnung zu tragen. In § 110b Abs. 3 StPO hat er dies – in bislang verfassungsrechtlich nicht beanstandeter Weise – dergestalt getan, dass die Geheimhaltung der Identität eines Verdeckten Ermittlers auch noch nach der Beendigung seines Einsatzes erlaubt ist. Diese Geheimhaltung der Identität eines Verdeckten Ermittlers wäre indessen bei einer ausnahmslosen Benachrichtigungspflicht faktisch nicht möglich. Diesem Aspekt trägt der aus § 110d Abs. 1 StPO übernommene Zurückstellungsgrund der Gefährdung des weiteren Einsatzes eines Verdeckten Ermittlers Rechnung.

Gründe, die gegen die Beibehaltung dieses Zurückstellungsgrundes sprechen können, sind demgegenüber nicht von gleich hohem Gewicht: Der Einsatz eines Verdeckten Ermittlers ist typischerweise nicht mit einem derart intensiven Eingriff in Grundrechte verbunden, wie dies etwa bei der akustischen Wohnraumüberwachung regelmäßig der Fall sein wird. Soweit der Verdeckte Ermittler im Einzelfall eine fremde Wohnung betritt, darf dies nach § 110c StPO nur mit Einverständnis des Berechtigten erfolgen. Ferner ist zu berücksichtigen, dass mit der Neuregelung der Benachrichtigungspflichten das Vorliegen auch des Zurückstellungsgrundes der Gefährdung des weiteren Einsatzes eines Verdeckten Ermittlers einer – gegebenenfalls auch wiederholten – gerichtlichen Überprüfung unterstellt wird (vgl. § 101 Abs. 6 bis 8 StPO-E) und damit der Rechtsschutz Betroffener eine zusätzliche Absicherung erhält. Eine Abwägung sämtlicher Gesichtspunkte ergibt hiernach, dass die Beibehaltung des Zurückstellungsgrundes der Gefährdung des weiteren Einsatzes eines Verdeckten Ermittlers insgesamt gerechtfertigt ist.

Satz 2 bestimmt, dass die Zurückstellung der Benachrichtigung aus einem der in Satz 1 genannten Gründe aktendkundig zu machen ist. Dies fördert eine ordnungsgemäße Handhabung der Zurückstellungsregelungen und trägt dazu bei, die Zurückstellungsgründe im Rahmen einer gerichtlichen Überprüfung nach Absatz 6 nachvollziehen zu können.

Zu § 101 Abs. 6 StPO-E

Absatz 6 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.

Satz 1 bestimmt daher, dass eine über zwölf Monate hinausgehende Zurückstellung der Benachrichtigung nach Absatz 5 der gerichtlichen Zustimmung bedarf. Die Frist beginnt mit der Beendigung der Maßnahme. Im Falle der akustischen Wohnraumüberwachung setzt die gerichtliche Kontrolle – entsprechend der bisherigen Regelung in § 100d Abs. 9 Satz 1 StPO – nach der Sonderregelung in Satz 4 Halbsatz 1 bereits nach sechs Monaten ein. Auf die Fristberechnung finden die allgemeinen Regelungen der §§ 42 ff. StPO Anwendung. Das Gericht hat zu prüfen, ob die in Absatz 5 genannten Zurückstellungsgründe vorliegen, und bejahendenfalls seine Zustimmung zur weiteren Zurückstellung zu geben. Verweigert das Gericht die Zustimmung, so hat die Benachrichtigung zu erfolgen, es sei denn, die Staatsanwaltschaft führt im Wege der Beschwerde (§ 304 StPO) eine gerichtliche Zustimmung zur Zurückstellung der Benachrichtigung doch noch herbei.

Stimmt das Gericht der Zurückstellung der Benachrichtigung zu, so hat es nach Satz 2 Halbsatz 1 zugleich die Dauer der weiteren Zurückstellung zu bestimmen. Diese Bestimmung obliegt inhaltlich dem Ermessen des Gerichts. Es wird hierbei aber anhand der Umstände des Einzelfalls einzuschätzen haben, wann eine Benachrichtigung voraussichtlich wird erfolgen können. Um die gerichtliche Kontrolle auch unter Rechtsschutzgesichtspunkten effektiv ausüben zu können, wird sich in aller Regel – von besonderen Fallgestaltungen abgesehen – eine Zurückstellung über mehr als ein weiteres Jahr nicht empfehlen. Im Fall der akustischen Wohnraumüberwachung darf – die bisherige Regelung in § 100d Abs. 9 Satz 2 StPO übernehmend – die jeweilige Zurückstellungsdauer sechs Monate nicht überschreiten, wie Satz 4 Halbsatz 2 ausdrücklich bestimmt.

Eine über den vom Gericht bestimmten Zeitpunkt hinausreichende Zurückstellung ist nach Satz 2 Halbsatz 2 möglich, bedarf aber ebenfalls der gerichtlichen Zustimmung.

Satz 3 trifft eine praktischen Bedürfnissen Rechnung tragende Sonderregelung für den Fall, dass mehrere der in Absatz 1 genannten Maßnahmen in einem engen zeitlichen Zusammenhang durchgeführt worden sind. In solchen Fällen beginnt die anzurechnende Zurückstellungsdauer erst mit der Beendigung der letzten Maßnahme. Diese Regelung ist sachgerecht. Vor einer Beendigung der letzten verdeckten Ermittlungsmaßnahme werden regelmäßig die Zurückstellungsgründe des Absatzes 5 hinsichtlich der zuvor durchgeführten verdeckten Maßnahmen vorliegen, insbesondere der Zurückstellungsgrund einer Gefährdung des Untersuchungszwecks.

Satz 4 enthält die zu Satz 1 bereits erläuterten Sonderreglungen zur maximal jeweils zulässigen Zurückstellungsdauer bei Maßnahmen der akustischen Wohnraumüberwachung nach § 100c StPO.

Zu § 101 Abs. 7 StPO-E

Absatz 7 übernimmt in Anlehnung an § 12 Abs. 1 Satz 3 Nr. 1 und 2 G 10 eine Regelung zum endgültigen Absehen von der Benachrichtigung. Voraussetzung ist, 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. Bei sorgfältiger Prüfung dieser Voraussetzungen, insbesondere der Prognose, dass die Voraussetzungen für eine Benachrichtigung mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft nicht eintreten werden, wird die Regelung in der praktischen Anwendung voraussichtlich keinen breiten Anwendungsbereich haben. Sie ist gleichwohl aufgenommen worden, um bei Vorliegen eines solchen Ausnahmefalles die Strafverfolgungsbehörden und Gerichte nicht mit fortwährenden Prüfungen weiterer Zurückstellungen zu belasten, wenn absehbar ist, dass eine Benachrichtigung ohnehin auch in Zukunft nicht wird erfolgen können.

Zu § 101 Abs. 8 StPO-E

Absatz 8 bestimmt, dass die nach den Absätzen 6 und 7 veranlassten gerichtlichen Entscheidungen von dem für die Anordnung zuständigen Gericht zu treffen sind. Das ist regelmäßig das Amtsgericht am Sitz der Staatsanwaltschaft, § 162 Abs. 1 StPO-E, im Fall der akustischen Wohnraumüberwachung die in § 74a Abs. 4 GVG bestimmte Kammer des Landgerichts. Die auch zur Sicherung eines rechtsstaatlichen Verfahrens nicht zwingend

notwendige Sonderregelung in § 100d Abs. 9 Satz 4 StPO, dass über Zustimmungen zu Zurückstellungen über 18 Monate hinaus das Oberlandesgericht entscheidet, ist hingegen im Interesse einer möglichst einheitlichen und damit harmonischen Regelung nicht übernommen worden.

Zu § 101 Abs. 9 StPO-E

Absatz 9 regelt, dass gegen die in Absatz 1 aufgeführten, regelmäßig in nicht unerheblicher Weise eingriffsintensiven verdeckten Ermittlungsmaßnahmen nachträglicher Rechtsschutz zu gewähren ist. Die Möglichkeit der Erlangung nachträglichen Rechtsschutzes ist unabdingbarer Teil einer rechtsstaatlichen Ausgestaltung verdeckter Ermittlungsmaßnahmen. Regelungstechnisch ist die Vorschrift § 100d Abs. 10 StPO nachgebildet (vgl. BT-Drs. 15/4533, S. 19), der aufgrund der allgemeinen Regelung in Absatz 9 aufgehoben wird.

Die ausdrückliche Regelung über den nachträglichen Rechtsschutz in Absatz 9 hat im wesentlichen die Funktion, den Betroffenen den Nachweis eines Rechtsschutzbedürfnisses im Einzelfall zu ersparen, führt aber nicht dazu, dass die schon bislang anerkannten Rechtsbehelfe verdrängt werden (vgl. Löffelmann, a. a. O. , § 100d StPO, Rn. 10). So kann der von einer noch andauernden verdeckten Ermittlungsmaßnahme Betroffene – so er von der Maßnahme Kenntnis erlangt – stets Rechtsschutz entsprechend § 98 Abs. 2 Satz 2 StPO erlangen. Entsprechendes gilt unter Berücksichtigung der Rechtsprechung des Bundesverfassungsgerichts auch dann, wenn sich die Maßnahme erledigt hat, aber ein Rechtsschutzinteresse an der nachträglichen Feststellung der Rechtswidrigkeit der Maßnahme besteht. Die Antwort darauf, unter welchen Voraussetzungen ein solches Rechtsschutzbedürfnis gegeben ist, führt in der Praxis allerdings immer wieder zu Unsicherheiten (vgl. zu einzelnen Fallgestaltungen bei Beschlagnahmen: Nack, a. a. O., § 98, Rn. 24 ff.). Anerkannt ist indessen, dass bei tiefgreifenden Grundrechtseingriffen ein Rechtsschutzbedürfnis auch nach Beendigung der Maßnahme zu bejahen ist. Die von § 101 StPO-E erfassten verdeckten Ermittlungsmaßnahmen begründen erhebliche, nur unter jeweils besonderen Voraussetzungen zulässige Grundrechtseingriffe. Es ist daher sachgerecht, die von solchen Maßnahmen Betroffenen von der konkreten Darlegung eines Rechtsschutzbedürfnisses im Einzelfall zu entlasten und ihnen mit Absatz 9 durchgehend eine nachträgliche Rechtsschutzmöglichkeit zu eröffnen. Da Absatz 4 Satz 1 bei der Bestimmung der zu benachrichtigenden Personen gerade dem Gesichtspunkt der Betroffenheit Rechnung trägt, knüpft Absatz 9 bei der Bestimmung derjenigen Personen, denen nach dieser Regelung nachträglicher Rechtsschutz zu gewähren ist, an den in Absatz 4 Satz 1 genannten Personenkreis an.

Gerichtet ist der nachträgliche Rechtsschutz auf die Überprüfung der Rechtmäßigkeit der verdeckten Ermittlungsmaßnahme sowie der Art und Weise ihres Vollzugs. Die vom Gericht zu treffende Feststellung über die Rechtmäßigkeit oder Rechtswidrigkeit enthält keine Entscheidung über die Verwertbarkeit der aus der Maßnahme gewonnenen Erkenntnisse. Die Frage der Verwertbarkeit ist vielmehr im Rahmen eines etwaigen Hauptverfahrens vom erkennenden Gericht zu beurteilen. Das Gesetz sieht auch keine Bindungswirkung für das erkennende Gericht an die im Verfahren des nachträglichen Rechtschutzes zur Rechtmäßigkeit bzw. Rechtswidrigkeit der Maßnahme getroffene Entscheidung vor, obgleich die Rechtmäßigkeit bzw. Rechtswidrigkeit für die Beurteilung der Verwertbarkeit mitbestimmend sein wird. Das Absehen von der Festschreibung einer Bindungswirkung rechtfertigt sich daraus, dass es im Verfahren des nachträglichen Rechtschutzes einerseits und bei der Frage der Verwertbarkeit andererseits um Prüfungsgegenstände geht, die nicht identisch sind. Während es beim nachträglichen Rechtsschutz um die Rechtmäßigkeit der Maßnahme bei deren Anordnung und in ihrem Vollzug geht, sind bei der Frage der Verwertbarkeit, die ureigene Aufgabe des erkennenden Gerichtes ist, auch andere Gesichtspunkte zu berücksichtigen, die auch erst nach Anordnung und Vollzug der Maßnahme liegen können.

Darüber hinaus ermöglicht das Verfahren des nachträglichen Rechtschutzes regelmäßig nur eine instanzgerichtliche Rechtsprechung durch das Anordnungsgericht und das Beschwerdegericht, womit eine höchstrichterliche Klärung von oft schwierigen Fragen der Rechtmäßigkeit bzw. Rechtswidrigkeit verdeckter Ermittlungsmaßnahmen weitgehend ausgeschlossen ist. Demgegenüber unterliegt eine an die Entscheidungen im nachträglichen Rechtsschutzverfahren nicht gebundene eigenständige Beurteilung der Verwertbarkeit durch das erkennende Gericht im Rahmen der Berufung und Revision der Überprüfung durch die ober- und höchstrichterliche Rechtsprechung. Dies trägt zur Klärung von Streitfragen und damit zur Rechtssicherheit bei.

Satz 1 regelt, dass die in Absatz 4 Satz 1 maßnahmespezifisch aufgeführten Betroffenen Rechtsschutz auch noch 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.

Die Anknüpfung an den Kreis der dem Grunde nach zu benachrichtigenden Personen – d. h. ungeachtet etwaiger Möglichkeiten des Absehens von der Benachrichtigung aus Verhältnismäßigkeitsgründen, wegen der Beeinträchtigung von Drittinteressen oder aus Gründen der Unbekanntheit der zu benachrichtigen Person – begrenzt zugleich den Kreis der nach Absatz 9 rechtsschutzbefugten Personen. Beispielsweise ist im Falle der Überwachung eines

Telekommunikationsanschlusses grundsätzlich jeder Beteiligte der überwachten Telekommunikation nach Absatz 4 Satz 1 Nr. 3 dem Grunde nach zu benachrichtigen und hat damit nach Absatz 9 die Möglichkeit, nachträglichen Rechtsschutz zu erlangen. Umgekehrt ist der Beschuldigte nicht schon aufgrund seiner Beschuldigteneigenschaft dem Grunde nach zu benachrichtigen und damit rechtsschutzbefugt im Sinne des Absatzes 9; denn im Falle der Überwachung der Telekommunikation eines Nachrichtenmittlers ist der Beschuldigte nicht notwendigerweise selbst Teilnehmer der überwachten Telekommunikation.

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 Satz 1 vorgesehene zweiwöchige Frist greift als Ausschlussfrist mithin nur im Falle der Benachrichtigung ein, was durch die Verwendung der Wörter „bis zu“ zum Ausdruck gebracht wird.

Es ist erwogen worden, auf die Befristung des Rechtsbehelfs entsprechend der Regelung in § 98 Abs. 2 StPO zu verzichten. Dagegen spricht jedoch, dass es einer solchen zeitlichen Grenze mit Blick auf die – verfassungsrechtlich gebotene – Löschungsregelung in Absatz 10 bedarf. Das Bundesverfassungsgericht hat in seinem Urteil zur akustischen Wohnraumüberwachung ausgeführt, dass eine Löschung erst dann in Betracht kommt, wenn sichergestellt ist, dass die Daten für eine gerichtliche Nachprüfung der Rechtmäßigkeit der Maßnahme nicht oder nicht mehr benötigt werden (BVerfG, 1 BvR 2378/98 vom 3.3.2004, Absatz-Nr. 350). Ein unbefristeter Rechtsbehelf würde daher einer Löschung dauerhaft entgegenstehen, obgleich auch die Löschung grundsätzlich verfassungsrechtlich geboten ist, sobald die erhobenen Daten für nicht mehr benötigt werden (BVerfG, a. a. O., Absatz-Nr. 349). Dieser Zielkonflikt zwischen Löschungsgebot einerseits und Aufbewahrungsgebot für Rechtsbehelfszwecke kann sachgerecht nur mit einer Befristung der Rechtsbehelfsmöglichkeit gelöst werden.

Satz 2 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 das Amtsgericht am Sitz der Staatsanwaltschaft, im Fall der akustischen Wohnraumüberwachung die in § 74a Abs. 4 GVG genannte Kammer des Landgerichts. Dies erscheint sachgerecht, weil mit dem nachträglichen Rechtschutz nach Absatz 9 das bei verdeckten Maßnahmen zunächst nicht mögliche rechtliche Gehör des Betroffenen nachgeholt werden soll.

Satz 3 ermöglicht im Wege der sofortigen Beschwerde eine Überprüfung der im Rahmen nachträglichen Rechtsschutzes ergehenden Entscheidung des Anordnungsgerichts. Die sofortige Beschwerde ist auch gegen Entscheidungen des Ermittlungsrichters des Bundesgerichtshofs und der Oberlandesgerichte zulässig (vgl. § 304 Abs. 4 Satz 2 Nr. 1 und Abs. 5 StPO-E).

