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. Dadurch 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, dürfen – entgegen einer verbreiteten Auffassung im Schrifttum – nicht pauschal auf andere verdeckte Ermittlungsmaßnahmen übertragen werden (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 Anordnungsvoraussetzungen 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. Dies 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 z. B. 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 zahlreiche Personen in den Wirkungsbereich der Maßnahme einbezogen, ohne dafür einen Anlass gegeben zu haben, d. h. eine Vielzahl von – auch dritten – Personen kann von diesen Maßnahmen betroffen sein (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 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 Ermittlungen 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). Schwierigkeiten bereitete in der Praxis die Feststellung, welche Personen Beteiligte im Sinne des § 101 Abs. 1

Satz 1 StPO und damit zu benachrichtigen sind (a. a. O., S. 451). Diese Unzulänglichkeiten 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 belegt auch, dass das in der Praxis bestehende Defizit bei der Auseinandersetzung mit der Frage der Benachrichtigung nicht durch die Ausübung der Dienstaufsicht behoben werden kann. 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 nicht nur auf alle eingriffsintensiven verdeckten Ermittlungsmaßnahmen, sondern konkretisiert zugleich auch den Kreis der zu benachrichtigenden Personen. Damit wird der nachträgliche Rechtsschutz gestärkt 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 erstreckt (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 für die Dauer von jeweils einem Monat zulässig.

Ausgehend von den Erkenntnissen der Untersuchung, die die Telekommunikationsüberwachung als ein wichtiges und unabdingbares Ermittlungsinstrument insbesondere im Bereich der opferlosen (Transaktions-)Kriminalität herausgearbeitet hat (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, 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 Ermittlungsrichters 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.). Die Umsetzung beider Vorschläge erscheint im Hinblick auf das Ziel einer Stärkung der unabhängigen Kontrolle durch einen Ermittlungsrichter nicht geboten und wäre zudem mit hohem Kosten- und Personalaufwand verbunden. Es ist indessen eine der wichtigsten und vornehmsten 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 akustischen Wohnraumüberwachung durch das Gesetz zur Umsetzung des Urteils des Bundes-

verfassungsgerichts 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 1979, 1 ff.; Amelung, Informationsbeherrschungsrechte im Strafprozess, 1990; Fezer, Grundfragen 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 der gesetzlichen Grenzen von Ermittlungsmaßnahmen 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. 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 das rechtsstaatliche Gemeinwesen, sondern auch das Recht des Beschuldigten auf ein faires, rechtsstaatliches Verfahren beeinträchtigen, weil die aufgrund von Erhebungs- und Verwertungsverboten nicht erlangten Erkenntnisse nicht nur der Anklage sondern auch der Verteidigung entzogen sind. 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 mithin 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 Einwilligung (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 StPO ein Zeugnisverweigerungsrecht zubilligt, sieht § 53b Abs. 2 StPO-E ein relatives, durch eine Prüfung der Verhältnismäßigkeit im Einzelfall determiniertes Beweiserhebungs- und -verwertungsverbot unter der Voraussetzung vor, das eine Abwägung der widerstreitenden Interessen im konkreten Fall dies gebietet.

- Berufshelfer (§ 53a StPO) werden von § 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 Reichweite der Neuregelung in § 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 keine Anwendung findet.

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 sie bekannt sind (§ 100b Abs. 2 Nr. 1 StPO-E).

- Durch die in § 100b Abs. 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 für die Zulässigkeit der Beschlagnahme solcher Daten die Anwendbarkeit der allgemeinen Beschlagnahmevorschriften der §§ 94 ff. StPO klar (§ 100g Abs. 3 StPO-E). Dies entspricht auch den verfassungsrechtlichen Vorgaben, die sich aus dem inzwischen ergangenen Urteil des Bundesverfassungsgericht vom 2. März 2006, 2 BvR 2099/04, ergeben, 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, o. g. Urt., NJW 2006, 976, 978).

- 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 ermittlungsrichterlichen Tätigkeit fördert und damit eine gesteigerte Effektivität des Richtervorbehalts 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 § 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; 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,

[1] IMEI = International Mobile Equipment Identity.

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 zur 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 ist und nicht auf die Erhebung von – bei Stellung 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 richtet (vgl. BT-Drs. 14/7008, S. 7).

Zu berücksichtigen ist darüber hinaus, dass die §§ 111 bis 113 TKG Gegenstand eines derzeit beim Bundesverfassungsgericht anhängigen Verfassungsbeschwerdeverfahrens sind (1 BvR 1299/05). Während der Anhängigkeit eines solchen Verfahrens erscheint es ratsam, Änderungen der betroffenen Vorschriften nur dann vorzunehmen, wenn hierzu ein unabweisbares Bedürfnis besteht. In Anbetracht der inzwischen gefestigten Rechtsprechung, die zur Anwendung der §§ 111 ff. TKG gelangt, ist ein solches unabweisbares Bedürfnis nicht gegeben. Ein gesetzgeberischer Handlungsbedarf besteht daher insoweit derzeit nicht.

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 Artikel 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. PC) räumlich getrennte Teile eines Computersystems (z. B. Server 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 zu erstrecken, zu denen der Betroffene zugangsberechtigt ist, und Daten, die für die Untersuchung von Bedeutung sein können, zu speichern, wenn bis zur Sicherstellung der Datenträger ihr Verlust zu besorgen ist.

- Im Zusammenhang mit der von Artikel 17 des Übereinkommens angesprochenen beschleunigten Sicherung von Verkehrsdaten ist ferner problematisch, dass bei Auskunftsverlangen nach den §§ 100g, 100h StPO die benötigten Daten entweder überhaupt nicht gespeichert werden oder mitunter bereits automatisch gelöscht sind, bevor eine richterliche Auskunftsanordnung erwirkt werden oder eine entsprechende staatsanwaltschaftliche Eilanordnung ergehen kann. Es ist daher fraglich, ob die grundsätzlich notwendige richterliche 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 Kontaktaufnahme durch die Strafverfolgungsbehörden mit den Diensteanbietern mit der Bitte um vorläufige Sicherung der benötigten Daten (vgl. Gercke, MMR 2004, 801, 802) zu begegnen, ist deshalb zunächst erwogen worden, in § 100g StPO-E die zur Mitwirkung bei entsprechenden Auskunftsersuchen 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 eine richterliche 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 von Auskunftsersuchen an Stellen, die Telekommunikationsdienste geschäftlich erbringen, wie bisher in § 100g Abs. 1 Satz 1 StPO vorgesehen, 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 deutlich 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 u.

a. durch die weitgehend Bezugnahme in § 100g Abs. 2 Satz 1 StPO-E auf § 100b StPO-E erreicht.

Hinsichtlich der Erhebung von Standortdaten in Echtzeit soll es allerdings bei der bisherigen rechtspolitischen Entscheidung bleiben, dass dies bei Vorliegen einer in § 100a StPO-E genannten schweren Straften zulässig ist. 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 gerade nicht mit 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 Auf-

schluss 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. 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 entsprechen 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. Die Verpflichtung der Mitgliedstaaten zur Übermittlung der im Einzelnen beschriebenen Angaben bedingt die abweichungsfeste Ausgestaltung der Verfahrensvorschriften zu ihrer statistischen Erhebung.

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 Rahmenbe-

schluss, der auf die Artikel 31, 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 Rechtsvorschriften 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 ge-

schwächt 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 Nichtigkeitsklage (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 § 110a 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 § 110a 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 § 110a 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 § 110a Abs. 7 TKG-E dürfen Daten, die Aufschluss über den Inhalt der Kommunikation geben, auf Grund der vorstehenden Speicherungsregelungen nicht gespeichert werden.

§ 110a Abs. 1 Satz 1 TKG-E sieht eine Speicherungsdauer von sechs Monaten vor.

Die Verwendung der gespeicherten Verkehrsdaten ist nach § 110b Abs. 1 TKG-E für Strafverfolgungszwecke zulässig. Nach § 100g Abs. 1 StPO-E können die Strafverfolgungsbehörden 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 Investitionen zur Erfüllung von Speicherungspflichten

(etwa nach § 9 des Geldwäschegesetzes) nicht erstattet. Überdies wäre eine Entschädigung mit erheblichen praktischen Problemen verbunden, da 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 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, NJW 2006, 976, 981; BVerfGE 107, 299, 316). Die Befugnis der Strafverfolgungsbehörden, Auskunft von Diensteanbietern über gespeicherte 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 zu-

nehmenden 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.), 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. Hinzu kommt, dass solche Aufbewahrungsanordnungen regelmäßig nur während der üblichen Geschäftszeiten bei den Diensteanbietern angebracht werden können, Recherchen der Ermittlungsbehörden jedoch aus ermittlungstaktischen Gründen gerade auch außerhalb der üblichen Geschäftszeiten stattfinden müssen.

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, NJW 2006, 976, 980 f.). 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 der Bundesregierung belastbare Angaben zu den tatsächlich zu erwartenden Kosten nicht vorliegen.

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, NJW 2006, 976, 980; 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 § 110a Abs. 2 bis 4 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, NJW 2006, 1939, 1943), 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.

VIII.

Die Gesetzgebungskompetenz des Bundes folgt aus Artikel 74 Abs. 1 Nr. 1 GG (gerichtliches Verfahren) und Artikel 73 Nr. 7 GG (Telekommunikation).

Aufgrund der in § 100b Abs. 5 und 6 sowie in § 100g Abs. 4 StPO-E vorgesehenen - abweichungsfesten (vgl. Artikel 7 − § 12 EGStPO-E) - Verpflichtung der Länder, statistische Daten zu erheben und an das Bundesamt für Justiz weiter zu leiten, bedarf das Gesetz nach Artikel 84 Abs. 1 Satz 5 und 6 GG der Zustimmung des Bundesrates.

IX.

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.

X.

Von dem Entwurf sind folgende kostenrelevante Auswirkungen zu erwarten:

1.

Die Neufassung der Regelung der verdeckten Ermittlungsmaßnahmen in der Strafprozessordnung kann für die Behörden und Gerichte des Bundes und der Länder Mehraufwand verursachen, dessen Umfang sich jedoch nicht verlässlich schätzen lässt. Dieser Mehraufwand kann insbesondere durch die Erfüllung von Kennzeichnungs-, Benachrichtigungs- und Statistikpflichten sowie durch die eine eventuell steigende Wahrnehmung der nunmehr ausdrücklich eröffneten Möglichkeit für Betroffene, nachträglichen Rechtsschutz bei allen verdeckten Ermittlungsmaßnahmen zu erwirken, entstehen. Der hiermit verbundene erhöhte Aufwand ist aufgrund verfassungs- bzw. europarechtlicher (Artikel 10 der Richtlinie 2006/24/EG) Vorgaben nicht vermeidbar.

Zusätzlicher, nicht näher quantifizierbarer Aufwand für Strafverfolgungsbehörden und Gerichte kann zudem daraus resultieren, dass aufgrund der Einführung von Speicherungspflichten für Verkehrsdaten künftig mehr Straftaten als bislang aufgeklärt werden können. Dieser Mehraufwand ist aufgrund der Verpflichtung zur Umsetzung der Richtlinie 2006/24/EG nicht vermeidbar und im Interesse einer effektiven Strafverfolgung geboten.