Satz 4 trifft für den Fall, dass bereits Anklage erhoben und der Angeklagte benachrichtigt worden ist, aus Gründen der Zweckmäßigkeit und Effizienz eine Sonderregelung zur gerichtlichen Zuständigkeit dahingehend, dass über den Antrag auf nachträglichen Rechtsschutz das mit der Sache befasste Gericht in der das Verfahren abschließenden Entscheidung (z. B. dem Urteil) befindet. Dies kann, wenn der Antrag auf nachträglichen Rechtsschutz bereits vor Anklageerhebung bzw. vor der Benachrichtigung des Angeklagten angebracht worden ist, zu einem Übergang der gerichtlichen Entscheidungszuständigkeit führen.

Erwogen wurde, die Zuständigkeitsregelung in Satz 4 auf den Fall zu beschränken, dass der Angeklagte um nachträglichen Rechtsschutz nachsucht. Dies hätte allerdings zur Folge, dass für entsprechende Rechtsschutzbegehren anderer Betroffener weiterhin das Anordnungsgericht zuständig bliebe. Dies erscheint im Sinne einer effizienten Verfahrensweise sowie zur Vermeidung divergierender Entscheidungen aber nicht ratsam.

Zu § 101 Abs. 10 StPO-E

Absatz 10 trifft eine dem aufzuhebenden § 100d Abs. 5 StPO nachgebildete – redaktionell noch klarer gefasste – Regelung über die Löschung nicht mehr benötigter personenbezogener Daten, die aus einer der in Absatz 1 genannten Maßnahmen erlangt worden sind.

Erwogen wurde, insoweit auch feste Löschungsprüffristen vorzusehen, wie sie etwa in § 489 Abs. 4 StPO enthalten sind. Im Ergebnis wurde hiervon aber mangels Erforderlichkeit abgesehen:

- Soweit die aus verdeckten Ermittlungsmaßnahmen erlangten personenbezogenen Daten im Einzelfall in Dateien gespeichert sind, finden die Löschungsprüffristen nach § 489 Abs. 4 StPO sowie korrespondierende Fristen in anderen Vorschriften (z. B. § 32 Abs. 3 BKAG) ohnehin Anwendung, so dass es der zusätzlichen Regelung einer Löschungsprüffrist in § 101 Abs. 10 StPO-E nicht bedarf.

- Soweit die aus verdeckten Ermittlungsmaßnahmen erlangten personenbezogenen Daten im Einzelfall hingegen in der Strafakte enthalten sind, unterliegt diese Akte einer fortlaufenden Kontrolle durch die aktenbearbeitende Stelle. Insbesondere hat nach rechtskräftigem Abschluss des Strafverfahrens eine Überprüfung dahingehend stattzufinden, ob und welche Aktenbestandteile und Asservate aufzubewahren, herauszugeben oder zu vernichten sind. Anhaltspunkte dafür, dass dieser gebotenen Vorgehensweise in der Praxis keine hinreichende Beachtung geschenkt würde, liegen nicht vor.

Zu Nummer 12 (§ 110 Abs. 3 StPO-E)

§ 110 StPO erlaubt die Durchsicht von Datenträgern, um festzustellen, ob sie Informationen enthalten, die für das Strafverfahren von Bedeutung sind und daher eine Beschlagnahme des Datenträgers in Betracht kommt. Die Vorschrift macht damit z. B. die Beschlagnahme umfangreicher Aktenbestände entbehrlich, in denen einzelne beweisrelevante Dokumente vermutet werden. Dieser Gedanke gilt auch für elektronische Datenträger. Dort besteht allerdings die Besonderheit, dass das Speichermedium mit dem Zugangsgerät keine räumliche Einheit bilden muss. Eine Beschlagnahme des Zugangsgeräts als solches ist daher u. U. nutzlos. Die Beschlagnahme des Speichermediums kann aufgrund der räumlichen Trennung – ggf. muss erst ermittelt werden, wo sich das Speichermedium befindet – mitunter nur mit erheblicher zeitlicher Verzögerung erfolgen. Auch rechtlich ist eine Beschlagnahme des Speichermediums aufgrund von Gefahr im Verzug wegen der engen Auslegung dieses Begriffs durch das Bundesverfassungsgericht (vgl. BVerfGE 103, 142, 155 ff.) nicht unproblematisch. Dies begründet eine erhebliche Gefahr des Beweismittelverlusts, weil beweisrelevante Daten nach Bekanntwerden der – offen durchzuführenden (vgl. BGH, Beschluss vom 31. Januar 2007 − StB 18/06) – Durchsuchungsmaßnahme vom Speichermedium gelöscht werden können, bevor dieses beschlagnahmt werden kann. Die neue Vorschrift des § 110 Abs. 3 StPO-E erlaubt daher, die Durchsicht elektronischer Datenträger auf räumlich getrennte Speichereinheiten, zu denen der Betroffene den Zugriff zu gewähren berechtigt ist, zu erstrecken, um festzustellen, ob dort beweisrelevante Daten gespeichert sind. Da dieses Vorgehen weniger eingriffsintensiv als die Beschlagnahme des Datenträgers ist, wird damit der Grundsatz der Verhältnismäßigkeit besonders berücksichtigt. Daten, die für die Untersuchung von Bedeutung sein können, dürfen nach Satz 2 der Vorschrift gespeichert werden, wenn bis zur Sicherstellung der Datenträger ihr Verlust zu besorgen ist. Sie sind zu löschen, sobald sie für die Strafverfolgung nicht mehr erforderlich sind.

Durch diese Befugnis zur vorläufigen Sicherung der Daten wird auch der Forderung von Artikel 19 Abs. 2 des Übereinkommens über Computerkriminalität entsprochen. Dort haben sich

die Vertragsparteien verpflichtet, die erforderlichen gesetzgeberischen Maßnahmen zu treffen, um sicherzustellen, dass ihre Behörden, wenn sie ein bestimmtes Computersystem oder einen Teil davon durchsuchen oder in ähnlicher Weise darauf Zugriff nehmen und Grund zu der Annahme haben, dass die gesuchten Daten in einem anderen Computersystem oder einem Teil davon innerhalb ihres Hoheitsgebiets gespeichert sind, und diese Daten von dem ersten System aus rechtmäßig zugänglich oder verfügbar sind, die Durchsuchung oder den ähnlichen Zugriff rasch auf das andere System ausdehnen können.

Nicht erlaubt wird durch § 110 Abs. 3 StPO-E der heimliche Online-Zugriff auf zugangsgeschützte Datenbestände im Sinne eines mitunter so genannten „staatlichen Hackings“ oder einer heimlichen Online-Durchsuchung. Der Online-Zugriff auf öffentlich zugängliche Datenbestände, die keiner besonderen Zugangsberechtigung bedürfen, erfordert hingegen keine besondere Ermächtigungsgrundlage.

Soweit § 110 Abs. 3 Satz 1 StPO-E darauf abstellt, dass der Betroffene den Zugang zu gewähren berechtigt sein muss, bedeutet dies nicht, dass die Maßnahme nur zulässig wäre, wenn der Betroffene der Strafverfolgungsbehörde den Zugang auch tatsächlich gewährt. Vielmehr handelt es sich auch bei diesem Teil der Durchsuchung um eine gegenüber dem Betroffenen zwangsweise durchsetzbare Maßnahme.

Andererseits soll die Regelung – wie bereits dargelegt – keine heimliche Online-Durchsuchung erlauben. Als eine solche heimliche Maßnahme könnte sich die Online-Durchsuchung aber gegenüber demjenigen darstellen, in dessen Gewahrsam die online zugänglichen Daten gespeichert sind. Dies wird etwa bei so genannten Telearbeitsplätzen der Fall sein, wenn der Arbeitgeber dem Arbeitnehmer gestattet, von zu Hause aus auf im Betrieb gespeicherte Daten online zuzugreifen. In einer solchen Fallgestaltung ist der Arbeitnehmer regelmäßig nicht berechtigt, diesen Zugang auch anderen Personen zu gewähren, so dass es an der von Absatz 3 Satz 1 vorausgesetzten Berechtigung zur Zugangsgewährung fehlt. Anderes sind hingegen die von Absatz 3 Satz 1 erfassten Fallgestaltungen zu beurteilen, in denen der Betroffene frei darüber befinden kann, ob er auch dritten Personen den Zugang zu den andernorts gespeicherten Daten ermöglichen will. Dies wird etwa der Fall sein, wenn der Betroffene von einem entsprechenden Anbieter online zugänglichen Speicherplatz gemietet hat. In solchen Fällen steht es dem Betroffenen regelmäßig frei, auch dritten Personen den Zugang zu den virtuell gespeicherten Daten zu ermöglichen. Eben solche und ähnliche Fälle werden von § 110 Abs. 3 StPO-E erfasst.

Zu Nummer 13 (§§ 110d, 110e StPO-E)

Zu § 110d StPO-E

§ 110d StPO wird aufgehoben, weil sein Regelungsgegenstand (Benachrichtigung, getrennte Aktenführung) nunmehr in den allgemeinen Regelungen des § 101 Abs. 2 und 4 bis 8 StPO-E enthalten ist.

Zu § 110e StPO-E

Die Verwendungsregelung des § 110e StPO entfällt; ihr Regelungsgehalt wird ersetzt und ergänzt durch die allgemeinen Verwendungsregelungen in § 161 Abs. 2 und § 477 Abs. 2 Satz 2 und 3 StPO-E.

Zu Nummer 14 (§ 161 StPO-E)

Zu Buchstabe a (Absatz 2 – neu)

Der neu eingefügte Absatz 2 Satz 1 regelt die Verwendung von Daten, die durch andere – nicht strafprozessuale – hoheitliche Maßnahmen erlangt wurden. Gedanklicher Anknüpfungspunkt der Vorschrift ist die Idee des so genannten hypothetischen Ersatzeingriffs. Sofern die Erhebung von Daten durch strafprozessuale Maßnahmen nur bei Verdacht bestimmter Straftaten zulässig ist und personenbezogene Daten, die durch entsprechende Maßnahmen nach anderen Gesetzen erlangt wurden, in Strafverfahren verwendet werden sollen, ist diese Verwendung zu Beweiszwecken nur zulässig, wenn sie zur Aufklärung einer Straftat dient, aufgrund derer eine solche Maßnahme nach der Strafprozessordnung angeordnet werden dürfte. Die Vorschrift generalisiert im Sinne einer Gleichbehandlung aller vom Verdacht bestimmter Straftaten abhängiger Ermittlungsmaßnahmen den bereits in § 100d Abs. 6 Nr. 3 StPO (§ 100f Abs. 2 StPO a. F.) angelegten Gedanken, um dem datenschutzrechtlichen Zweckbindungsgrundsatz in angemessener Weise Rechnung zu tragen. Wird die Zulässigkeit einer Ermittlungshandlung durch eine gesetzgeberische Wertung vom Vorliegen des Verdachts bestimmter Straftaten abhängig gemacht, so erlauben solche Befugnisse regelmäßig schwerwiegende Eingriffe in grundrechtlich geschützte Positionen, insbesondere in das Recht auf informationelle Selbstbestimmung. Die der Erlangung der Daten zugrunde liegende gesetzgeberische Wertung muss auch für die weitere, Beweiszwecken dienende Verwendung der Daten, durch die der ursprüngliche Eingriff noch vertieft werden kann, gel-

ten (vgl. BVerfGE 100, 313, 360; 109, 279, 375 f.). Werden Daten aus vergleichbaren Maßnahmen nach anderen Gesetzen (etwa den Polizeigesetzen oder den Gesetzen über die Nachrichtendienste) in das Strafverfahren eingeführt, so gilt das auch für deren Verwendung, um einer Umgehung der engen strafprozessualen Anordnungsvoraussetzungen vorzubeugen.

Soweit die Verwendung der Daten im Strafverfahren nicht zu Beweiszecken, sondern etwa als weiterer Ermittlungsansatz (Spurenansatz) oder zur Ermittlung des Aufenthaltsortes eines Beschuldigten erfolgen soll, greifen diese Beschränkungen allerdings nicht. Rechtmäßig gewonnene Zufallserkenntnisse, die nicht Katalogtaten betreffen, dürfen nach der gefestigten und vom Bundesverfassungsgericht gebilligten fachgerichtlichen Rechtsprechung zwar nicht zu Beweiszwecken – d. h. im Rahmen der Beweisaufnahme in der Hauptverhandlung (§§ 243 ff. StPO) – verwertet werden; sie können aber Anlass zu weiteren Ermittlungen zur Gewinnung neuer Beweismittel sein (BVerfG, 2 BvR 866/05 vom 29. Juni 2005, NJW 2005, 2766 ff., m. w. N.; vgl. auch die Ausführungen und Nachweise zu § 477 Abs. 2 StPO-E). Diese Rechtsprechung berücksichtigt einerseits den Schutz etwa des Grundrechts aus Artikel 10 Abs. 1 GG, indem weitergehende Ermittlungen nur in den Fällen für zulässig gehalten werden, in denen die Maßnahme nach § 100 a StPO rechtmäßig war; andererseits wird auch das Interesse an einer wirksamen Strafrechtspflege hierdurch berücksichtigt.

Begrenzt auf Maßnahmen nach

- § 98a (Rasterfahndung),

- § 100f StPO-E (§ 100f Abs. 2 StPO bzw. § 100c Abs. 1 Nr. 2 a. F. – akustische Überwachung mit technischen Mitteln außerhalb von Wohnungen) und

- § 110a StPO (Einsatz eines Verdeckten Ermittlers)

war eine ähnliche Regelung bereits im Entwurf des Strafverfahrensänderungsgesetzes 1999 – StVÄG 1999 – vorgesehen (vgl. BT-Drs. 14/1484, S. 6, 23). Sie wurde aber im Vermittlungsausschuss wieder gestrichen (BT-Drs. 14/3525, S. 2). Aufgrund der zwischenzeitlich ergangenen Rechtsprechung des Bundesverfassungsgerichts und dem Ziel einer Harmonisierung des Rechts der verdeckten Ermittlungsmaßnahmen und Verbesserung des Rechtsschutzes Betroffener folgend ist eine solche Regelung nunmehr geboten.

Satz 2 bestimmt, dass die besondere Verwendungsregelung bei Maßnahmen der akustischen Wohnraumüberwachung in § 100d Abs. 5 Nr. 3 StPO-E unberührt bleibt, mithin § 161 Abs. 2 Satz 1 StPO vorgeht.

Zu Buchstabe b (Absatz 3 – neu, bisheriger Absatz 2)

Der Begriff „Informationen“ im bisherigen Absatz 2, der zu Absatz 3 wird, wird in redaktioneller Anpassung an die gängige datenschutzrechtliche Terminologie durch den Begriff „Daten“ ersetzt.

Zu Nummer 15 (§ 162 StPO-E)

Zu Absatz 1

Absatz 1 wird zu einer Konzentrationsregelung umgestaltet, der zufolge die Staatsanwaltschaft Anträge auf gerichtliche Untersuchungshandlungen grundsätzlich bei dem Amtsgericht zu stellen hat, in dessen Bezirk sie ihren Sitz hat; wird der Antrag durch eine Zweigstelle der Staatsanwaltschaft gestellt, so ist er bei dem Amtsgericht zu stellen, in dessen Bezirk die Zweigstelle ihren Sitz hat (Satz 1). Durch diese praktisch bedeutsame Regelung wird die Bestimmung der ermittlungsgerichtlichen Zuständigkeit erheblich vereinfacht und beschleunigt, was nach derzeitiger Rechtslage nur in den Verfahren möglich ist, in denen mehrere Untersuchungshandlungen vorzunehmen sind. Auch kann auf diese Weise die notwendige Bereitstellung eines gerichtlichen Bereitschaftsdienstes (vgl. BVerfGE 100, 313, 401; 103, 142, 152; 105, 239, 248; 109, 279, 358; BVerfGK 2, 176, 179) besser sichergestellt werden, da er bei Gerichten in kleineren Amtsgerichtsbezirken aufgrund der dort typischerweise gegebenen Personalsituation mit zumutbarem Aufwand oftmals nicht gewährleistet werden kann. Durch die Konzentration der Zuständigkeit kann auch eine Kompetenzbündelung gerade für die Anordnung von Ermittlungsmaßnahmen mit technischem Hintergrund und dadurch eine Verbesserung des Rechtsschutzes Betroffener erreicht werden.

Satz 2 sieht Ausnahmen von dieser Konzentrationsregelung für gerichtliche Vernehmungen und Augenscheinnahmen zum Zweck der Verfahrensbeschleunigung und im Interesse Betroffener vor, wenn diesen nicht zugemutet werden kann, in den Amtsgerichtsbezirk, in dem die Staatsanwaltschaft ihren Sitz hat, anzureisen (vgl. RiStBV Nr. 4c, 19a). Eine weitere Ausnahme im Sinne einer Eilzuständigkeit eines anderen Gerichts erscheint im Hinblick dar-

auf, dass in Eilfällen regelmäßig auch eine Eilkompetenz der Staatsanwaltschaft oder ihrer Ermittlungspersonen gegeben ist, nicht erforderlich.