Die Umsetzung der Richtlinie zur „Vorratsspeicherung“ von Verkehrsdaten wird voraussichtlich zu vermehrten, der Entschädigungspflicht nach § 23 JVEG unterliegenden Auskunftsersuchen der Strafverfolgungsbehörden an Telekommunikationsunternehmen nach § 100g StPO führen. Hierdurch wird sich die Summe der aus den Haushalten von Bund und Ländern zu erbringenden Entschädigungszahlungen erhöhen. In welchem Umfang dies der Fall sein 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. Grob geschätzt könnte die Anzahl zusätzlicher entschädigungspflichtiger Auskunftsersuchen zwischen 500 und 10.000 pro Jahr liegen. Damit 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 zusätzlich 8.500 bis 170.000 Euro pro Jahr, das im Hinblick auf die

primäre Zuständigkeit der Länder für die Strafverfolgung zum wesentlichen Teil aus den Länderhaushalten zu finanzieren sein wird.

Diesem Mehraufwand bei öffentlichen Stellen stehen nicht näher bezifferbare unmittelbare und mittelbare Einsparungen gegenüber, die daraus resultieren, dass die Ermittlungsmöglichkeiten im Strafverfahren effektiviert und damit die hohe gesamtgesellschaftliche Schäden verursachende Kriminalität besser bekämpft werden kann.

Haushaltsausgaben ohne Vollzugsaufwand sind nicht zu erwarten.

2.

Für die von der Speicherungspflicht für Verkehrsdaten betroffenen Unternehmen entsteht durch die ordnungsgemäße, auch datenschutzrechtliche Schutzvorkehrungen erfüllende Speicherung ein zusätzlicher Aufwand, der sich derzeit nicht genau beziffern lässt und sich auch künftig ohne umfassende Mitwirkung der betroffenen Unternehmen nicht genau quantifizieren lassen wird. 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 grundsätzlich bei ihrer Preisgestaltung einkalkulieren und damit gegebenenfalls auf ihre Kunden abwälzen werden, soweit dies der Telekommunikationsmarkt zulässt. Nach Schätzungen eines großen deutschen Telekommunikationsdiensteanbieters mit einem Jahresumsatz von annähernd 60 Mrd. Euro betragen die bei ihm durch die Erfüllung der Speicherungspflichten entstehenden Zusatzkosten etwa 700.000 Euro pro Jahr und damit 0,00116 % des Jahresumsatzes dieses Anbieters. Das Verbraucherpreisniveau im Bereich der Telekommunikationsdienstleistungen dürfte daher durch die Erfüllung der Speicherpflichten voraussichtlich nicht oder allenfalls ganz geringfügig steigen.

Bei kleineren Unternehmen wird von der in § 3 Abs. 2 Nr. 7 TKÜV-E vorgesehenen Anhebung der sog. Marginaliengrenze von 1.000 auf 20.000 Teilnehmer bzw. sonstigen Nutzungsberechtigte eine deutliche Entlastung ausgehen.

Zudem werden die betroffenen Unternehmen 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 entbehr-

lich werden dürfte 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.

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.

3.

Der Entwurf enthält keine Regelungen zur Entschädigung der Telekommunikationsunternehmen. Eine Neuregelung der Entschädigung und die Frage ihres Standortes werden Gegenstand eines besonderen Gesetzgebungsverfahrens, das unverzüglich 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 ein. Zur grundsätzlichen Konzeption wird auf die obigen Ausführungen im Allgemeinen Teil der Begründung (dort unter A. I. 3.) Bezug genommen

Zu Absatz 1

Absatz 1 begründet – flankiert durch Löschungs- und Dokumentationspflichten sowie der Möglichkeit gerichtlicher Prüfung – 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, 4 StPO) umfasst sind. Die Regelung übernimmt damit die vom Gesetzgeber bereits in § 100h Abs. 2 StPO getroffene Wertung, diesen Berufsgruppen im Rahmen der Reichweite des ihnen zukommenden Zeugnisverweigerungsrechts besonderen Schutz zukommen zu lassen. Zugleich wird damit die bisherige Spezialregelung in § 100h Abs. 2 StPO entbehrlich. Der damit einhergehende Schutz 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 damit, soweit die Genannten im Wirkungsbereich ihres jeweiligen Zeugnisverweigerungsrechtes tätig werden, durch Ermittlungsmaßnahmen gleich welcher Art nicht 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 nehmen zu können, 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 bedarf als Ausprägung des Kernbereichs privater Lebensgestaltung, der dem staatlichen Zugriff schlechthin entzogen ist, umfassenden Schutzes (BVerfGE 109, 279, 322).

Das Zeugnisverweigerungsrecht des Abgeordneten und das damit korrespondierende Beschlagnahmeverbot ist bereits in Artikel 47 GG enthalten und schützt das mandatsbezogene Vertrauensverhältnis zwischen dem Abgeordneten und Dritten. Dieser bereits verfassungsrechtlich unabhängig von Verhältnismäßigkeitserwägungen im Einzelfall vorgegebene Schutz dient der Stärkung des freien Mandats und zugleich der ungestörten parlamentarischen Arbeit sowie daraus folgend der Funktionsfähigkeit der Volksvertretung. 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).

Die Betroffenheit der genannten Personen ist nicht erst dann gegeben, wenn sie zielgerichtet in die Maßnahme einbezogenen sind, sondern schon dann, wenn sie (lediglich) mitbetroffen sind, d. h. von der Maßnahme berührt werden.

Im Umfang des von Satz 1 begründeten Erhebungsverbots enthält Satz 2 ein Verwertungsverbot. Danach dürfen nach Satz 1 in unzulässiger Weise erlangte Erkenntnisse in Strafverfahren nicht verwertet werden. Dieses Beweisverwertungsverbot trägt zum einen dem Umstand Rechnung, dass nicht stets von vornherein erkennbar ist, ob von einer Ermittlungsmaßnahme ein von Satz 1 erfasster Berufsgeheimnisträger in einer das Erhebungsverbot auslösenden Weise betroffen sein wird. Zum anderen sichert das Verwertungsverbot des Satzes 2 aber auch die Einhaltung des Erhebungsverbotes nach Satz 1, weil sich so Verstö-

ße gegen das Erhebungsverbot des Satzes 1 als ineffektiv – weil im Ergebnis keine verwertbaren Erkenntnisse hervorbringend – erweisen.

Da aus einem Erhebungsverbot nicht automatisch 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 beeinträchtigt werden kann, ist das Verwertungsverbot auch ausdrücklich im Gesetzestext zu verankern.

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.

Nach Satz 4 ist die Tatsache der Erlangung unter das Erhebungsverbot des Satzes 1 fallender Erkenntnisse sowie die Löschung dieser Erkenntnisse in geeigneter Form 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.

Die Regelungen in Satz 5 und 6 sind § 100c Abs. 7 StPO nachgebildet.

Nach Satz 5 hat die Staatsanwaltschaft, wenn Zweifel bestehen, ob erlangte Erkenntnisse unter das Erhebungs- und Verwertungsverbot nach Satz 1 und 2 fallen, unverzüglich eine Entscheidung des Gerichts über die Verwertbarkeit herbeizuführen. Damit wird gewährleistet, dass eine unabhängige Stelle entscheidet. Zuständig für die Entscheidung nach Satz 5 ist dasjenige Gericht, das für die Anordnung der Maßnahme zuständig ist, im Ermittlungsverfahren also regelmäßig der Ermittlungsrichter am Sitz der Staatsanwaltschaft, § 162 StPO-E.

Satz 6 gewährleistet die Effektivität dieser Regelung dadurch, dass eine die Nichtverwertbarkeit feststellende Entscheidung des Gerichts für das weitere Verfahren bindend ist. Von einer Bindungswirkung auch bei einer die Verwertbarkeit bejahenden Entscheidung war hingegen abzusehen, da die Frage der Verwertbarkeit von Beweismitteln stets vom erkennenden Gericht zu beurteilen ist und nur ausnahmsweise dessen Beurteilung dann entzogen sein muss, wenn dies erforderlich ist, um die Vertiefung eines erfolgten – unzulässigen – Eingriffs zu vermeiden (vgl. dazu bereits BT-Drs 15/4533, S. 28).

Zu Absatz 2

Absatz 2 enthält ein relatives, an Verhältnismäßigkeitsgesichtspunkten orientiertes und in der Rechtsprechung im Rahmen der so genannte Abwägungslehre (vgl. Meyer-Goßner, a. a. O., Einl., Rn. 55a m. w. N.) im Grundsatz anerkanntes 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 in Bezug genommenen Medienmitarbeiter. Im Rahmen der von Satz 1 geforderten Abwägung ist das primär öffentliche – je nach Fallgestaltung (Opferinteressen) allerdings auch individuell begründete – Interesse an einer wirksamen, auf die Ermittlung der materiellen Wahrheit und die Findung einer gerechten Entscheidung gerichteten Strafrechtspflege mit dem öffentlichen Interesse an den durch die zeugnisverweigerungsberechtigten Personen wahrgenommenen Aufgaben und dem 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 ihrem Wesen 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 Personen sowie der Grundsatz, dass kein Beschuldigter verpflichtet ist, aktiv an seiner eigenen Überführung mitzuwirken, gebieten tendenziell Zurückhaltung bei der Erhebung von Erkenntnisse aus dem vom Zeugnisverweigerungsrecht des Berufsgeheimnisträgers geschützten Sphäre. Da der Tätigkeit der Beratungs- und Heilberufe in einem sozialen Rechtsstaat auch gesamtgesellschaftlich 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 teil-

weise oder ganz nicht gegeben wäre – sich die Notwendigkeit einer Beschränkung oder Unterlassung der Maßnahme ergeben; Letzteres stellt Satz 2 ausdrücklich klar.

In dieses Regelungskonzept des Absatzes 2 werden auch die in § 53 Abs. 1 Satz 1 Nr. 5 StPO in Bezug genommenen Medienschaffenden eingebunden. Die Verfassung gewährt der Tätigkeit der Medienschaffenden 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 Medienschaffenden 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 sich aufgrund zwischenzeitlicher Änderungen der Sachlage eine im Ergebnis andere Bewertung ergeben 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. BGHSt 18, 227, 230; 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. 3 StPO auf die jeweiligen Berufshelfer erstreckt.

Zu Absatz 4

Entsprechend den 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 die Schutzregelungen nicht allein aufgrund bloßer Vermutungen zu umgehen. Dieser Schutz wird – ebenfalls rechtspolitischem Willen Rechnung tragend – durch Satz 2 für Medienschaffende bei Antrags- und Ermächtigungsdelikten zusätzlich dahingehend verstärkt, dass die Verstrickungsregelung des Satzes 1 bei Medienangehörigen, die in Verdacht stehen, in die Tat verstrickt zu sein, erst dann anzuwenden ist, wenn der erforderliche Antrag vorliegt bzw. die Ermächtigung erteilt ist.

Zu Absatz 5

Absatz 5 stellt klar, dass die spezielleren Regelungen des § 97 und des § 100d 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 § 100c 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 § 53 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 Ermittlungsrichters 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, da 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 Mobilfunkmarktes in Deutschland 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, 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 „ohne Wissen der Betroffenen“, die 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.