Sonderregelungen, die die Zuständigkeit des Ermittlungsgerichts abweichend von der generellen Bestimmung des § 162 StPO-(E) regeln (wie z. B. § 125 StPO), gehen auch weiterhin als speziellere Regelung § 162 StPO-E vor (vgl. Meyer-Goßner, a. a. O., § 162 Rn. 8).

Zu Absatz 2

Die bisherige Regelung in § 162 Abs. 2 StPO entfällt als Konsequenz der Änderung in Absatz 1. Der bisherige Absatz 3 wird daher zum neuen Absatz 2 und hierbei redaktionell angepasst.

Zu Nummer 16 (§ 163d StPO-E)

Zu Buchstabe a (Absatz 1)

Die redaktionelle Folgeänderung in Absatz 1 Satz 1 Nr. 2 trägt der Neufassung des § 100a StPO-E Rechnung.

Zu Buchstabe b (Absatz 4 und 5)

Die Verwendungsregelungen in Absatz 4 Satz 4 und 5 entfallen; ihr Regelungsgehalt wird ersetzt und ergänzt durch die umfassenden Verwendungsregelungen in § 161 Abs. 2 und § 477 Abs. 2 und 3 StPO-E. Die Benachrichtigungspflicht in Absatz 5 StPO wird ersetzt durch die allgemeine Regelung in § 101 Abs. 4 bis 8 StPO-E.

Zu Nummer 17 (§ 163e StPO-E)

Zu Buchstabe a (Absatz 3)

Die Ersetzung des Wortes „Informationen“ durch das Wort „Daten“ in Absatz 3 dient der Vereinheitlichung der Begrifflichkeiten innerhalb der Strafprozessordnung.

Zu Buchstabe b (Absatz 4)

Durch die Ersetzung der Formulierung „den Richter“ durch „das Gericht“ und „richterliche“ durch „gerichtliche“ in Satz 1, 3 und 4 wird § 1 Abs. 2 BGleiG Rechnung getragen.

Der bisherige Verweis auf § 100b Abs. 1 Satz 5 StPO in Satz 6 wird aus Gründen der besseren Lesbarkeit ausformuliert. Auch wäre die mit einer Beibehaltung des Verweise aufgrund der Neuregelung in § 100b Abs. 1 Satz 5 StPO-E verbundene Verkürzung der Verlängerungsfrist auch bei der Ausschreibung zur polizeilichen Beobachtung nicht sachgerecht.

Zu Nummer 18 (§ 163f StPO-E)

Zu Buchstabe a (Absatz 3)

Um einen effektiven vorbeugenden Rechtsschutz der von einer längerfristige Observation nach § 163f StPO Betroffenen zu gewährleisten, wird die Anordnung einer solchen Maßnahme in Satz 1 dem Richtervorbehalt unterstellt. Eine Eilkompetenz verbleibt für die Staatsanwaltschaft und ihre Ermittlungspersonen. Ein Richtervorbehalt ist hier mit Blick auf das Ziel der Harmonisierung der verdeckten Ermittlungsmaßnahmen notwendig, weil die längerfristige Observation im Einzelfall mit erheblichen Eingriffen in das Recht auf informationelle Selbstbestimmung des Betroffenen verbunden sein und mit Blick auf die Problematik der Kumulierung von Ermittlungsmaßnahmen (vgl. BVerfG, 2 BvR 581/01 vom 12. April 2005, Absatz-Nr. 60 ff., NJW 2005, 1338, 1341), insbesondere durch den Einsatz technischer Mittel (§ 100h Abs. 1 Nr. 2 StPO-E, § 100f Abs. 1 Nr. 2 StPO), eine Eingriffsintensität erreichen kann, die eine staatsanwaltliche Anordnung nicht mehr als ausreichend erscheinen lässt. Das anordnende Gericht muss auch als Sachwalter der Rechte der Betroffenen von solchen Maßnahmen mit hoher Eingriffsintensität Kenntnis haben, damit den speziellen Subsidiaritätsklauseln, die die Befugnisse zur Vornahme verdeckter Ermittlungen enthalten, Rechnung getragen werden kann. Eine Anordnung der Maßnahme durch das Gericht ist auch praktisch ohne weiteres möglich, weil sie während des Laufs einer kurzfristigen Observation erfolgen kann, die bereits auf Grundlage der §§ 161, 163 StPO zulässig ist, und zudem bei Gefahr im Verzug eine Eilanordnungskompetenz der Staatsanwaltschaft und ihrer Ermittlungsbeamten verbleibt.

Satz 2 regelt entsprechend § 100b Abs. 1 Satz 3 Halbsatz 1 das Außerkrafttreten der Eilanordnung der Staatsanwaltschaft oder ihrer Ermittlungspersonen, wenn die Anordnung nicht binnen drei Werktagen vom Gericht bestätigt wird.

Satz 3 ersetzt den bisherigen Absatz 4, indem er § 100b Abs. 1 Satz 3 Halbsatz 2, Satz 4, 5 und Abs. 2 Satz 1 für entsprechende anzuwenden erklärt. Daraus ergibt sich, dass

- die aufgrund einer Eilanordnung erlangten personenbezogenen Daten nicht zu Beweiszwecken verwertet werden dürfen, wenn Gefahr im Verzug nicht bestand (§ 100b Abs. 1 Satz 3 Halbsatz 2),
- die Anordnung einer längerfristigen Observation auf maximal zwei Monate zu befristen ist (§ 100b Abs. 1 Satz 4),
- Verlängerungen der Anordnung um jeweils nicht mehr als zwei Monate zulässig sind, wenn die Voraussetzungen der Anordnung unter Berücksichtigung der gewonnenen Ermittlungsergebnisse fortbestehen (§ 100b Abs. 1 Satz 5), und
- die Anordnung schriftlich zu ergehen hat (§ 100b Abs. 2 Satz 1).

Zu Buchstabe b (Absatz 4)

Die bisherigen Regelungen in Absatz 4 werden in Folge der Neufassung des Absatzes 3 entbehrlich, so dass Absatz 4 aufgehoben wird:

Die bislang in Satz 1 enthaltene Verpflichtung der Staatsanwaltschaft oder ihrer Ermittlungspersonen, die Anordnung unter Angabe der maßgeblichen Gründe aktenkundig zu machen, entfällt aufgrund der Einführung des Richtervorbehalts in Absatz 3 Satz 1; für die künftig notwendige gerichtliche Anordnung ergibt sich die Begründungspflicht bereits aus § 34 StPO.

Die bisher in Satz 2 bestimmte Anforderung, dass eine Verlängerung der Maßnahme nur durch das Gericht getroffen werden kann, bedarf es nicht mehr, da dies nunmehr bereits aus dem in Absatz 3 Satz 1 enthaltenen Richtervorbehalt folgt.

Zu Nummer 19 (§ 304 StPO-E)

Die Ergänzungen in § 304 Abs. 4 Nr. 1 und Abs. 5 regeln, dass im Falle des nachträglichen Rechtsschutzes nach § 101 Abs. 9 StPO-E die dort in Satz 3 eröffnete sofortige Beschwerde

auch gegen Entscheidungen und Verfügungen des Oberlandesgerichts sowie des Ermittlungsrichters des Oberlandesgerichts oder des Bundesgerichtshofs nicht ausgeschlossen ist.

Zu Nummer 20 (§ 477 StPO-E)

Zu Buchstabe a (Absatz 2)

Die Neufassung des Absatzes 2 trifft insbesondere in den Sätzen 3 und 4 eine allgemeine Regelung über eine verfahrensübergreifende Verwendung von personenbezogenen Daten, die aus Maßnahmen erlangt worden sind, welche nur bei Verdacht bestimmter Straftaten zulässig sind. Die Verwendung von Erkenntnissen aus entsprechenden Maßnahmen im selben (Ausgangs-)Strafverfahren unterliegt hingegen nicht den – die Verwertung beschränkenden – Regelungen des § 477 Abs. 2 StPO(-E). Insbesondere steht einer Verwertung entsprechender Erkenntnisse im Ausgangsverfahren nicht entgegen, dass sich der Verdacht einer Katalogstraftat nicht bestätigt hat. In rechtmäßiger Weise erlangte Erkenntnisse sind im Ausgangsverfahren – sowohl als Spurenansatz als auch zu Beweiszwecken – sowohl hinsichtlich anderer Begehungsformen der zunächst angenommenen Katalogtat als auch hinsichtlich sonstiger Straftatbestände und anderer Tatbeteiligten insoweit verwertbar, als es sich noch um dieselbe Tat im prozessualen Sinn handelt (vgl. beispielhaft für Erkenntnisse aus einer Maßnahme nach § 100a Meyer-Goßner, a. a. O., § 100a, Rn. 14 ff. m. w. N.; Allgayer, NStZ 2006, 603 ff. m. w. N.).

Für die von § 477 Abs. 2 StPO geregelte verfahrensübergreifende Verwertung sieht der Entwurf im Einzelnen folgende Änderungen vor:

Der bisherige Satz 1 wird unverändert übernommen.

Als neuer Satz 2 wird eine besondere Verwendungsregelung eingefügt, die die Verwendung von personenbezogenen Daten, die durch strafprozessuale Maßnahmen erlangt wurden, die nur bei Verdacht bestimmter Straftaten zulässig sind, für Beweiszwecke in einem anderen Strafverfahren regelt. Der Vorschrift, die auf Regelungsvorbilder in § 98b Abs. 3 Satz 3, § 100b Abs. 5, § 100d Abs. 5 a. F., § 100h Abs. 3 und § 110e StPO sowie auf eine gefestigte fachgerichtliche Rechtsprechung (BGHSt 26, 298, 303; 27, 355, 358; 28, 122, 125 ff.; BGHR StPO § 100a Verwertungsverbot 4, 5, 10) zurückgeht, liegt der Gedanke des „hypothetischen Ersatzeingriffs“ zugrunde. Insoweit wird auf die Ausführungen zu § 161 Abs. 2 StPO-E verwiesen.

Der bisherige weitere Regelungsgehalt des Satzes 2 wird im Wesentlichen unverändert in die in Satz 3 Nr. 1 und 2 enthaltene besondere Verwendungsregelung übernommen und mit Blick auf eine Harmonisierung mit § 161 Abs. 2 und § 477 Abs. 2 Satz 2 StPO-E allgemein gefasst. Hierbei wird klargestellt, dass eine ohne Einwilligung der betroffenen Personen erfolgende Verwendung der in Satz 2 umschriebenen Daten zur Abwehr einer erheblichen Gefahr nur dann zulässig ist, wenn sich diese Gefahr auf die öffentliche Sicherheit bezieht. Bloße Gefahren für die öffentliche Ordnung genügen, auch wenn sie erheblich sind, künftig nicht mehr. Ferner wird die bisherige Beschränkung der Regelung auf personenbezogene Daten, die „erkennbar“ aus den in Bezug genommenen Maßnahmen erlangt worden sind, beseitigt. Die Schutzbedürftigkeit und damit die beschränkte Verwendbarkeit der Daten kann nicht von dieser Erkennbarkeit abhängig sein. Vielmehr wird die Erkennbarkeit in diesem Sinne künftig durch die in § 101 Abs. 3 StPO-E vorgesehenen Kennzeichnungspflichten sichergestellt.

Satz 3 Nr. 3 knüpft an den bisherigen Satz 3 an und regelt, dass eine Verwendung personenbezogener Daten, die durch nur bei Verdacht bestimmter Straftaten zulässige strafprozessuale Maßnahmen erlangt wurden, auch für Forschungszwecke nach Maßgabe des § 476 StPO verwendet werden dürfen. Die bisherige Einschränkung, dass Gegenstand der Untersuchung eine der im bisherigen Satz 2 genannten Vorschriften sein muss, entfällt, da ihr im Hinblick auf die insoweit in § 476 Abs. 1 Satz 1 Nr. 1 vorausgesetzte Erforderlichkeit der Datenübermittlung für den jeweiligen Forschungszweck keine sinnvolle eigenständige Bedeutung zukommt.

Von den in den Sätzen 1 bis 3 enthaltenen Verwendungsbeschränkungen ausgenommen blieben auch weiterhin die nach Maßgabe des § 406e StPO dem durch die Straftat Verletzten zustehende Rechte auf Akteneinsicht durch einen Rechtsanwalt sowie auf die Erteilung von Auskünften und Abschriften aus den Akten. Dass die Verwendungsbeschränkungen des § 477 Abs. 2 StPO(-E) insoweit keine Anwendung finden, folgt im Wege des Gegenschlusses aus dem in § 406e Abs. 6 enthaltenen ausschließlichen Verweis auf die Zweckbindungsregelung des § 477 Abs. 5 StPO. Im Zusammenhang mit den für die Telekommunikationsüberwachung in § 100a Abs. 2 Nr. 2 StPO-E neu aufgenommnen Anlassstraftaten nach der Abgabenordnung besteht damit künftig nach Maßgabe des § 406e StPO die Möglichkeit, der zuständigen Finanzbehörde für Zwecke des Besteuerungsverfahrens auch Erkenntnisse etwa aus Telekommunikationsüberwachungsmaßnahmen zu übermitteln, soweit der Gesetzgeber der Abgabenordnung sich entschließen sollte, die Verwendung solcher Daten im Besteuerungsverfahren zuzulassen.

Satz 4 stellt durch die Bezugnahme auch auf § 100d Abs. 5 StPO-E klar, dass die in dieser Vorschrift enthaltenen besonderen Verwendungsregelungen für personenbezogene Daten, die aus einer akustischen Wohnraumüberwachung erlangt wurden, der allgemeinen Regelung des § 477 Abs. 2 StPO-E vorgehen, also leges speciales hierzu sind. Die bisher in Satz 4 enthaltene Bezugnahme auf § 481 StPO entfällt: Zum einen sind die in § 481 StPO enthaltenen Bestimmungen über die Verwendung personenbezogener Informationen aus Strafverfahren durch die Polizeibehörden auch ohne die bisherige Bezugnahme anwendbar. Zum anderen verweist aber § 481 Abs. 2 StPO seinerseits auf besondere bundesgesetzliche Verwendungsregelungen und damit auch auf § 477 Abs. 2 StPO-E (zu den daraus bislang resultierenden Unsicherheiten zum Regelungsgehalt der Unberührtheitsklausel vgl. Weßlau, in: Systematischer Kommentar zur StPO, § 477 StPO, Rn. 27 m. w. Nw.). Durch die Streichung der Bezugnahme auf § 481 StPO ergibt sich nunmehr ein klares und stimmiges Regelungskonzept: Die Polizeibehörden dürfen nach Maßgabe der Polizeigesetze personenbezogene Informationen aus Strafverfahren verwenden (§ 481 Abs. 1 Satz 1 StPO). Zu diesem Zweck dürfen ihnen entsprechende Informationen übermittelt werden (§ 481 Abs. 1 Satz 2 StPO). Bei der Verwendung - und damit auch bei der Übermittlung - sind aber stets die besonderen bundes- oder landesgesetzlichen Verwendungsregelungen - und damit insbesondere auch die in § 477 Abs. 2 Satz 3 Nr. 1 StPO-E enthaltene Verwendungsbeschränkung - zu beachten (§ 481 Abs. 2 StPO).

Zu Buchstabe b (Absatz 5)

Die Ersetzung des Wortes „Informationen“ durch das Wort „Daten“ in Absatz 5 dient der Vereinheitlichung der Terminologie innerhalb der Strafprozessordnung.

Zu Artikel 2 (Änderung des Telekommunikationsgesetzes)

Zu Nummer 1 (§ 97 TKG-E)

Zu Buchstabe a (Absatz 3)

Nach Maßgabe der Richtlinie 2006/24/EG werden künftig bestimmte Arten von Verkehrsdaten für bestimmte Zeit zu speichern sein. Die hiervon betroffenen Datenarten und die Speicherungsdauer werden in § 113a TKG-E festgelegt. § 97 Abs. 3 Satz 3 TKG-E stellt klar, dass nicht von der Speicherungspflicht des § 113a TKG-E erfasste Verkehrsdaten weiterhin grundsätzlich unverzüglich zu löschen sind. Die allein aus Gründen der klareren sprachlichen

Darstellung des Regelungsziels erfolgte Neufassung der Sätze 2 und 3 macht eine Anpassung des Verweises in Absatz 3 Satz 4 erforderlich.