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).

3. In Absatz 1 Nr. 2 wird klargestellt, dass die 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), Rech-

nung 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 gegen-

über 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 Strafverfolgung 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 ge-

nannten 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 schweren 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.

- § 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).

- § 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.).

- 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 der gewerbs- oder bandenmäßigen Steuerhinterziehung nach § 370a AO soll in erster Linie die Bekämpfung 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.][1]

  - Die Einbeziehung des 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 Steuerhehlerei nach § 374 AO, deren Einbeziehung als Anlasstat eine notwendige Ergänzung darstellt, um der Nutzziehung aus Schmuggeldelikten und damit auch der Finanzierung organisierter Kriminalität den Boden zu entziehen.

- In Absatz 2 Nr. 3 bis 7 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 ohne inhaltliche Änderung übernommen worden.

- In Absatz 2 Nr. 8 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.

---

[1] Zur Erläuterung des Kursivdrucks: Im politischen Raum wird derzeit im Hinblick auf die Entscheidung des Bundesgerichtshofs vom 22. Juli 2004 (5 StR 85/04 - wistra 2004, S. 393 ff.) eine Modifizierung des § 370a AO erwogen. Inwieweit § 370a AO in § 100a Abs. 2 StPO-E einzubeziehen ist, wird auch vom Ergebnis dieser Beratungen abhängen.

- In Absatz 2 Nr. 9 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).

- *[In Absatz 2 Nr. 10 werden besonders schwere Fälle einer Straftat nach dem Arzneimittelgesetz neu aufgenommen. Durch die Einbeziehung des gewerbs- oder bandenmäßigen Inverkehrbringens von Dopingmitteln nach § 95 Abs. 3 Satz 2 Nr. 2 Buchstabe b AMG-E soll die Bekämpfung der gewerbs- und bandenmäßig organisierten unerlaubten Leistungssteigerung im Sport begegnet werden. Die Einbeziehung zielt auf ein effektives Vorgehen gegen den organisierten Handel mit Dopingmitteln.]*[1]

Zu § 100a Abs. 3 StPO-E

Die Vorschrift wird inhaltlich unverändert aus § 100a Satz 2 StPO übernommen. Die redaktionelle Umstellung von der Mehrzahl auf die Einzahl („eine Person“ statt „Personen“) dient lediglich der Angleichung an den sonst im Gesetz üblichen Sprachgebrauch.

---

[1] Zur Erläuterung des Kursivdrucks: Im politischen Raum wird derzeit folgende Erweiterung des § 95 Abs. 3 AMG erwogen:

„(3) In besonders schweren Fällen ist die Strafe Freiheitsstrafe von einem Jahr bis zu zehn Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

1. durch eine der in Absatz 1 bezeichneten Handlungen
   a) die Gesundheit einer großen Zahl von Menschen gefährdet,
   b) einen anderen in die Gefahr des Todes oder einer schweren Schädigung an Körper oder Gesundheit bringt oder
   c) aus grobem Eigennutz für sich oder einen anderen Vermögensvorteile großen Ausmaßes erlangt oder
2. in den Fällen des Absatzes 1 Nr. 2a Arzneimittel zu Dopingzwecken im Sport
   a) an Personen unter 18 Jahren abgibt oder bei diesen Personen anwendet oder
   b) in den Verkehr bringt und dabei gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung solcher Taten verbunden hat.“

Inwieweit zur Aufklärung der in Absatz 3 Satz 2 Nr. 2 Buchstabe b AMG-E genannten besonders schweren Fälle in Form einer banden- oder gewerbsmäßigen Begehung eine Telekommunikationsüberwachung nach § 100a StPO-E erforderlich ist, bedarf noch der rechtstatsächlichen Klärung durch eine Befragung der Praxis. Es wird daher gebeten, im Rahmen der Stellungnahmen zu diesem Entwurf auch auf diese Frage einzugehen. Dabei wird von besonderem Interesse sein, inwieweit sich in belastbarer Weise Hinweise dafür ergeben, dass der Einsatz der Telekommunikationsüberwachung (etwa im Hinblick auf abgeschottet und organisiert agierende Beteiligte) ein unverzichtbares Mittel zur Aufklärung schwerer Dopingstraftaten ist.

Zu § 100a Abs. 4 StPO-E

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, 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 jährlich bislang durchschnittlich etwa 30 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 Gesprächen, 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 Bundesver-

fassungsgericht hinweist (BVerfG 1 BvR 668/04, 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 durch eine Telekommunikationsüberwachung nicht in den Kernbereich privater Lebensgestaltung eingegriffen werden darf, 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 höchstpersönlicher Lebensgestaltung vorgesehen wird (so z. B. für den Bereich der Polizeigesetze: Sicherheits- 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 und auszuschließen, dass keine kernbereichsrelevanten 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 unabdingbar. 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. 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 allein – d. h. ausschließlich – Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erwarten lässt. Die Regelung ermöglicht damit auch weiterhin eine zur Verfolgung von schweren Straftaten notwendige effektive Durchführung von Telekommunikationsüberwachungsmaßnahmen.

Nach Absatz 4 Satz 2 dürfen Erkenntnisse aus dem Kernbereich privater Lebensgestaltung in Strafverfahren 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.

Mit dem Verwertungsverbot korrespondiert in Absatz 4 Satz 3 die Pflicht, durch einen Eingriff in den Kernbereich erlangte Erkenntnisse unverzüglich zu löschen.

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

Absatz 4 Satz 5 und 6 sind der Regelung in § 100c Abs. 10 StPO nachgebildet. Bei Zweifeln über das Vorliegen kernbereichsrelevanter Erkenntnisse hat die Staatsanwaltschaft eine Entscheidung des Gerichts über die Verwertbarkeit der Erkenntnisse herbeizuführen, die im Fall der Nichtverwertbarkeit für das weitere Verfahren bindend ist. Dies gewährleistet in problematischen Fällen eine Kontrolle durch eine unabhängige Instanz, entlastet damit zugleich die ermittelnden Personen von der Prüfung und Entscheidung mitunter schwieriger Abgrenzungsfragen und beugt zudem einer voreiligen Bejahung der Kernbereichsrelevanz vor, die aufgrund des Löschungsgebots nach Absatz 4 Satz 3 zu einem endgültigen Verlust beweiserheblicher Erkenntnisse führen kann. Zuständig ist dasjenige Gericht, das für die Anordnung der Maßnahme zuständig ist, im Ermittlungsverfahren also regelmäßig der Ermittlungsrichter, § 162 StPO.

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 der Ermittlungsrichter 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 erlassen (Eilanordnung).

Nach Satz 3 tritt die Eilanordnung der Staatsanwaltschaft – ebenfalls entsprechend dem geltenden Recht – außer Kraft, wenn sie nicht binnen drei Werktagen von dem Gericht bestätigt wird. Für die Fristberechnung gelten die allgemeinen Vorschriften der §§ 42 ff. StPO (vgl. eingehend zur Berechnung der Fristen im Rahmen des § 100b StPO: Günther, Kriminalistik 2006, 683 ff.). Neu ist in Satz 3 die Regelung, dass die aufgrund der Eilanordnung der Staatsanwaltschaft erlangten personenbezogenen Daten nicht zu Beweiszwecken verwertet werden dürfen, wenn die Eilanordnung mangels gerichtlicher Bestätigung nach drei Tagen außer Kraft tritt. Dies trägt dem Gedanken einer effektiven gerichtlichen Kontrolle Rechnung.

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 einen Monat 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. 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 er-

lassen 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.

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 Bundesgerichtshof 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 wurden hier – 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, aufgrund 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 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.

- 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 Konkretisierun-

gen, die auch die Art des technischen Zugriffs auf die zu überwachende Telekommunikation betreffen, wird erreicht, dass die Maßnahme zielgerichtet eingesetzt und der Richtervorbehalt im Sinne einer umfassenden Prüfung aller eingriffsrelevanten Aspekte ausgeübt wird.

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 Per-

sonen 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 der Ermittlungsmaßnahmen 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 den Richter und den nach § 100b Abs. 3 StPO verpflichteten Telekommunikations-

diensteanbieter 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 Richters von der Beendigung der Maßnahme dahingehend aus, dass dieser 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 keinerlei 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.

Aufgrund der damit verbundenen – und durch § 12 EGStPO-E (Artikel 6) abweichungsfest ausgestalteten – Verpflichtung der Länder, entsprechende Daten zu erheben und an das derzeit noch in der Errichtung befindliche Bundesamt für Justiz (vgl. dazu den Regierungsentwurf eines Gesetzes zur Errichtung und zur Regelung der Aufgaben des Bundesamtes für Justiz, BT-Drs. 16/1827) weiter zu leiten, unterliegt die Regelung nach Artikel 84 Abs. 1 Satz 5 und 6 GG der Zustimmung des Bundesrates. Das von Artikel 84 Abs. 1 Satz 5 GG gefor-

derte besondere Bedürfnis für eine bundeseinheitliche Regelung ist darin begründet, dass auf andere Weise eine aussagekräftige bundesweite Übersicht über die nach Absatz 6 zu erhebenden Daten nicht zu gewinnen ist. Eine solche Übersicht ist für den Bundesgesetzgeber indessen notwendig, um die Praxis der Telekommunikationsüberwachung zumindest anhand von Rahmendaten evaluieren und beobachten und so auf einer verlässlichen rechtstatsächlichen Grundlage beurteilen zu können, ob und inwieweit sich die Regelungen zur Telekommunikationsüberwachung bewähren oder der Überarbeitung durch den Gesetzgeber bedürfen (kritisch zu derartigen, die Praxis zusätzlich belastenden statistischen Berichtspflichten Löffelmann, ZStW 118 [2006], 358, 373 f.).

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 Beteiligten an der überwachten Telekommunikation. Die Angabe soll Erkenntnisse darüber erbringen, in welchem Ausmaß durch Telekommunikationsüberwachungsmaßnahmen Personen betroffen und damit Grundrechte beschränkt werden. Die Erhebung der Anzahl der Beteiligten wird in der Praxis voraussichtlich keinen übermäßigen zusätzlichen Aufwand verursachen. Denn grundsätzlich sind alle Beteiligten der überwachten Kommunikation schon aufgrund verfassungsrechtlicher Vorgaben von der Maßnahme (nachträglich) zu benachrichtigen. Soweit § 101 Abs. 4 ff. StPO-E hiervon – ggf. zeitlich begrenzte – Ausnahmen vorsieht, setzt dies eine Einzelfallprüfung hinsichtlich eines jeden Beteiligten voraus. Bei sorgfältiger Vornahme dieser Prüfung entsteht durch die zusätzliche Erfassung der Anzahl aller Beteiligten kein übermäßiger Aufwand.