Zu Buchstabe b (Absatz 4)

Die bisherigen Sätze 1 und 2 in Absatz 4 sind aufzuheben, weil sie der zur Umsetzung der Richtlinie 2006/24/EG einzufügenden Vorschrift des § 113a Abs. 2 Nr. 1 TKG-E widersprechen, nach der Rufnummern und andere Anschlusskennungen künftig ungekürzt zu speichern sind. Der bisherige Satz 3 hat die Bekanntgabe von Rufnummern ankommender Verbindungen zum Gegenstand, für die der angerufene Teilnehmer entgeltpflichtig ist. Diese Regelung ist bereits systematisch richtig in § 99 Abs. 1 Satz 7 TKG-E eingestellt und daher in § 97 Abs. 4 TKG zu streichen. Als Folgeänderung hierzu entfällt auch Satz 4, so dass Absatz 4 insgesamt aufzuheben ist.

Zu Buchstabe c (Absätze 5 und 6)

Es handelt sich um eine Folgeänderung zur Aufhebung des Absatzes 4.

Zu Nummer 2 (§ 99 TKG-E)

Zu Buchstabe a (Absatz 1)

§ 99 Abs. 1 Satz 2 TKG-E stellt klar, dass der Teilnehmer für den Einzelverbindungsnachweis die Wahl hat, ob ihm die von seinem Anschluss aus gewählten Rufnummern entgeltpflichtiger Verbindungen ungekürzt oder um die letzten drei Ziffern gekürzt mitgeteilt werden. Eine Beschränkung auf die Mitteilung gekürzter Rufnummern erscheint insbesondere in Fällen von mitbenutzten Anschlüssen etwa in Haushalten oder in Unternehmen geeignet, sowohl Erstattungsansprüchen als auch datenschutzrechtlichen Aspekten in jeweils angemessener Weise Rechnung zu tragen. Durch die in Satz 8 neu aufgenommene Verweisung auf Satz 2 wird jedoch klargestellt, dass dieses Wahlrecht nicht besteht für Teilnehmer geschlossener Benutzergruppen, wenn der Diensteanbieter seinen Dienst nur Teilnehmern dieser Benutzergruppe anbietet.

Eine gesetzliche (Zweifels-)Regelung für den Fall, dass der Teilnehmer eine Wahl zwischen den vorgenannten Alternativen nicht trifft, erscheint dagegen – anders als ursprünglich erwogen – nicht erforderlich. Es ist vielmehr durch die Vertragsgestaltung zwischen Diensteanbie-

ter und Teilnehmer sicherzustellen, dass der Teilnehmer eine Wahl für oder gegen die Mitteilung ungekürzter Rufnummern trifft.

Bei den geänderten Verweisungen in Absatz 1 Satz 5 und 8 handelt es sich um redaktionelle Folgeanpassungen an die vorgenannten Änderungen. Die übrigen Vorschriften des Absatzes 1 bleiben unverändert.

Zu Buchstabe b (Absatz 3)

Es handelt sich um Folgeänderungen zu den Änderungen in Absatz 1.

Zu Nummer 3 (§ 110 TKG-E)

Zu Buchstabe a (Überschrift)

Die Änderung der Überschrift ist veranlasst, weil sich die Vorschrift des § 110 TKG nicht allein auf Vorgaben zur technischen Umsetzung von Überwachungsmaßnahmen beschränkt. Zum einen wird von den nach dieser Vorschrift Verpflichteten auch gefordert, bestimmte organisatorische Vorkehrungen zu treffen; zum anderen bezieht sich die Verordnungsermächtigung des Absatzes 2 nicht mehr allein auf die Umsetzung von Überwachungsmaßnahmen, sondern erfasst nunmehr auch die Erteilung von Auskünften.

Zu Buchstabe b (Absatz 2)

Die Erweiterung der Verordnungsermächtigung, auch Regelungen zu treffen über die Erteilung von Auskünften, ist wegen der in § 100g Abs. 1 StPO-E vorgesehenen Befugnis zur Erhebung von Verkehrsdaten in Echtzeit geboten. Die Festlegung hierdurch etwa veranlasster technischer und organisatorischer Anpassungen kann – ebenso wie bei den bestehenden Erfordernissen im Zusammenhang mit der Umsetzung von Überwachungsmaßnahmen, die ihre Regelung in der Telekommunikations-Überwachungsverordnung (TKÜV) gefunden haben – aufgrund der erforderlichen Detailgenauigkeit und technischen Ausgestaltung der Vorschriften angemessen nicht im Wege des förmlichen Gesetzes erfolgen, sondern ist auf den Verordnungsgeber zu übertragen. Eine inhaltliche Anpassung der TKÜV selbst bleibt insoweit jedoch einer künftigen Änderung vorbehalten.

Zu Buchstabe c (Absatz 8)

§ 110 Abs. 8 TKG ist im Hinblick auf die in § 100b Abs. 5 und 6 StPO-E neu aufgenommenen Pflichten zur Erhebung und Übermittlung statistischer Daten im Zusammenhang mit Maßnahmen der Telekommunikationsüberwachung aufzuheben, da diese Pflichten künftig öffentlichen Stellen (Länder, Generalbundesanwalt, Bundesamt für Justiz) obliegen werden. Die zu erfassenden Daten werden benötigt, um tragfähige rechtstatsächliche Erkenntnisse über die Anwendungshäufigkeit von Maßnahmen der Telekommunikationsüberwachung im Bereich der Strafverfolgung sowie über die Entwicklung dieses politisch sensiblen Bereichs zu gewinnen und um eventuellen Missbräuchen vorzubeugen (vgl. BT-Drs. 13/3609, S. 55, zu § 85 Abs. 5 TKG a. F.). Diese Statistik dient damit in erster Linie hoheitlichen Zwecken, so dass es geboten ist, die Daten von öffentlichen Stellen erheben und übermitteln zu lassen (so auch Klesczewski, in: Berliner Kommentar zum TKG, 2006, § 110, Rn. 67). Die Verlagerung dieser Pflichten auf öffentliche Stellen bewirkt zugleich eine Entlastung der bislang hierzu verpflichteten Diensteanbieter.

Zu Nummer 4 (§ 111 TKG-E)

Zu Buchstabe a (Absatz 1)

Die Untergliederung in Absatz 1 Satz 1 Nr. 1 bis 6 dient der besseren Übersichtlichkeit; dabei entsprechen die Nummern 1 bis 4 und 6 weitgehend der bisherigen Rechtslage, lediglich die weiteren Erhebungs- und Speicherungspflichten betreffend „andere Anschlusskennungen“ ergänzen die bestehenden Verpflichtungen. Diese Ergänzung trägt dem Umstand Rechnung, dass heute nicht mehr allein Rufnummern sondern – etwa bei der DSL-Technologie, deren Verbreitung derzeit rasant zunimmt – auch andere Kennungen zur Bezeichnung von Telekommunikationsanschlüssen vergeben werden, und daher etwa eine Ermittlung der Teilnehmerbestandsdaten allein auf Grundlage gespeicherter Rufnummern nicht mehr hinreichend gewährleistet ist.

Nummer 5 begründet eine weitere Erhebungs- und Speicherungsverpflichtung der Diensteanbieter. Danach haben die im Bereich der Mobilfunktelefonie tätigen Diensteanbieter künftig auch die Gerätenummern der von ihnen neben dem Mobilfunkanschluss überlassenen Mobilfunkgeräte (so genannte IMEI) zu erfassen und zu speichern, um Auskünfte nach den §§ 112 und 113 TKG erteilen zu können. Diese Informationen sind in den Fällen unverzichtbar, in denen Beschuldigte eine Mehrzahl von Mobilfunkkarten nutzen und somit

eine anschlussbezogene Auskunft oftmals kaum weiterführende Erkenntnisse erbringt (vgl. hierzu auch § 100b Abs. 2 Satz 2 Nr. 2 StPO-E und die Erläuterungen dazu).

Der bisherige Satz 2 wird unverändert übernommen.

Der neu eingefügte Satz 3 dient der Umsetzung von Vorgaben aus Artikel 5 Abs. 1 Buchstabe a Nr. 2 und Buchstabe b Nr. 2 der Richtlinie 2006/24/EG und schreibt die Speicherung bestimmter Kundendaten auch für den Bereich so genannter E-Mail-Konten vor, soweit diese Daten von dem E-Mail-Diensteanbieter ohnehin zu eigenen Zwecken erhoben werden. Eine Pflicht zur Erhebung dieser Daten wird nicht begründet.

Bei den Ergänzungen in Satz 4 (bislang Satz 3) handelt es sich um redaktionelle Folgeänderungen zu dem neu eingefügten Satz 3.

Der Regelungsinhalt der bisherigen Sätze 4 und 5 wird inhaltlich unverändert in die neuen Absätze 4 und 5 übernommen.

Zu den Buchstaben b und c (Absätze 2 und 3)

Es handelt sich jeweils um lediglich redaktionelle Folgeanpassungen.

Zu Buchstabe d (Absätze 4 und 5)

Aus Gründen der besseren Übersichtlichkeit wird die bisherige Regelung des Absatzes 1 Satz 4 zu Absatz 4 und die bisherige Regelung des Absatzes 1 Satz 5 zu Absatz 5.

Zu Nummer 5 (§ 112 TKG-E)

Zu Buchstabe a (Absatz 1)

Bei den Änderungen in Absatz 1 Satz 1 und 2 TKG-E handelt es sich um redaktionelle Folgeanpassungen an die Änderungen in § 111 TKG-E.

Zu Buchstabe b (Absatz 3)

Die Neufassung von Absatz 3 Satz 1 Nr. 3 betrifft die gesetzlichen Vorgaben zur Ausgestaltung der Ähnlichenfunktion durch die Rechtsverordnung nach Absatz 3. Die Erarbeitung eines Entwurfs für diese Rechtsverordnung hat Probleme im Zusammenhang mit der bisherigen Vorgabe aufgezeigt, wonach für die Ähnlichenfunktion bestimmte Zeichenfolgen festzulegen und in die – ansonsten bitgenaue – Suche einzubeziehen waren. Mit einem solchen Verfahren ließen sich nur vordefinierte Zeichenfolgen als ähnlich erkennen, nicht aber etwa sonstige Namensähnlichkeiten, Schreibfehler oder Buchstabenvertauschungen. Eine brauchbare Ähnlichenfunktion muss auch in der Lage sein, die in der zu suchenden Zeichenkette vorkommenden Zeichen und deren Position nach einem wissenschaftlichen Verfahren zu bewerten, das auch Fehlerquellen berücksichtigt, die typisch für menschliche Dateneingaben sind.

Diese Vorgabe wird nunmehr – deutlicher als bisher – in Absatz 3 Satz 1 Nr. 3 beschrieben. Die bisher in dem Halbsatz vor Buchstabe a enthaltene Regelung wird durch die Regelungen in den neuen Buchstaben b und c abgelöst. Buchstabe a bleibt mit seinem bisherigen Inhalt bestehen. Der Regelungsgehalt im bisherigen Buchstabe b findet sich in präzisierter Weise nunmehr im neuen Buchstaben d. Die im bisherigen Buchstaben c enthaltene Bestimmung zur Löschung nicht benötigter Datensätze ist bereits durch Absatz 1 Satz 5 so klar geregelt, dass kein Bedarf für eine Detailregelung in der Verordnung verbleibt.

Zu Buchstabe c (Absatz 4)

In Absatz 4 Satz 4 werden die von der Bundesnetzagentur bei Bestandsdatenabfragen nach § 112 TKG zu protokollierenden Datenarten aus Gründen eines besseren Datenschutzes präziser umschrieben und um Angaben zur Bezeichnung der ersuchenden Person ergänzt.

Zu Nummer 6 (§§ 113a und 113b TKG-E)

Zu § 113a TKG-E

§ 113a TKG-E dient als Kernregelung der Umsetzung der Artikel 3, 5, 6, 7 und 8 der Richtlinie 2006/24/EG, indem er die Adressaten sowie die Grundvoraussetzungen der Speicherungspflichten bestimmt, die zu speichernden Datenarten sowie die Speicherungsdauer festlegt und Vorgaben für den Umgang mit den gespeicherten Daten sowie für deren Löschung

macht. Da für die verschiedenen Telekommunikationsdienste unterschiedliche technische Gegebenheiten zu beachten sind, erfolgt eine nach einzelnen Telekommunikationsdiensten gegliederte Präzisierung der von der Richtlinie vorgegebenen jeweiligen Speicherungspflichten in den Absätzen 2 bis 4. Hieraus folgt jedoch nicht die Verpflichtung der Diensteanbieter, alle im Zuge der Nutzung des jeweiligen Telekommunikationsdienstes zu speichernden Daten zusammengefasst in einer gemeinsamen Datenbank aufzubewahren. Insoweit ist es den Diensteanbietern – in den Grenzen geltender Datenschutz- und Datensicherheitsbestimmungen – freigestellt, die einzelnen Datenarten nach Maßgabe ihrer jeweiligen Systemstrukturen und technischen Gegebenheiten in unterschiedlichen Datenbanken zu speichern, sofern dies dem Erfordernis unverzüglicher Auskunftserteilung nicht entgegen steht.

Zu Absatz 1

Absatz 1 Satz 1 beschreibt den Kreis der zur Speicherung Verpflichteten. Danach richten sich die Speicherungspflichten an diejenigen, die öffentlich zugängliche Telekommunikationsdienste für Endnutzer erbringen. Daraus folgt zugleich, dass für den nicht öffentlichen Bereich (z. B. unternehmensinterne Netze, Nebenstellenanlagen oder E-Mail-Server von Universitäten ausschließlich für dort immatrikulierte Studierende oder Bedienstete sowie die Telematikinfrastruktur im Gesundheitswesen) eine Speicherungspflicht nicht besteht. Satz 2 stellt klar, dass auch diejenigen Diensteanbieter zur Speicherung verpflichtet sind, die keine eigenen Telekommunikationsanlagen betreiben, sondern solche anderer Anbieter in Anspruch nehmen und daher nicht selbst Verkehrsdaten erzeugen oder verarbeiten. Auch in diesem Fall hat der Anbieter des Telekommunikationsdienstes die Speicherung der in dieser Vorschrift im Einzelnen aufgeführten Daten sicherzustellen. Auf welche Weise ein solcher Anbieter die Erfüllung der Speicherungspflichten sicherstellt, hat er auf Verlangen gegenüber der Bundesnetzagentur nachzuweisen.

Satz 1 bestimmt zudem, dass die betroffenen Diensteanbieter die in § 113a TKG-E genannten Daten nur dann zu speichern haben, wenn diese von ihnen bei der Nutzung des von ihnen bereitgestellten Telekommunikationsdienstes erzeugt oder verarbeitet werden. Diese – „vor die Klammer gezogene“ – Maßgabe stellt klar, dass die Diensteanbieter nicht verpflichtet sind, Daten zu speichern, die von ihnen weder erzeugt noch verarbeitet werden und die daher in ihren Systemen nicht verfügbar sind. Diese Bestimmung begrenzt die einzelnen Speicherungspflichten der Absätze 2 bis 4 somit richtlinienkonform auf diejenigen Daten, die dem Verpflichteten im Zuge der Erbringung seines Telekommunikationsdienstes vorliegen. Dadurch und durch die Fokussierung der Speicherungspflicht auf die Erbringer von Telekommunikationsdiensten für Endnutzer i. S. v. § 3 Nr. 8 TKG soll eine Mehrfachspeicherung

gleichartiger Daten weitgehend vermieden und der den Verpflichteten treffende Aufwand so gering wie möglich gehalten werden. Der Begriff des „Verarbeitens“ ist allerdings in einem weiten Sinne zu verstehen und erfasst etwa auch die Fallgestaltung, dass ein Mobilfunknetzbetreiber die von einem Teilnehmer eines anderen Netzbetreibers initiierte Verbindung „übernimmt“ und die Verbindung zu seinem eigenen Endnutzer herstellt; auch dies stellt ein („Weiter“-)Verarbeiten der vom anderen Netzbetreiber übermittelten Verkehrsdaten im Sinne dieser Vorschrift dar. Andererseits steht nach Satz 1 fest, dass etwa diejenigen Netzbetreiber, die keine eigenen Telekommunikationsdienste anbieten, sondern lediglich die hierfür erforderlichen Übertragungswege bereitstellen, vorbehaltlich der Regelung in Absatz 6 nicht zur Speicherung der von anderen Diensteanbietern über die bereitgestellten Übertragungswege übermittelten Daten verpflichtet sind.

Satz 1 legt auch die Speicherungsdauer fest. Die in § 113a TKG-E im Einzelnen beschriebenen Daten sind danach für die Dauer von sechs Monaten zu speichern. Dies entspricht der nach Artikel 6 der Richtlinie 2006/24/EG vorgesehene Mindestspeicherungsdauer und der Forderung des Deutschen Bundestages in seinem Beschluss vom 16. Februar 2006 (BT-Drs. 16/545, S. 4). Die Beschränkung der Speicherungsdauer auf das nach der Richtlinie vorgegebene Mindestmaß ist angemessen. Fachlich erscheint diese Speicherungsdauer ausreichend, um in der weitaus überwiegenden Anzahl von Auskunftsersuchen eine Verfügbarkeit der maßgeblichen Daten sicherzustellen (vgl. BKA, Rechtliche, rechtspolitische und polizeipraktische Bewältigung der defizitären Rechtslage im Zusammenhang mit Mindestspeicherungsfristen für Telekommunikationsverbindungsdaten, 2005, S. 21 f.; Büllingen u. a., Stand und Perspektiven der Vorratsdatenspeicherung im internationalen Vergleich, 2004, S. 8). Zudem entspricht diese Beschränkung auf die von der Richtlinie vorgegebene Mindestspeicherungsdauer dem Gebot einer möglichst grundrechtsschonenden Umsetzung der Richtlinie.