- Die in den Nummern 5 und 6 vorgesehenen Angaben sollen im Rahmen dieses Entwurfs zunächst nur zur Diskussion gestellt werden. Es handelt sich um Angaben dazu, ob die Maßnahme Erkenntnisse erbracht hat, die für das weitere oder andere Strafverfahren relevant sind oder voraussichtlich relevant sein werden. Diese Angaben zielen auf eine Evaluierung, in welchem Ausmaß mit Telekommunikationsüberwachungsmaßnahmen – sowohl belastende oder auch entlastende – Ermittlungserfolge erzielt werden konnten, die mit Eingriffen in Grundrechte verbundenen Maßnahmen sich also insoweit „gelohnt“ haben. Problematisch an der Erfassung dieser Angaben erscheint indessen, dass sie eine umfassende Kenntnis und Würdigung des Sachstandes voraussetzen und dadurch ggf. einen nicht unerheblichen zusätzlichen Aufwand verursachen können. Hinzu kommt, dass es sich bei diesen Angaben letztlich stets um subjektive Einschätzungen handeln wird.

Zu Nummer 8 (§ 100c StPO-E)

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

- 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. Hierbei werden die durch das künftige Bundesamt für Justiz nach Satz 1 i. V. m. § 100b Abs. 5 StPO-E zu erstellenden Übersichten zugrunde zu legen sein.

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.

- 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 enthaltene Löschungspflicht wird durch die nun für alle verdeckten Ermittlungsmaßnahmen geltende Vorschrift des § 101 StPO-E ersetzt, 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 modifizierter und übersichtlicherer Weise im neuen Absatz 2 Satz 2.

- Der bisherige Absatz 4 findet sich im neuen Absatz 3.

- 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, 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. § 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. 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.

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 engen vorgesehenen 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 würde 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 könnten, wenn dieses aktuell nicht genutzt wird. Eine solche die Strafverfolgung erleichternde Möglichkeit soll aus rechtspolitischen Gründen jedoch nur bei schweren Straftaten im Sinne des § 100a Abs. 2 StPO-E eröffnet werden. Dies wird durch § 100g Abs. 1 Satz 3 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 subsumie-

ren – wird sprachlich dahingehend präzisiert, dass die Straftat „mittels Telekommunikation“ begangenen sein muss (Absatz 1 Satz 1 Nr. 2). Ferner bedarf 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, §§ 110a, 110b TKG-E) verhältnismäßigen Befugnisnorm der 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 durch die lediglich andere Straftaten vorbereitet werden sollen, 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 – unter den dortigen Voraussetzungen – 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 die Ermittlung des Sachverhalts auf andere Weise ausgeschlossen ist. Es bedarf daher künftig einer Einzelfallprüfung, ob etwaige alternative Ermittlungsmaßnahmen zu schwereren Eingriffen führen würden und damit 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 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 Ausgestaltung der Erhebungsbefugnis in § 100g Abs. 1 StPO-E steht 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 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 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. Ferner trägt die in besonderer Weise am Verhältnismäßigkeitsgrundsatz orientierte Ausgestaltung der Erhebungsbefugnisse nach § 100g Abs. 1 StPO-E den Anforderungen des Artikels 4 der Richtlinie Rechnung und steht auch nicht in Widerspruch zu den Vorgaben des Übereinkommens über Computerkriminalität; denn eine am Verhältnismäßigkeitsgrundsatz 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 aufgrund der zugleich umzusetzenden Richtlinie zur „Vorratsdatenspeicherung“ entbehrlich geworden: Die Daten, die aufgrund einer solchen Speicherungsanordnung „einzufrieren“ wären, werden künftig bereits aufgrund

der in den §§ 110a, 110b TKG-E (Artikel 2 dieses Gesetzes) vorgesehenen Speicherungsfristen aufbewahrt.

Würde allerdings, wie dies in der rechtspolitischen Diskussion zum Teil erwogen wird, was der Entwurf aber u. a. 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 einem 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 Diensteanbie-

tern 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, § 110a 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 gedeckt durch die allgemeine Erhebungsbefugnis nach § 100g Abs. 1 StPO-E, die auch die Anordnung einer Zielwahlsuche erlaubt. 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:

- 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).

- 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 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 StPO in § 100h Abs. 1 Satz 3 Halbsatz 2 StPO (Beendigung der Maßnahme bei Wegfall der Anordnungsvoraussetzungen).

§ 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. 3 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 Sicherstellung von Gegenständen (z. B. elektronische Datenträger, aber auch Verbindungsnachweise in Papierform), die Aufschluss über Verkehrsdaten geben können und sich nicht im Gewahrsam des Diensteanbieters befinden, nach den allgemeinen Vorschriften, also insbesondere nach den §§ 94 ff. StPO richtet und § 100g Abs. 1 und 2 StPO-E insoweit nicht anzuwenden ist. Mit dieser Klarstellung wird die durch den Kammerbeschluss des Bundesverfassungsgerichts 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, Urteil vom 2. März 2006, 2 BvR 2099/04, NJW 2006, 976, 978).

Zu § 100g Abs. 4 StPO-E

In § 100g Abs. 4 StPO-E sind in Umsetzung von Artikel 10 der Richtlinie zur „Vorratsdatenspeicherung“ 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 Erläuterungen zu § 100g Abs. 1 Satz 2 StPO-E):

- § 100h Abs. 1 Satz 1 StPO wird ersetzt durch den Verweis auf § 100b Abs. 2 in § 100g Abs. 3 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.

- § 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 StPO mit enthaltenen Bestimmungen zum Einsatz technischer Mittel, soweit sich diese auf Bildaufnahmen und Observationsmittel beziehen:

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

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

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

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

- § 100h Abs. 4 StPO-E entspricht inhaltlich dem bisherigen § 100f Abs. 4 StPO und übernimmt 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 sogenannten „IMSI[1]-Catcher“-Einsatz wird - mit Ausnahme des in Absatz 6 neu angefügten Satzes 2 - lediglich redaktionell überarbeitet, ohne damit wesentliche, über notwendige Folgeänderungen hinausgehende inhaltliche Änderungen zu verbinden:

- Der bisherige Absatz 1 bleibt inhaltlich unverändert erhalten, erfährt aber eine sprachliche Vereinfachung dadurch, dass in Nummer 2 einheitlich der Begriff „Festnahme“ verwendet wird.