Um sicherzustellen, dass die Daten entsprechend der Vorgabe aus Artikel 8 der Richtlinie 2006/24/EG den berechtigten Stellen unverzüglich zur Verfügung gestellt werden können, bestimmt Satz 1 zudem, dass die Speicherung der Daten im Inland oder in einem anderen Mitgliedstaat der Europäischen Union zu erfolgen hat.

Der Zweck der Speicherung, nämlich die Sicherstellung der Verfügbarkeit der in § 113a TKG-E genannten Daten insbesondere für die Zwecke der Strafverfolgung, aber auch der Gefahrenabwehr und der Aufgabenerfüllung der Nachrichtendienste ergibt sich aus der Verwendungsregelung in § 113b Satz 1 Halbsatz 1 TKG-E. Dies lässt eine ausdrückliche Regelung des Speicherungszwecks in § 113a TKG-E entbehrlich erscheinen.

Zu Absatz 2

Absatz 2 Satz 1 regelt die einzelnen Speicherungspflichten für Anbieter öffentlich zugänglicher Telefondienste, wobei die technische Realisierung derartiger Dienste unerheblich ist und daher auch Ausprägungen wie Festnetz-, Mobilfunk- und Internettelefonie umfasst. Die Kenntnis der in Absatz 2 genannten Daten ist für Strafverfolgungsbehörden unverzichtbar, um zurückliegende Telekommunikationsvorgänge zuverlässig nachvollziehen zu können. Satz 2 stellt klar, dass diese Speicherungspflichten bei der Übermittlung von Kurznachrichten (SMS), Multimedianachrichten (MMS) und vergleichbaren Nachrichten (z. B. EMS) entsprechend gelten, wobei sich die zu speichernden Zeitangaben mangels bestehender Verbindung auf die Versendung und den Empfang der Nachricht beziehen. Hinzuweisen ist auf Folgendes:

Nummer 1 setzt Vorgaben aus Artikel 5 Abs. 1 Buchstabe a Nr. 1 und 2, Buchstabe b Nr. 1 und 2 sowie Buchstabe e Nr. 1, 2 und 3 der Richtlinie 2006/24/EG um und stellt sicher, dass – auch im Falle von Um- oder Weiterschaltungen eines Anrufs – die im Bereich der Telefonie zur Identifizierung der Kommunikationsteilnehmer erforderlichen Rufnummern oder anderen Anschlusskennungen (etwa auch Kennungen von Anschlüssen aus dem Bereich der Internet-Telefonie, die nach einem anderen als dem herkömmlichen E-164-Nummerierungsplan bezeichnet sein können) verfügbar sind.

Nummer 2 setzt Vorgaben aus Artikel 5 Abs. 1 Buchstabe c Nr. 1 und 2 der Richtlinie 2006/24/EG um und stellt die genaue zeitliche Bestimmbarkeit einer erfolgten Telekommunikation sicher.

Nummer 3 setzt Vorgaben aus Artikel 5 Abs. 1 Buchstabe d Nr. 1 und 2 der Richtlinie 2006/24/EG um und betrifft die Fallgestaltung, dass im Rahmen des Telefondienstes weitere Dienste in Anspruch genommen werden können. In diesem Fall ist auch die Angabe zu speichern, welcher Dienst bei dem jeweiligen Telekommunikationsvorgang genutzt wurde (im ISDN etwa Sprach-, Telefax- oder Datenübertragung; im Mobiltelefondienst etwa die Versendung von Kurzmitteilungen [SMS] oder von Multimediadaten [MMS]).

Nummer 4 beschreibt besondere Speicherungsvorgaben für den Bereich der Mobilfunktelefonie und setzt Vorgaben aus Artikel 5 Abs. 1 Buchstabe e Nr. 2 und Buchstabe f Nr. 1 der Richtlinie 2006/24/EG um.

- Nach Buchstabe a sind die internationalen Kennungen für mobile Teilnehmer für den anrufenden und den angerufenen Anschluss zu speichern (so genannte IMSI).

- Nach Buchstabe b sind die internationalen Kennungen der anrufenden und der angerufenen Endgeräte zu speichern (so genannte IMEI).

- Nach Buchstabe c sind die Standortdaten des anrufenden und des angerufenen Anschlusses bei Beginn der Verbindung, also die konkreten Bezeichnungen der Funkzellen zu speichern, über die die Telekommunikationsteilnehmer beim Verbindungsaufbau versorgt werden. In den meisten Fällen können daraus zutreffende Rückschlüsse auf den Bereich gezogen werden, in dem sich die Telekommunikationsteilnehmer zum Zeitpunkt des Verbindungsaufbaus aufgehalten haben; indes können solche Rückschlüsse zu dem vermutlichen Aufenthaltsort der Telekommunikationsteilnehmer in Folge nicht kalkulierbarer Unwägbarkeiten auch mit Unsicherheiten behaftet sein.

- Nach Buchstabe d sind bei der Inanspruchnahme im Voraus bezahlter anonymer Telefondienste der Zeitpunkt der ersten Aktivierung des Dienstes sowie die Angabe der Funkzelle zu speichern, in der sich das Mobiltelefon bei Aktivierung des Dienstes befindet. Sofern die Aktivierung einer solchen so genannten Prepaidkarte mittels Anrufs beim Telekommunikationsdiensteanbieter erfolgt, werden diese Daten bereits durch die Nummern 1, 2 und 4 Buchstabe a bis c erfasst, so dass auf der Grundlage dieses Aktivierungsverfahrens Buchstabe d zu keiner zusätzlichen Datenspeicherung führt. Die Aufnahme von Buchstabe d ist gleichwohl geboten, um bei etwaigen Änderungen dieses Aktivierungsverfahrens weiterhin den Vorgaben der Richtlinie zu entsprechen. Soweit die Aktivierung des Dienstes auf eine Weise erfolgt, bei der Verkehrsdaten weder erzeugt noch verarbeitet werden, wie dies etwa der Fall sein kann, wenn die Freischaltung durch eine sofortige Onlineanmeldung bei Vertragschluss von einem Mitarbeiter des Diensteanbieters erfolgt, begründet dies nach Maßgabe von Absatz 1 Satz 1 keine Speicherungspflicht. Die Regelung des Buchstaben d kann derzeit in Deutschland auch deshalb weitgehend leerlaufen, weil anonyme Telefondienste aufgrund der bereits bestehenden Pflicht zur Bestandsdatenerhebung nach § 111 TKG kaum vorkommen dürften.

Nummer 5 setzt Vorgaben aus Artikel 5 Abs. 1 Buchstabe a Nr. 2 und Buchstabe b Nr. 2 der Richtlinie 2006/24/EG um und regelt für den Bereich der Internettelefonie die Pflicht zur Speicherung der Internetprotokoll-Adressen des anrufenden und des angerufenen Anschlusses, um eine Bestimmung des Anschlusses zu ermöglichen, der Ziel oder Ursprung eines Internettelefonats war.

Zu Absatz 3

Absatz 3 setzt Vorgaben aus Artikel 5 Abs. 1 Buchstabe a Nr. 2, Buchstabe b Nr. 2 sowie - zur zeitlichen Bestimmbarkeit einer Nachrichtenübermittlung – aus Buchstabe c Nr. 2 der Richtlinie 2006/24/EG um und regelt die einzelnen Speicherungspflichten für Anbieter öffentlich zugänglicher E-Mail-Dienste. Diese Daten sind für eine Rückverfolgbarkeit einer erfolgten Telekommunikation mittels E-Mail unverzichtbar. Die differenzierte Ausgestaltung der einzelnen Speicherungspflichten in den Nummern 1 bis 3 trägt den besonderen technischen Gegebenheiten der E-Mail-Kommunikation Rechnung, nach denen die Übermittlung von E-Mails in verschiedenen Phasen verläuft. Hierbei ist unter dem Zugriff auf das elektronische Postfach nach Nummer 3 der Telekommunikationsvorgang zu verstehen, bei dem der E-Mail-Kunde die ihm vom E-Mail-Anbieter bereitgestellte persönliche Posteingangseite öffnet, auf der die Kopfzeilen (header) der eingegangenen E-Mails, nicht aber zwingend auch der Inhalt (body) der auf dem Server des Anbieters gespeicherten E-Mails aufgelistet sind. Entsprechendes gilt, wenn der Nutzer die E-Mail von einem E-Mail-Programm auf sein Endgerät herunterladen lässt, da auch in diesem Falle auf das elektronische Postfach zugegriffen wird. Die Speicherung auch der Internetprotokoll-Adressen ist erforderlich, weil die jeweils übermittelte E-Mail-Adresse ohne größeren Aufwand oder besondere technische Kenntnisse verändert werden kann und manche Betreiber Server einsetzen, die die Richtigkeit dieser Angaben nicht überprüfen, wodurch die Rückverfolgbarkeit von E-Mails unmöglich oder zumindest aber erheblich erschwert wird.

Zu Absatz 4

Absatz 4 setzt Vorgaben aus Artikel 5 Abs. 1 Buchstabe a Nr. 2, Buchstabe c Nr. 2 und Buchstabe e Nr. 3 der Richtlinie 2006/24/EG um und regelt die einzelnen Speicherungspflichten für Anbieter von Internetzugängen. Die Verfügbarkeit der zu speichernden Daten – Internetprotokoll-Adressen nach Nummer 1, Anschlusskennungen (etwa auch von DSL-Anschlüssen) nach Nummer 2 und Zeitangaben nach Nummer 3 – ist für Ermittlungszwecke unverzichtbar, um nachvollziehen zu können, welchem Anschluss zu einem bestimmten Zeitpunkt eine bestimmte Internetprotokoll-Adresse zugewiesen war, die für einen bestimmten Kommunikationsvorgang im Internet genutzt wurde. Hierbei ist von Bedeutung, dass die Richtlinie keine Speicherung der im Internet aufgerufenen Adressen (so genannte URL [Uniform Resource Locator]) fordert. Diese Angabe ist somit nicht Gegenstand der Speicherungspflicht nach § 113a Abs. 4 TKG-E, wie auch Absatz 8 nochmals ausdrücklich klarstellt. Es wird somit auch auf Grundlage der zu speichernden Internetdaten nicht das gesamte „Surfverhalten“ von Internetnutzern nachvollziehbar werden.

Zu Absatz 5

Absatz 5 bestimmt, dass Verkehrsdaten über so genannte „erfolglose Anrufversuche“ der Speicherungspflicht nur unterfallen, soweit der Verpflichtete Daten hierüber ohnehin zu eigenen Zwecken speichert oder protokolliert. Hiervon ist etwa auszugehen, wenn ein Teilnehmer von seinem Diensteanbieter per SMS darüber informiert wird, dass ein für seinen Anschluss bestimmter Anruf nicht entgegengenommen wurde, weil etwa der Anschluss belegt war oder sich das Mobiltelefon zur Zeit des Anrufversuchs außerhalb des Versorgungsbereichs einer Funkzelle (in einem „Funkloch“) befand. Diensteanbieter, die solche Anrufversuche nicht speichern, werden dazu auch durch § 113a TKG-E nicht verpflichtet. Keinesfalls besteht eine Speicherungspflicht in den Fällen, in denen schon der Verbindungsaufbau scheitert.

Zu Absatz 6

Absatz 6 bestimmt, dass diejenigen Diensteanbieter, die bei der Erbringung ihres Telekommunikationsdienstes solche Angaben verändern, die nach Maßgabe der Absätze 2 bis 4 zu speichern sind, sowohl die ursprüngliche Angabe als auch die neue Angabe und den Zeitpunkt der Umschreibung der Angaben zu speichern haben. Hierdurch wird etwa die Fallgestaltung erfasst, dass ein Diensteanbieter ohne eigene Endnutzerbeziehung lediglich die technische Einrichtung zur Weiterleitung für eine von anderen Diensteanbietern initiierte Telekommunikation zur Verfügung stellt und hierbei die von den anderen Diensteanbietern erzeugten oder verarbeiteten – und nach Maßgabe der Absätze 2 bis 4 zu speichernden – Verkehrsdaten verändert. Die Vorgabe des Absatzes 6 ist erforderlich, um einerseits die grundsätzliche Speicherungsverpflichtung nach Absatz 1 auf die Diensteanbieter mit Endnutzerbeziehung beschränken zu können und andererseits gleichwohl eine Rückverfolgbarkeit der Telekommunikation auch im Falle einer Änderung der relevanten Daten durch einen zwischengeschalteten Diensteanbieter ohne Endnutzerbeziehung sicherzustellen. In welcher Weise das ursprüngliche Datum verändert wird, ist hierbei gleichgültig. Regelmäßig wird das Verändern darin bestehen, dass das ursprüngliche Datum gelöscht und durch ein anderes ersetzt wird (vgl. Dammann, in: Simitis, Bundesdatenschutzgesetz, 6. Aufl., 2006, § 3, Rn. 141).

Hierbei kommt es auch nicht darauf an, ob die Zwischenschaltung des Diensteanbieters etwa aus technischen oder wirtschaftlichen Gründen durch die an der Erbringung der Telekommunikationsdienste beteiligten Diensteanbieter geschieht oder ob die Zwischenschaltung

auf Veranlassung des Endnutzers gezielt zur Veränderung der nach Maßgabe der Absätze 2 bis 4 zu speichernden Daten erfolgt, wie dies etwa bei der Nutzung von Anonymisierungsdiensten der Fall ist. In beiden Fällen besteht die Speicherungsverpflichtung nach Absatz 6, wenn die maßgeblichen Daten bei der Erbringung des Telekommunikationsdienstes verändert werden.

Soweit eine Speicherungsverpflichtung danach auch für die Anbieter von Anonymisierungsdiensten begründet wird, ist zu berücksichtigen, dass auch diese Anbieter öffentlich zugängliche Telekommunikationsdienste erbringen. Öffentlich zugängliche Telekommunikationsdienste sind alle Telekommunikationsdienste im Sinne von § 3 Nr. 24 TKG, die jedermann zugänglich sind. Nach § 3 Nr. 24 TKG fallen darunter die „reinen“ Telekommunikationsdienste (also Dienste, die ausschließlich in der Übertragung von Signalen über Telekommunikationsnetze bestehen) sowie Dienste mit Doppelnatur, die zwar auch unter den Rechtsrahmen für Telemedien fallen, aber zugleich Telekommunikationsdienste nach § 3 Nr. 24 TKG sind, weil sie überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen. Dies sind in erster Linie diejenigen Dienste, die sowohl der Bereitstellung eines Internetzugangs als auch der Übertragung elektronischer Post dienen. Auch Anonymisierungsdienste weisen allerdings eine solche Doppelnatur auf, da ihre Tätigkeit sowohl in der Durchleitung der Nachricht als auch in der Ersetzung der Ausgangskennung des Telekommunikationsnutzers besteht. Diese Dienste sind daher sowohl Telemedien als auch – im Hinblick auf ihre Transportfunktion – Telekommunikationsdienste für die Öffentlichkeit (vgl. hierzu jetzt auch § 11 Abs. 3 Telemediengesetz [TMG], ferner Schmitz, in: Spindler/Schmitz/Geis, TDG-Kommentar, 2004, § 1 TDDSG, Rn. 16).

Zu Absatz 7

Absatz 7 setzt Vorgaben aus Artikel 5 Abs. 1 Buchstabe f Nr. 2 der Richtlinie 2006/24/EG um und betrifft Angaben zur Netzplanung der Mobilfunknetzbetreiber, regelt also nicht die Speicherung von Verkehrsdaten. Diese Angaben sind erforderlich, um die nach Absatz 1 Nr. 4 Buchstabe c zu speichernden Funkzellenbezeichnungen, die regelmäßig nur in alphanumerischer Form dargestellt werden und damit als solche für Ermittlungszwecke weithin unbrauchbar sind, bestimmten geografischen Bereichen zuordnen zu können. Da diese Funkzellenbezeichnungen aus Gründen sich fortentwickelnder Netzstrukturen von den Diensteanbietern nicht dauerhaft zugewiesen und etwa bei Großereignissen oftmals weitere Funkzellen nur kurzfristig eingerichtet werden, ist es erforderlich sicherzustellen, dass die geografische Zuordnung für die Dauer der Speicherungspflicht nach Maßgabe dieser Vorschrift beauskunftet werden kann. Die Angabe der Hauptstrahlrichtungen der einzelnen

Funkantennen konkretisiert die Richtlinienvorgabe und dient der Ermöglichung einer genaueren Ermittlung des Standorts, von dem aus oder zu dem eine Telekommunikationsverbindung aufgebaut wurde.

Zu Absatz 8

Absatz 8 setzt die Vorgabe des Artikels 5 Abs. 2 der Richtlinie 2006/24/EG um und stellt klar, dass weder der Kommunikationsinhalt noch Daten über aufgerufene Internetseiten nach dieser Vorschrift nicht gespeichert werden dürfen. Dies erlangt etwa auch Bedeutung für solche Dienste, bei denen Inhalte im so genannten Zeichenkanal übermittelt werden (z. B. bei der Übermittlung von (SMS-)Kurzmitteilungen im Mobiltelefondienst). Hier muss der Verpflichtete dafür Sorge tragen, dass inhaltsbezogene Anteile der Kommunikation aufgrund der Vorschrift des § 113a TKG-E nicht gespeichert werden.

Zu Absatz 9

Mit der Regelung in Absatz 9 wird eine Vorgabe aus Artikel 8 der Richtlinie 2006/24/EG umgesetzt und sichergestellt, dass die Daten von dem Verpflichteten in einer Weise gespeichert werden, die eine effektive und schnelle Recherche zulässt, so dass erforderliche Auskünfte unverzüglich erteilt werden können.

Zu Absatz 10

Absatz 10 stellt klar, dass der Verpflichtete die zu speichernden Verkehrsdaten mit der Sorgfalt zu behandeln hat, die beim Umgang mit vom Fernmeldegeheimnis geschützten Daten erforderlich ist; dies gilt sowohl im Hinblick auf die Zuverlässigkeit, dass die Daten korrekt und unverändert gespeichert werden, als auch für den Schutz der Daten vor unberechtigten Zugriffen. Zur Erhöhung des Schutzniveaus legt Satz 2 fest, dass der Verpflichtete durch technische und organisatorische Maßnahmen dafür Sorge zu tragen hat, dass auf die gespeicherten Verkehrsdaten ausschließlich Personal zugreifen kann, das hierzu besonders ermächtigt ist.

Zu Absatz 11

Absatz 11 bestimmt, dass die nach § 113a TKG-E gespeicherten Verkehrsdaten innerhalb eines Monats nach Ablauf der Speicherungsfrist zu löschen sind. Dies begrenzt den bei den

Diensteanbietern erforderlichen Aufwand für die Löschung gegenüber einer tagesgenauen Vorgabe, ohne die Speicherungsdauer der Daten übermäßig zu verlängern.

Zu § 113b TKG-E

Die Vorschrift regelt die Verwendung der nach Maßgabe von § 113a TKG-E gespeicherten Verkehrsdaten. Im Einzelnen:

Satz 1 Halbsatz 1 bestimmt, dass der nach Maßgabe von § 113a TKG-E zur Speicherung verpflichtete Diensteanbieter die nach § 113a TKG-E gespeicherten Daten für die in den Nummern 1 bis 3 genannten Zwecke an die hierfür jeweils zuständigen Stellen übermitteln darf, wenn dies erstens im jeweils einschlägigen Fachgesetz (z. B. § 100g StPO) unter Bezugnahme auf § 113a TKG(-E) vorgesehen und zweitens die Übermittlung im Einzelfall angeordnet ist. Ob die zuständigen Stellen berechtigt sind, ein solches Verlangen an den Diensteanbieter zu richten, ist mithin nicht Regelungsgegenstand von § 113b TKG-E, sondern bestimmt sich nach den für die zuständigen Stellen jeweils maßgeblichen fachgesetzlichen Vorschriften. Ob die Voraussetzungen für ein Übermittlungsverlangen vorliegen, haben die zuständigen Stellen in eigener Verantwortung zu prüfen. Dem Diensteanbieter kommt insoweit weder eine inhaltliche Prüfungspflicht noch -befugnis zu. Der Diensteanbieter hat sich allerdings zu vergewissern, ob es sich bei dem die Übermittlung Verlangenden um eine für die in § 113b TKG-E genannten Aufgaben zuständige Stelle handelt, die zur Ausübung des Übermittlungsverlangens legitimiert ist. Soweit das Verlangen auf die Übermittlung von Verkehrsdaten gerichtet ist, die allein nach Maßgabe von § 113a TKG-E gespeichert worden sind, muss die zuständige Stelle sich durch eine im jeweiligen Fachgesetz näher bestimmte Einzelfallanordnung (etwa einen Beschluss eines Ermittlungsgerichts nach § 100g i. V. m. § 100b StPO) legitimeren können.

Eine Verwendung der allein nach Maßgabe von § 113a TKG-E gespeicherten Daten für andere als in § 113b Satz 1 Halbsatz 1 TKG-E genannte Zwecke ist dem Diensteanbieter gemäß § 113b Satz 1 Halbsatz 2 TKG-E nicht gestattet.

Die Verwendung der nach Maßgabe von § 113a TKG-E gespeicherten Daten für die Zwecke sowohl der Strafverfolgung als auch der Gefahrenabwehr und der Aufgabenerfüllung der Nachrichtendienste steht in Einklang mit der Richtlinie 2006/24/EG. Zwar macht die Richtlinie lediglich Vorgaben zur Speicherung von Daten für die Zwecke der Strafverfolgung; dies steht jedoch einer Verwendung der gespeicherten Daten für andere Zwecke nicht entgegen. Den

Mitgliedstaaten steht es vielmehr – in den Grenzen von Artikel 15 Abs. 1 der Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG) – frei, in ihrem nationalen Recht Regelungen zu treffen über die Verwendung der gespeicherten Verkehrsdaten für andere als Strafverfolgungszwecke.

Die Beschreibung des Anwendungsbereichs der Richtlinie in Artikel 1 Abs. 1 hindert eine weiter gehende Verwendung der gespeicherten Verkehrsdaten nicht. Aus dieser Vorschrift lässt sich nicht ableiten, dass eine Verwendung der gespeicherten Verkehrsdaten für andere als Strafverfolgungszwecke ausgeschlossen sein soll. Zunächst findet die Annahme einer solchen strikten Zweckbindung im Wortlaut der Richtlinie keine Stütze. Die Richtlinie enthält gerade keine Regelung, wonach die gemäß ihren Vorgaben gespeicherten Verkehrsdaten nicht auch zu anderen als Strafverfolgungszwecken sollen Verwendung finden dürfen. Eine solche Regelung wäre jedoch zu erwarten, wenn die Richtlinie dies hätte sicherstellen wollen. Auch den Erwägungsgründen lässt sich eine solche Intention nicht entnehmen.

Zudem stellt Artikel 11 der Richtlinie 2006/24/EG in Verbindung mit Artikel 15 Abs. 1 der Richtlinie 2002/58/EG klar, dass die Richtlinie 2006/24/EG lediglich Mindestvorgaben für die Verwendung der „auf Vorrat“ gespeicherten Verkehrsdaten trifft. Aus dem neu eingefügten Artikel 15 Abs. 1a der Richtlinie 2002/58/EG folgt, dass Artikel 15 Abs. 1 dieser Richtlinie nicht anwendbar ist auf solche Verkehrsdaten, die nach Maßgabe der Richtlinie 2006/24/EG gespeichert werden; zugleich ergibt sich hieraus, dass Artikel 15 Abs. 1 der Richtlinie 2002/58/EG weiterhin Geltung beansprucht für solche Verwendungszwecke, die nicht von der Richtlinie 2006/24/EG erfasst sind. Dies bestätigt Erwägungsgrund 12 der Richtlinie 2006/24/EG ausdrücklich.

Auch die Entstehung der Richtlinie 2006/24/EG bestätigt dieses Verständnis. In den Verhandlungen auf europäischer Ebene bestand Einvernehmen, dass die Richtlinie (wie auch der zunächst verhandelte Rahmenbeschluss) als Mindestvorgabe nur die Speicherung von Verkehrsdaten für Strafverfolgungszwecke regeln sollte, ohne weiter gehende nationale Regelungen über die Verwendung der gespeicherten Verkehrsdaten für andere Zwecke auszuschließen. Noch im letzten Dokument zur Beratung des Rahmenbeschlussentwurfs war eine ausdrückliche Regelung vorgesehen, nach der bestimmte im Einzelnen aufgeführte nationale Rechtsbereiche und Maßnahmen von dem Rahmenbeschluss unberührt bleiben sollten. Hierzu zählten etwa nationale Rechtsvorschriften über die „Vorratsspeicherung“ von Kommunikationsdaten für die Zwecke der Gefahrenabwehr und der nationalen Sicherheit. Zwar wurde eine solche ausdrückliche enumerative Klarstellung in dem von der Kommission am 21. September 2005 vorgelegten Richtlinienvorschlag zugunsten des oben dargestellten Ar-

tikels 11 der Richtlinie 2006/24/EG aufgegeben. Eine sachliche Änderung im Sinne einer strikten Zweckbindung der gespeicherten Verkehrsdaten war damit jedoch nicht beabsichtigt. Es war vielmehr während der gesamten Verhandlungen ein wesentliches Anliegen nahezu sämtlicher Mitgliedstaaten, keine abschließende Regelung zu schaffen, sondern klarzustellen, dass weiter gehende nationale Verwendungsregelungen zulässig bleiben sollten.

Die in § 113b Satz 1 Halbsatz 1 Nr. 2 und 3 TKG-E zugelassene Verwendung der nach Maßgabe von § 113a TKG-E gespeicherten Daten für die Zwecke der Gefahrenabwehr und der Aufgabenerfüllung der Nachrichtendienste ist von Artikel 15 Abs. 1 der Richtlinie 2002/58/EG in Verbindung mit der dort in Bezug genommenen Vorschrift des Artikels 13 Abs. 1 Buchstabe a bis d der Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (95/46/EG) gedeckt, da die Verwendung der Daten auch für diese Zwecke erforderlich und angemessen ist. Auch zur Abwehr von erheblichen Gefahren für die öffentliche Sicherheit und zur Erfüllung der gesetzlichen Aufgaben der Nachrichtendienste – zumal im Bereich der Bekämpfung des internationalen Terrorismus – ist die Kenntnis des Kommunikationsverhaltens der Zielpersonen von unverzichtbarem ermittlungstaktischem Nutzen für die Aufklärung komplexer Organisationsstrukturen etwa von kriminellen oder terroristischen Vereinigungen. Dieselben Gründe, die die Einführung von Speicherungspflichten für Zwecke der Strafverfolgung rechtfertigen (vgl. dazu oben A. VI. 5.), sind geeignet eine Verwendung der gespeicherten Daten für die Zwecke der Gefahrenabwehr und der Nachrichtendienste zu rechtfertigen, zumal Anlass für die Verabschiedung der Richtlinie – neben dem Gesichtspunkt der EU-weiten Harmonisierung der Speicherungspflichten – gerade auch die Terroranschläge in Madrid im Jahr 2004 und in London im Jahr 2005 waren. Ohne eine Kenntnis der Verkehrsdaten wäre es den Gefahrenabwehrbehörden und den Nachrichtendiensten vielfach nicht möglich, Verflechtungen und Zusammenhänge im Bereich des internationalen Terrorismus zu erkennen und die hiervon ausgehenden Gefahren wirksam abzuwehren. Gerade im Hinblick auf die im Bereich des internationalen Terrorismus anzutreffenden stark nach außen abgeschottet und konspirativ handelnden Gruppierungen ist eine Kenntnis von Telekommunikationsverkehrsdaten unabdingbar.

Die Verwendung der nach Maßgabe von § 113a TKG-E gespeicherten Daten für die Zwecke der Gefahrenabwehr und der Aufgabenerfüllung der Nachrichtendienste steht überdies in Einklang mit dem Beschluss des Deutschen Bundestages vom 16. Februar 2006 (BT-Drs. 16/545, S. 4). Dieser enthält eine Forderung hinsichtlich der Verwendung der gespeicherten Daten nur insoweit, als ein Zugriff auf diese Daten „zu Zwecken der Strafverfolgung“ auf die

Verfolgung erheblicher oder mittels Telekommunikation begangener Straftaten beschränkt sein soll. Zur Verwendung der Daten im Übrigen verhält sich der Beschluss dagegen nicht.

Aus Verhältnismäßigkeitserwägungen erscheint es gleichwohl geboten, eine Verwendung der allein nach Maßgabe von § 113a TKG-E gespeicherten Daten für Gefahrenabwehrzwecke auf die Abwehr erheblicher Gefahren für die öffentliche Sicherheit zu beschränken und daher bereits im Telekommunikationsgesetz festzulegen, dass der jeweilige Fachgesetzgeber eine Befugnis zum Zugriff auf diese Daten nicht zur Abwehr jeglicher Gefahren für die öffentliche Sicherheit begründen kann. Diese Beschränkung trägt – im Hinblick auf die Rechtsprechung des Bundesverfassungsgerichts (vgl. BVerfGE 65, 1, 46; 100, 313, 360) – zugleich dem Erfordernis einer hinreichend konkreten Verwendungsbestimmung hinsichtlich der „auf Vorrat“ gespeicherten Daten Rechnung. Eine entsprechende Beschränkung findet sich in der Regelung zur zweckumwandelnden Verwendung von in bestimmter Weise erhobenen personenbezogener Daten in § 477 Abs. 2 Satz 3 StPO-E; zum Begriff der erheblichen Gefahr vgl. im Einzelnen Schmidtbauer in: Schmidtbauer/Steiner, Bayerisches Polizeiaufgabengesetz und Bayerisches Polizeiorganisationsgesetz, 2. Aufl. (2006), Art. 11 PAG Rn. 48.

Nach Satz 2 ist die Regelung des § 113 Abs. 1 Satz 4 TKG entsprechend anzuwenden. Dies bedeutet, dass der Diensteanbieter gegenüber seinen Kundinnen und Kunden sowie gegenüber Dritten Stillschweigen über eine Auskunftserteilung zu wahren hat, und dient mithin dazu, dass verdeckt geführte Ermittlungen nicht vorzeitig bekannt werden.

Zu Nummer 7 (§ 115 Abs. 2 TKG-E)

Die Einfügung des Verweises auf § 113a TKG-E in Absatz 2 Satz 1 Nr. 1 dient der Sicherstellung der Erfüllung der Speicherungspflichten nach § 113a TKG-E. Die weiteren Änderungen stellen redaktionelle Folgeanpassungen an die Änderungen in § 111 TKG-E dar.

Zu Nummer 8 (§ 149 TKG-E)

Zu Buchstabe a (Absatz 1)

Die Ergänzung der Ordnungswidrigkeitentatbestände in Absatz 1 um die Nummern 30a und 36 bis 39 sowie die Änderung der Nummern 29 und 30 dienen zum einen der Umsetzung

von Artikel 5 und 13 der Richtlinie 2006/24/EG, wonach sowohl die ordnungsgemäße Erfüllung der Speicherungs- und Löschungspflichten sicherzustellen ist als auch abschreckende Sanktionen vorzusehen sind, um einen unzulässige Zugang zu und Umgang mit den nach Maßgabe der Richtlinie gespeicherten Daten zu verhindern; zum anderen handelt es sich um Folgeanpassungen an die Änderungen in § 111 TKG-E. Die Änderung der Nummer 35 erstreckt den bestehenden Ordnungswidrigkeitentatbestand auf Fälle, in denen der Diensteanbieter nicht Stillschweigen über die Auskunftserteilung über nach § 113a TKG-E gespeicherte Daten wahrt.

Zu Buchstabe b (Absatz 2)

Durch die Ergänzung in Absatz 2 wird eine angemessene Bußgeldhöhe für die einzelnen Ordnungswidrigkeitentatbestände nach Absatz 1 festgelegt.

Zu Nummer 9 (§ 150 Abs. 12b TKG-E)

Absatz 12b Satz 1 schiebt die Anwendung der Ordnungswidrigkeitentatbestände nach § 149 Abs. 1 Nr. 36 und 37 TKG-E bis zum 1. Januar 2009 auf. Damit wird dem Umstand Rechnung getragen, dass die Vorgaben aus § 113a TKG-E für die verpflichteten Unternehmen nicht ohne weiteres kurzfristig umzusetzen sind, sondern es hierzu bestimmter technischer, organisatorischer und sonstiger betriebsinterner Maßnahmen bedarf, deren konkrete Ausgestaltung sich vor Abschluss des Gesetzgebungsverfahrens – aus Sicht der verpflichteten Unternehmen – oftmals nicht mit der gebotenen Gewissheit einschätzen lassen dürfte. Aus diesem Grunde erscheint es angemessen, zwar einerseits die Speicherungspflichten für die Diensteanbieter im Bereich der Festnetz- und der Mobilfunktelefonie unmittelbar in Kraft treten zu lassen, aber die Sanktionsbewehrung dieser Verpflichtungen für einen Zeitraum von einem Jahr aufzuschieben. Dies ist auch im Hinblick auf die Pflicht zur richtlinienkonformen innerstaatlichen Umsetzung der Speicherungsvorgaben vertretbar, da die Richtlinie 2006/24/EG eine Sanktionsbewehrung zur Sicherstellung der Speicherungspflichten nicht vorgibt.

Einer entsprechenden Übergangsregelung bedarf es bei der in § 111 TKG-E vorgesehenen Speicherungsverpflichtung von Bestandsdaten bei E-Mail-Adressen nicht. Denn diese Verpflichtung setzt voraus, dass der Diensteanbieter die Bestandsdaten bereits zu eigenen Zwecken erhebt und damit bereits heute regelmäßig auf Dauer speichern wird.

Zu Artikel 3 (Änderung der Abgabenordnung)

Die mit dem Steuerverkürzungsbekämpfungsgesetz vom 19. Dezember 2001 (BGBl. I S. 3922) eingeführte und durch das Fünfte Gesetz zur Änderung des Steuerbeamten-Ausbildungsgesetzes und zur Änderung von Steuergesetzen vom 23. Juli 2002 (BGBl. I S. 2715) geänderte Regelung des § 370a AO sollte die Strafbarkeit der Steuerhinterziehung bei gewerbsmäßiger oder bandenmäßiger Begehung und besonders großem Taterfolg verschärfen. Der 5. Strafsenat des Bundesgerichtshofs hat allerdings in seinem Beschluss vom 22. Juli 2004 (5 StR 85/04, NJW 2004, 2990) erhebliche Bedenken an der Verfassungsmäßigkeit der Vorschrift geäußert. Da das Steuerstrafrecht im Rahmen der Blankettnorm des § 370 AO durch eine serielle Begehungsweise geprägt ist, sei die in § 370a AO enthaltene Voraussetzung einer „gewerbsmäßigen Begehung“ nicht geeignet, den Tatbestand des § 370a AO hinreichend einzugrenzen. Auch das Tatbestandsmerkmal „in großem Ausmaß“ sei im Hinblick auf Artikel 103 Abs. 2 des Grundgesetzes als Tatbestandsmerkmal eines Verbrechenstatbestandes zu unbestimmt. Die Vorschrift des § 370a AO genüge danach nicht den Anforderungen des Bundesverfassungsgerichts, wonach eine Strafnorm umso präziser sein müsse, je schwerer die angedrohte Strafe ist.

Mit den vorgesehenen Änderungen der Abgabenordnung soll diesen Bedenken Rechnung getragen werden. Zugleich sollen die – ebenfalls vom Bundesgerichtshof beanstandeten – Wertungswidersprüche zu den Straftatbeständen der §§ 373, 374 AO beseitigt und der besonderen Schwere der dort genannten Delikte, insbesondere bei bandenmäßiger Tatbegehung, Rechnung getragen werden. Außerdem sollen Klarstellungen in den Straftatbeständen erfolgen.

Zu Nummer 1 (Inhaltsübersicht)

Es handelt sich um eine Folgeänderung zur Streichung des § 370a (vgl. Nummer 4).

Zu Nummer 2 (§ 370 AO-E)

Ein besonders schwerer Fall der Steuerhinterziehung nach § 370 Abs. 3 Nr. 1 AO-E soll künftig in der Regel bereits dann vorliegen, wenn in großem Ausmaß Steuern verkürzt oder

nicht gerechtfertigte Steuervorteile erlangt werden. Das bislang zusätzlich enthaltene, aber schwer bestimmbare Merkmal des „groben Eigennutzes“ wird gestrichen (vgl. zur schweren Bestimmbarkeit BGH vom 13. Juni 1985, NStZ 1985, 459).

Der neue § 370 Abs. 3 Satz 2 Nr. 5 AO-E bestimmt, dass ein besonders schwerer Fall der Steuerhinterziehung in der Regel auch dann vorliegt, wenn der Täter als Mitglied einer Bande, die sich zur fortgesetzten Begehung von Taten nach § 370 Abs. 1 AO verbunden hat, Umsatzsteuer oder Verbrauchsteuern verkürzt oder nicht gerechtfertigte Umsatz- oder Verbrauchsteuervorteile erlangt. Die Strafzumessungsregel ersetzt den bisherigen Qualifikationstatbestand in § 370a AO.

Nach der Entscheidung des Großen Senats des Bundesgerichtshofs vom 22. März 2001 (GSSt 1/00, BGHSt 46, 321) besteht eine Bande aus einem Zusammenschluss von mindestens drei Personen, die sich mit dem Willen verbunden haben, künftig für eine gewisse Dauer mehrere selbständige, im Einzelnen noch ungewisse Straftaten des im Gesetz genannten Deliktstyps (hier also Steuerhinterziehung) zu begehen. Ein „gefestigter Bandenwille“ oder ein Tätigwerden in einem „übergeordneten Bandeninteresse“ ist nicht erforderlich. Da der Tatbestand der Steuerhinterziehung nach § 370 AO nicht nur vom Steuerpflichtigen selbst begangen werden kann, sondern auch von anderen natürlichen Personen, die nicht zum eigenen Vorteil handeln müssen, sondern auch zum Vorteil Dritter handeln können, kommt als Mitglied einer solchen Bande auch jede andere mitwirkende Person in Betracht, selbst wenn sie nur in untergeordneter Tätigkeit als Gehilfe eingebunden ist. Nicht erforderlich ist es auch, dass es sich bei jedem Bandenmitglied um einen Steuerpflichtigen handelt. Ferner wird es für die bandenmäßige Begehung auch unerheblich sein, wenn z. B. nur ein Täter der Bande in Deutschland ansässig ist, da es sich nicht um einen im Inland bestehenden Zusammenschluss handeln muss. Es bleibt allerdings auch hier bei dem generellen Erfordernis, dass sich – soweit es sich nicht um Einfuhr- oder Ausfuhrabgaben handelt – die Tat auf das vom deutschen Fiskus verwaltete Steueraufkommen beziehen muss (vgl. § 370 Abs. 6 und 7 AO); da bei einer Steuerhinterziehung zu Lasten des deutschen Fiskus der Erfolg (Verkürzung des deutschen Steueranspruchs) immer im Inland eintritt, ist es unerheblich, ob die Tathandlung selbst im Ausland begangen wurde.

Nach § 370 Abs. 3 AO ist die Strafe in besonders schweren Fällen der Steuerhinterziehung Freiheitsstrafe von sechs Monaten bis zu zehn Jahren. Eine strafbefreiende Selbstanzeige nach § 371 AO ist wie bisher möglich.

Zu Nummer 3 (§ 370a AO-E)

Die Vorschrift wird aufgehoben. Die bandenmäßige Hinterziehung von Umsatz- und Verbrauchsteuern stellt nach dem neuen § 370 Abs. 3 Satz 2 Nr. 5 AO nunmehr ein Regelbeispiel für einen besonders schweren Fall der Steuerhinterziehung dar.

Zu Nummer 4 (§ 373 AO-E)

Durch die Änderung des § 373 AO (wie auch des § 374 AO) werden Wertungswidersprüche zwischen bandenmäßiger Umsatzsteuer- oder Verbrauchsteuerhinterziehung einerseits sowie bandenmäßigem Schmuggel und bandenmäßiger Steuerhehlerei andererseits beseitigt. Zugleich soll der besonderen Schwere dieser Delikte, gerade auch bei bandenmäßiger Tatbegehung, Rechnung getragen werden, indem der Strafrahmen für diese Delikte an die Strafrahmen des § 370 Abs. 3 AO angepasst wird.

Zu Buchstabe a (Absatz 1)

Mit der Änderung wird der Strafrahmen des gewerbsmäßigen, gewaltsamen oder bandenmäßigen Schmuggels (bislang: Freiheitsstrafe von drei Monate bis fünf Jahre) erhöht (künftig: Freiheitsstrafe von sechs Monate bis zehn Jahre) und damit an den Strafrahmen der Steuerhinterziehung im besonders schweren Fall nach § 370 Abs. 3 AO angepasst. Der neue Satz 2 regelt, dass für minderschwere Fälle ein reduzierter Strafrahmen (Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe) gilt. Dies ermöglicht eine angemessene Bestrafung des bandenmäßigen Schmuggels z. B. in Fällen, die nicht der typischen organisierten Kriminalität zuzurechnen sind.

Zu Buchstabe b (Absatz 2)

Um in allen Fällen des bandenmäßigen Schmuggels, auch soweit er außerhalb der Abgabenordnung geregelte Fälle des Bannbruchs betrifft, zu einem einheitlichen Bandenbegriff zu gelangen, und um auch innerhalb der Abgabenordnung (vgl. § 370 Abs. 3 Satz 2 Nr. 5 AO-E und § 374 AO-E) in der Sache nicht gebotene Differenzierungen zu vermeiden, wird in Absatz 2 Nr. 3 AO-E auf das bisherige Mitwirkungsmerkmal („unter Mitwirkung eines anderen Bandenmitglieds die Tat ausführt“) verzichtet. Es genügt künftig, dass der Täter als Mitglied einer Bande, die sich zur fortgesetzten Hinterziehung von Einfuhr- oder Ausfuhrabgaben oder des Bannbruchs verbunden hat, eine solche Tat begeht. Die Bandenverbindung kann

zudem künftig auch darauf gerichtet sein, fortgesetzt grenzüberschreitend Verbrauchssteuern zu hinterziehen.

Zu Buchstabe c (Absatz 3 und 4)

Durch die ausdrückliche Regelung der Versuchsstrafbarkeit in dem neuen Absatz 3 wird klargestellt, dass § 373 AO-E ein selbstständiger Qualifikationstatbestand zu § 370 Abs. 1 AO ist. Ein Rückgriff auf die Versuchsstrafbarkeit nach § 370 Abs. 2 AO ist künftig nicht mehr erforderlich. Eine Regelung für besonders schwere Fälle des § 373 AO oder eine Verweisung auf den Strafrahmen des § 370 Abs. 3 AO ist im Hinblick auf die Erhöhung des Strafrahmens in § 373 Abs. 1 AO nicht erforderlich. Damit entfällt auch die Notwendigkeit, für besonders schwere Fälle des § 373 AO den Strafrahmen der Strafzumessungsregel in § 370 Abs. 3 AO zu entnehmen (siehe hierzu: BGH vom 28. September 1983; 3 StR 280/83, BGHSt 32, 95).

Der neue Absatz 4 des § 373 AO erweitert den Anwendungsbereich des § 373 AO (entsprechend § 374 Abs. 4 AO-E) auf Einfuhr- oder Ausfuhrabgaben, die von einem anderen Mitgliedstaat der Europäischen Gemeinschaften verwaltet werden oder die einem Mitgliedstaat der Europäischen Freihandelsassoziation oder einem mit dieser assoziierten Staat zustehen.

Zu Nummer 5 (§ 374 AO-E)

Der Strafrahmen für Taten nach § 374 AO, welcher nach der bisherigen Regelung durch Verweisung auf § 370 Abs. 1 AO festgelegt wurde, soll zur Vereinfachung der Rechtsanwendung in § 374 Abs. 1 und 2 AO-E ausdrücklich geregelt werden. Gleiches gilt für die Regelung der Versuchsstrafbarkeit in Absatz 3. Auch hierfür soll die Verweisung auf § 370 Abs. 2 AO durch eine ausdrückliche Regelung ersetzt werden.

In Absatz 2 wird die bandenmäßige Steuerhehlerei zudem der gewerbsmäßigen Steuerhehlerei in ihrem Unrechtsgehalt gleichgestellt.

Die Neufassung des Absatzes 4 übernimmt die Neuregelung in § 373 Abs. 3 AO-E; auf die dortige Begründung wird Bezug genommen.

Zu Artikel 4 (Änderung des Strafgesetzbuchs)

Es handelt sich um Folgeänderungen zu der Änderung des § 374 AO und der Aufhebung des § 370a AO (vgl. Artikel 3).

1. Da die gewerbs- oder bandenmäßige Steuerhehlerei künftig in § 374 Abs. 2 AO gesondert geregelt werden soll, kann durch eine Aufnahme dieses Qualifikationstatbestandes in § 261 Abs. 1 Satz 2 Nr. 3 StGB auf die bisherige Einschränkung auf gewerbsmäßig begangene Taten verzichtet werden. Über das bisher geltende Recht hinaus soll zudem künftig auch die bandenmäßig begangene Steuerhehlerei zur tauglichen Vortat der Geldwäsche werden.

2. Bisher war die gewerbsmäßige oder bandenmäßige Steuerhinterziehung nach § 370a AO als Verbrechen nach § 261 Abs. 1 Satz 2 Nr. 1 StGB taugliche Vortat der Geldwäsche. Durch die vorgeschlagene Herabstufung solcher Taten zu einem Regelbeispiel für besonders schwere Fälle der Steuerhinterziehung nach § 370 Abs. 3 Nr. 5 AO in der Fassung des Entwurfs sollen die Taten nicht als Vortaten der Geldwäsche entfallen. Deshalb soll die Steuerhinterziehung nach § 370 AO in den Vortatenkatalog des § 261 Abs. 1 Satz 2 Nr. 4 StGB aufgenommen werden. Erfasst werden damit auch künftig im Wesentlichen die Taten, die bereits bisher taugliche Geldwäschevortaten waren, da § 261 Abs. 1 Satz 2 Nr. 4 voraussetzt, dass die Vortat gewerbsmäßig oder von dem Mitglied einer Bande, die sich zur fortgesetzten Begehung solcher Taten verbunden hat, begangen worden ist. Lediglich das bisher in § 370a AO enthaltene Merkmal der Steuerverkürzung im „großen Ausmaß“ wird künftig nicht mehr vorliegen müssen, um eine Steuerhinterziehung zur tauglichen Vortat der Geldwäsche zu qualifizieren.

Zu Artikel 5 (Änderung des Artikel 10-Gesetzes)

Da die Mitwirkungspflicht nach § 100b Abs. 3 Satz 1 StPO-E auch auf Personen und Stellen ausgedehnt wird, die Telekommunikationsdienste nicht geschäftsmäßig erbringen, muss, um den Erfolg der Überwachungsmaßnahme nicht zu gefährden, auch für diese Personen und Stellen die Verpflichtung gelten, Dritte über die Maßnahme nicht zu unterrichten. Deshalb wird in § 17 Abs. 1 G 10, der diese Verpflichtung enthält, das Wort „geschäftsmäßig“ gestrichen.

Zu Artikel 6 (Änderung des Vereinsgesetzes)

Der bisherige Verweis in § 10 Abs. 2 Satz 4 VereinsG u. a. auf die §§ 100 und 101 StPO wird aufgrund der Neuregelungen in diesen Vorschriften redaktionell angepasst:

Die bisherige Bezugnahme auf § 101 StPO wird entbehrlich hinsichtlich der dortigen Absätze 2 und 3, die nunmehr als Absätze 5 und 6 in den ohnehin in Bezug genommenen § 100 StPO-E eingestellt sind.

Die bisherige Bezugnahme auf § 101 Abs. 1 (Benachrichtigungspflicht) wird ersetzt durch die Bezugnahme auf die entsprechenden Regelungen in § 101 Abs. 4 bis 9 StPO-E. Damit werden die umfassenden Regelungen der Benachrichtigungspflicht, der Zurückstellung der Benachrichtigung nebst gerichtlicher Überprüfung sowie der nachträgliche Rechtsschutz auf die Postbeschlagnahme nach § 10 Vereinsgesetz ausgedehnt. Darüber hinaus wird durch die Bezugnahme auf § 101 Abs. 3 und 10 StPO-E auch die Kennzeichnungs- und Löschungspflicht eingeführt. Die Ausdehnung auf § 101 Abs. 3 bis 10 StPO-E erscheint sachgerecht, weil eine unterschiedliche Handhabung der Postbeschlagnahme nach § 99 StPO(-E) einerseits und § 10 Abs. 2 VereinsG i. V. m. § 99 StPO andererseits wertungswidersprüchlich wäre.

Eine Bezugnahme auf die Bestimmung zur getrennten Aktenführung, die bisher in § 101 Abs. 4 StPO geregelt und nunmehr in § 101 Abs. 2 StPO-E überführt worden ist, war und ist mangels Eingreifens dieser Regelung für die Postbeschlagnahme entbehrlich.

Zu Artikel 7 (Änderung des Bundeskriminalamtgesetzes)

Die Änderung des § 16 Abs. 3 Satz 3 BKAG trägt dem Umstand Rechnung, dass die Verwendung personenbezogener Information, die durch den Einsatz technischer Mittel zur Eigensicherung nach § 16 BKAG erlangt wurden, sich nicht allein nach der bislang in § 16 Abs. 3 Satz 3 in Bezug genommenen Regelung des bisherigen § 161 Abs. 2 StPO (nunmehr § 161 Abs. 3 StPO-E) bestimmt, sondern – je nach Fallgestaltung – auch nach dem neuen Absatz 2 in § 161 StPO-E bzw. – im Falle der akustischen Wohnraumüberwachung – nach § 100d Abs. 5 Nr. 3 StPO-E.

Zu Artikel 8 (Änderung des Gerichtsverfassungsgesetzes)

§ 120 Abs. 4 Satz 2 GVG wird redaktionell angepasst: Infolge der Neuregelungen zu den Benachrichtigungspflichten in § 101 Abs. 4 bis 8 StPO-E entfällt die bislang in § 100d Abs. 9 Satz 4 StPO enthaltene Zuständigkeit der Oberlandesgerichte für Entscheidungen über die Zustimmung zur Zurückstellung der Benachrichtigung über 18 Monate hinaus in Fällen der akustischen Wohnraumüberwachung (vgl. dazu die Erläuterungen zu § 101 Abs. 8 StPO-E). Die Bezugnahme in § 120 Abs. 4 Satz 2 GVG auf § 100d Abs. 9 Satz 4 StPO ist daher zu streichen.

Zu Artikel 9 (Änderung des Einführungsgesetzes zur Strafprozessordnung)

§ 12 EGStPO-E trifft Übergangsregelungen für die Statistikpflichten, die vom Telekommunikationsgesetz (§ 110 Abs. 8 TKG) und von der Telekommunikations-Überwachungsverordnung (§ 1 Nr. 8, § 25 und Anlage zu § 25 TKÜV) in die Strafprozessordnung verlagert (§ 100b Abs. 5, 6 StPO-E) bzw. dort neu begründet (§ 100g Abs. 4 StPO) werden. Absatz 1 Satz 2 stellt klar, dass die schon bestehende Statistikregelung in § 100e StPO(-E) von dieser Übergangsregelung unberührt bleibt.

Zu Artikel 10 (Änderung des IStGH-Gesetzes)

Die in der Vorschrift enthaltenen Verweisungen auf § 100a Abs. 1 Satz 1, § 101 Abs. 1, § 100b Abs. 5 und 6 StPO werden redaktionell an die Neufassung der §§ 100a, 100b, 477 Abs. 2 StPO-E angepasst. Ferner werden das in Absatz 1 Nr. 3 enthaltene Wort „Informationen“ durch die Wörter „personenbezogene Daten“ und das Wort „Vernichtung“ durch „Löschung“ ersetzt und damit an die Begriffe der Strafprozessordnung angeglichen.

Zu Artikel 11 (Änderung des Wertpapierhandelsgesetzes)

Die in § 16b Abs. 1 Satz 3 WpHG durch die Verweisung auf § 101 StPO enthaltene Benachrichtigungspflicht wird beibehalten durch die neue Bezugnahme auf § 101 Abs. 4 und 5 StPO-E. Von der Bezugnahme auch auf § 101 Abs. 6 ff. StPO-E wird abgesehen, da die dort vorgesehene gerichtliche Überprüfung der Zurückstellung der Benachrichtigung auch bislang im Bereich des Wertpapierhandelsgesetzes nicht vorgesehen ist und in Anbetracht der ge-

ringeren Eingriffsintensität der in § 16b Abs. 1 Satz 3 WpHG vorgesehene Maßnahme (lediglich Speicherungsanordnung, aber keine Zugriffsregelung) auch künftig nicht geboten erscheint.

Zu Artikel 12 (Änderung des Gesetzes über die Anwendung unmittelbaren Zwanges und die Ausübung besonderer Befugnisse durch Soldaten der Bundeswehr und verbündeter Streitkräfte sowie zivile Wachpersonen)

§ 7 Abs. 2 Satz 2 UZwGBw wird redaktionell angepasst, soweit er auf den bisherigen § 110 StPO verweist. Einer Bezugnahme auch auf den neuen Absatz 3 in § 110 StPO-E bedarf es in der von § 7 UZwGBw erfassten Fallgestaltung nicht.

Zu Artikel 13 (Änderung der Telekommunikations-Überwachungsverordnung)

Zu Nummer 1 (§ 1 TKÜV)

Zu Buchstaben a und c (Nummer 8)

Die auf die Erstellung der Statistik nach § 110 Abs. 8 TKG bezogene Regelung in § 1 Nr. 8 TKÜV wird in Folge der Aufhebung des § 110 Abs. 8 TKG zum 1. Januar 2009 ebenfalls zu diesem Zeitpunkt aufgehoben. Entsprechende statistische Erhebungen werden künftig nach Maßgabe von § 100b Abs. 5 und 6 StPO-E erfolgen. Zu den jeweiligen Übergangsregelungen vgl. Artikel 16 Abs. 2.

Zu Buchstabe b (Nummer 9)

Die neue Nummer 9 greift die erweiterte Verordnungsermächtigungen nach § 110 Abs. 2 TKG-E auf, nach denen künftig auch Regelungen über die grundlegenden technischen Anforderungen und die organisatorischen Eckpunkte für die Erteilung von Auskünften geregelt werden können. Diese Erweiterung des Regelungsbereichs ist wegen der in § 100g Abs. 1 StPO-E vorgesehenen Befugnis der Strafverfolgungsbehörden, Verkehrsdaten auch in Echtzeit zu erheben, geboten. Die konkrete Festlegung der Anforderungen an das Übermittlungsverfahren und das Datenformat sowie die Bestimmung der weiteren technischen und organisatorischen Ausgestaltungen bleibt einer künftigen Anpassung der TKÜV vorbehalten.

Zu Nummer 2 (§ 3 Abs. 2 TKÜV)

Zu Buchstabe a (Satz 1 Nr. 5)

Die Änderung hebt die Pflichtgrenze gemäß § 3 Abs. 2 Satz 1 Nr. 5 TKÜV(-E), ab deren Überschreiten Betreiber von Telekommunikationsanlagen technische und organisatorische Vorkehrungen zu treffen haben, von bisher 1 000 auf 10 000 angeschlossene Teilnehmer oder sonstige Nutzungsberechtigte an. § 110 Abs. 2 Nr. 2 Buchstabe c TKG bestimmt, dass in der Telekommunikations-Überwachungsverordnung geregelt werden kann, bei welchen Telekommunikationsanlagen u. a. aus Gründen der Verhältnismäßigkeit keine technischen Einrichtungen vorgehalten und keine organisatorischen Vorkehrungen für die Umsetzung von Überwachungsmaßnahmen getroffen werden müssen. Dadurch sollen kleine Telekommunikationsunternehmen von den für sie nicht unerheblichen Aufwendungen befreit werden, die für die Vorhaltung der technischen Einrichtungen und das Treffen der organisatorischen Vorkehrungen für die Umsetzung angeordneter Überwachungsmaßnahmen anfallen. Da man bei der Erstellung der TKÜV insoweit über keinerlei Erfahrungswerte verfügte, wurde der Grenzwert seinerzeit so festgelegt, dass die Betreiber solcher Telekommunikationsanlagen von der Vorhalteverpflichtung befreit sind, an die nicht mehr als 1 000 Teilnehmer oder sonstige Nutzungsberechtigte angeschlossen sind. Zwischenzeitlich erfolgte Prüfungen der Bundesnetzagentur über die Verteilung von Überwachungsmaßnahmen auf Unternehmen unterschiedlicher Größen ergaben, dass Netzbetreiber, deren Telekommunikationsanlage nur wenig größer ist als der durch die Verordnung festgelegte Grenzwert durchschnittlich nur etwa alle elf Jahre mit der Umsetzung einer Überwachungsmaßnahme rechnen müssen. In Anbetracht dessen ist die Verpflichtung, hierfür Vorkehrungen zu treffen, als nicht mehr verhältnismäßig zu werten. Ein vertretbarer Wert wird erreicht, wenn man die Pflichtgrenze von derzeit 1 000 auf künftig 10 000 Teilnehmer oder sonstige Nutzungsberechtigte anhebt.

Über die auf Erfahrungswerten der herkömmlichen Sprachtelefonie beruhenden Erkenntnisse hinaus hat die Bundesnetzagentur auch eine Studie hinsichtlich der Unternehmensgrößen von E-Mail-Anbietern beauftragt, deren Ergebnisse zumindest die gleiche Anhebung ratsam erscheinen lassen. Für den Bereich der Internet-Telefonie (VoIP) liegen zwar bislang keine Erfahrungswerte vor, es ist aber kein Grund zu erkennen, weshalb sich die Tendenz, dass kleine Netzbetreiber oder Diensteanbieter nur sehr selten für die Umsetzung einer Überwachungsmaßnahme in Anspruch genommen werden, für diesen Bereich auffällig ändern sollte.

Sollte sich im Zuge der weiteren technischen Entwicklung oder wegen erheblicher struktureller Veränderungen am Telekommunikationsmarkt – etwa aufgrund der zunehmenden Verbreitung der Internet-Telefonie – erweisen, dass die erhöhte Pflichtgrenze zu nicht mehr hinnehmbaren grundsätzlichen Problemen bei der Umsetzung von Überwachungsmaßnahmen führt, wird erforderlichenfalls über eine erneute Anpassung der Pflichtgrenze zu entscheiden sein. Nicht zu besorgen sein dürfte jedoch, dass einzelne Telekommunikationsunternehmen die Anhebung der Pflichtgrenze gezielt dazu nutzen werden, den telekommunikationsrechtlichen Verpflichtungen nach dem TKG und der TKÜV durch eine Unternehmensaufspaltung in kleinere, rechtlich selbständige Einheiten zu entgehen, da § 3 Abs. 2 TKÜV nicht an die Unternehmensgröße als solche sondern an die Größe der genutzten Telekommunikationsanlage anknüpft. Erforderlichenfalls wäre jedoch auch hierauf durch erneute Anpassungen in § 3 TKÜV zu reagieren, um einen effektiven Einsatz von Telekommunikationsüberwachungsmaßnahmen auch künftig sicherzustellen.

Zu Buchstabe b (Satz 3)

Der neue § 3 Abs. 2 Satz 3 TKÜV-E greift die durch das Gesetz zur Änderung telekommunikationsrechtlicher Vorschriften vom 18. Februar 2007 eingefügte Regelung des § 110 Abs. 1 Satz 1 Nr. 1a TKG auf und nimmt – als Rückausnahme zu der Ausnahmevorschrift in Satz 1 – die nach § 110 Abs. 1 Satz 1 Nr. 1a TKG verpflichteten Anlagenbetreiber und Diensteanbieter von der durch § 3 Abs. 2 Satz 1 Nr. 1 und 2 TKÜV geregelten Befreiung von der Pflicht, Vorkehrungen für die Umsetzung von Überwachungsmaßnahmen zu treffen, aus. Die Regelung des § 110 Abs. 1 Satz 1 Nr. 1a TKG betrifft Fallgestaltungen, bei denen das Erbringen des Telekommunikationsdienstes derart zwischen verschiedenen Diensteanbietern oder Netzbetreibern aufgeteilt ist, dass die einzelnen an der Erbringung der Telekommunikation Beteiligten nur noch bestimmte Teilfunktionen wahrnehmen und kein Beteiligter mehr einen vollständigen Überblick über oder Zugriff auf alle den jeweiligen Telekommunikationsvorgang betreffende technische Vorgänge hat. Diese „Arbeitsteilung“ wird insbesondere durch neue Technologien ermöglicht, bei denen die zur Steuerung der Telekommunikation erforderlichen Signale und die den Kommunikationsinhalt repräsentierenden Signale über voneinander getrennte Telekommunikationsanlagen übermittelt werden, wie dies etwa bei der so genannten VoIP-Telefonie der Fall ist. In einer solchen Fallgestaltung ist eine Überwachung der Telekommunikation nur durch das Zusammenwirken der einzelnen an der Erbringung der Telekommunikation Beteiligten möglich. Der neu eingefügte § 3 Abs. 2 Satz 3 TKÜV-E ist erforderlich, um zu verhindern, dass die Neuregelung des § 110 Abs. 1 Satz 1 Nr. 1a TKG unter Berufung auf die Ausnahmevorschrift des § 3 Abs. 2 Satz 1 Nr. 1 oder Nr. 2 TKÜV leerläuft.

Zu Nummer 3 (§ 4 Abs. 2 TKÜV)

Es handelt sich um eine redaktionelle Folgeänderung zur Aufhebung von § 21 TKÜV (vgl. die dortige Begründung).

Zu Nummer 4 (§ 7 Abs. 1 TKÜV)

§ 7 Abs. 1 Satz 1 Nr. 7 TKÜV-E passt die Verpflichtung der Diensteanbieter zur Mitteilung von Standortangaben im Zuge einer Telekommunikationsüberwachungsmaßnahme an die aktuelle technische Entwicklung an. Die Angabe von Standortdaten war bis vor kurzem nur bei der Überwachung von Mobiltelefonen von praktischer Bedeutung. Dies hat sich mit der zunehmenden Verfügbarkeit weiterer nicht ortsgebunden nutzbarer Telekommunikationsdienste (z. B. VoIP) geändert. Hieraus ist das Bedürfnis erwachsen, die auf die Standortangabe gerichtete Vorschrift in Nummer 7 entsprechend anzupassen.

Zu Nummer 5 (§ 11 TKÜV)

Der in § 11 Satz 1 TKÜV-E eingefügte Verweis auf die Vorschrift des § 12 Abs. 2 Satz 1 TKÜV(-E) ermächtigt die Bundesnetzagentur, die technischen Einzelheiten des elektronischen Übermittlungsverfahrens in der Technischen Richtlinie nach § 110 Abs. 3 TKG festzulegen.

Zu Nummer 6 (§ 12 Abs. 2 TKÜV)

Die Änderung beseitigt die bisherige missverständliche Formulierung, nach der unklar ist, ob auch im Falle der Übermittlung einer Anordnung auf gesichertem elektronischem Weg eine anschließende Übermittlung eines Originals der Anordnung zu erfolgen hat. Die geänderte Fassung, nach der das Wort „vorab“ sich nur noch auf die Übermittlung per Telefax bezieht, stellt klar, dass im Falle einer nicht per Telefax erfolgenden Übermittlung der Anordnung auf gesichertem elektronischem Wege eine anschließende Übermittlung des Originals der Anordnung oder einer beglaubigten Abschrift der Anordnung nicht erforderlich ist.

Zu Nummer 7 (§ 19 Abs. 3 TKÜV)

Es handelt sich um eine Folgeänderung zur Aufhebung von § 21 TKÜV (vgl. die dortige Begründung).

Zu Nummer 8 (§ 21 TKÜV)

Die bisherige Regelung, wonach die Bundesnetzagentur für Betreiber von Telekommunikationsanlagen, an die nicht mehr als 10 000 Teilnehmern oder sonstige Nutzungsberechtigte angeschlossen sind, unter bestimmten Voraussetzungen Abweichungen von den Vorschriften der TKÜV dulden sollte, ist aufgrund der Anhebung der Pflichtgrenze in § 3 Abs. 2 Satz 1 Nr. 5 TKÜV-E auf 10 000 Teilnehmer oder sonstige Nutzungsberechtigte entbehrlich und daher aufzuheben. Eine Beibehaltung dieser Ausnahmevorschrift und Anhebung der bisher bestimmten Grenze ist nicht geboten.

Zu Nummer 9 (§ 22 TKÜV)

Wegen der Aufhebung des § 21 TKÜV stellt § 22 TKÜV die einzige Regelung zu Abweichungen in Abschnitt 5 dar; die Überschrift ist daher entsprechend anzupassen.

Zu Nummer 10 (§ 25 TKÜV und Anlage zu § 25 TKÜV)

Es handelt sich um eine Folgeänderung zur Aufhebung der Statistikpflichten nach § 110 Abs. 8 TKG zum 1. Januar 2009.

Zu Nummer 11 (§ 27 Abs. 8 TKÜV)

Es handelt sich um eine Folgeänderung zur Aufhebung von § 21 TKÜV. Der nur noch für § 27 TKÜV weiterhin bedeutsame Regelungsgehalt des § 21 Abs. 4 Satz 1 Nr. 1 TKÜV ist ausdrücklich in § 27 Abs. 8 Satz 1 TKÜV-E aufzunehmen.

Zu Artikel 14 (Änderung des Gesetzes zur Änderung der Strafprozessordnung vom 20. Dezember 2001)

Durch die Vorschrift wird die Befristung der Geltungsdauer der §§ 100g, 100h StPO durch Artikel 2 des Gesetzes zur Änderung der Strafprozessordnung vom 20. Dezember 2001 aufgehoben. Damit wird sichergestellt, dass die durch das vorliegende Gesetz neu gefassten §§ 100g, 100h StPO nicht zum 1. Januar 2008 außer Kraft treten.

Zu Artikel 15 (Zitiergebot)

Mit der Vorschrift wird dem Zitiergebot des Artikels 19 Abs. 1 Satz 2 GG entsprochen.

Zu Artikel 16 (Inkrafttreten)

Die Vorschrift regelt das Inkrafttreten.