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

- Der bisherige Absatz 2 Satz 2 findet sich im neuen Absatz 3 Satz 1, wobei der bisherige Verweis auf § 100f Abs. 3 Satz 2 StPO zur besseren Verständlichkeit der Regelung durch eine Ausformulierung ersetzt wird. Dies berücksichtigt auch Stellungnahmen aus der Pra-

[1] IMSI = International Mobile Subscriber Identity.

xis, die die Lesbarkeit der Vorschrift bemängelten (vgl. Albrecht, Dorsch und Krüpe, a. a. O., S. 204).

- Der bisherige Absatz 2 Satz 3 entfällt. Die dort ausdrücklich erwähnte Zulässigkeit der Maßnahme zur Eigensicherung der mit der Festnahme betrauten Beamten des Polizeidienstes ergibt sich bereits aus Absatz 1 Nr. 2, da die Maßnahme auch in diesen Fällen „zur Festnahme“ erfolgt, es mithin der besonderen Erwähnung des Falles der Eigensicherung nicht bedarf.

- Der bisherige Absatz 3 wird im neuen Absatz 4 unverändert übernommen.

- Der bisherige Absatz 4 Satz 1 bis 3 wird inhaltlich in den neuen Absatz 5 übernommen und redaktionell angepasst.

- Der bisherige Absatz 4 Satz 4 wird inhaltlich in den neuen Absatz 6 Satz 1 übernommen.

- Der in Absatz 6 neu angefügte Satz 2 stellt entsprechend der Regelung in § 100b Abs. 3 Satz 3 StPO-E durch einen Verweis auf § 95 Abs. 2 StPO klar, dass die in Satz 1 enthaltene Mitteilungspflicht der Diensteerbringer ordnungsgeld- und zwangsmittelbewehrt ist. Eine ausdrückliche Regelung hierzu fehlt bislang in § 100i StPO, so dass sich die Praxis insoweit bislang mit einer analogen Anwendung des § 95 Abs. 2 StPO behilft (vgl. Nack, a. a. O., § 100i, Rn. 12). Der neu angefügte Satz 2 beseitigt die sich hieraus ergebende Unsicherheit.

Ferner wird § 100i StPO-E 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 DNS-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):

- 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 DNS-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 DNS-Abgleichs bekannt, wird das Untersuchungsergebnis der Person oh-

nehin 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; im Zusammenspiel mit der Aufzählung in Satz 3 ergibt sich, wer bei den einzelnen Maßnahmen Adressat der Benachrichtigung ist.

Soweit die zu benachrichtigen Personen allerdings nicht bekannt sind, kann deren Ermittlung mit weiteren Eingriffen oder aber mit einem erheblichen, im Einzelfall ggf. unangemessenen Aufwand (z. B. Feststellung der Betroffenen im Ausland im Wege der Rechtshilfe) verbunden und daher unverhältnismäßig sein. In diesen Fällen ist, wie Satz 1 ausdrücklich bestimmt, ein Absehen von der Benachrichtigung möglich. Dasselbe gilt nach Satz 1, wenn durch die Benachrichtigung überwiegende schutzwürdige Interessen anderer Betroffener (z. B. des Nachrichtenmittlers, wenn zufällig dessen Gespräch mit einem unbeteiligten Geschäftspartner erfasst wurde) der Benachrichtigung entgegenstehen.

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, nimmt den Fürsorgedanken des § 35a StPO auf und gestaltet die Rechtsschutzmöglichkeiten der Betroffenen damit effektiv aus.

Satz 3 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 3 entgegengewirkt werden.

- Die bislang in § 101 Abs. 1 StPO vorgesehene Benachrichtigungspflicht bei Maßnahmen nach § 81e StPO (DNS-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) unverändert übernommen worden.

- Bei der akustischen Überwachung mit technischen Mitteln außerhalb von Wohnungen nach § 100f StPO-E sind die Zielperson – also diejenige, die mittels der akustischen Ü-

berwachung 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 1 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 Benachrichtigung 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.

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 ausgeführt, 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 (sogenannter „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 zum einen eine ordnungsgemäße Handhabung der Benachrichtigungsregelungen und dient zum anderen dazu, dies später auch 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 Benach-

richtigung 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 der Ermittlungsrichter des Amtsgerichts 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 stellt klar, dass gegen die in Absatz 1 aufgeführten, regelmäßig in nicht unerheblicher Weise eingriffsintensiven verdeckten Ermittlungsmaßnahmen nachträglicher Rechtsschutz zu gewähren ist. Regelungstechnisch ist die Vorschrift § 100d Abs. 10 StPO nachgebildet (vgl. BT-Drs. 15/4533, S. 19), der aufgrund der allgemeinen Regelung des Absatzes 9 gestrichen wird.

Die 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. 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 erheblich 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 3 bei der Bestimmung der dem Grunde nach zu benachrichtigenden Personen gerade dem Gesichtspunkt einer erheblichen 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 3 genannten Personenkreis an.

Satz 1 stellt daher klar, dass die in Absatz 4 Satz 3 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 jeder Beteiligte der überwachten Telekommunikation nach Absatz 4 Satz 3 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 Worte „bis zu“ zum Ausdruck gebracht wird.

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 der Ermittlungsrichter des Amtsgerichts 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 trifft für den Fall, dass im Zeitpunkt des Antrags auf nachträglichen Rechtsschutz bereits Anklage erhoben und der Angeklagte benachrichtigt worden ist, aus Gründen der Zweckmäßigkeit und Effizienz eine Sonderregelung zur gerichtlichen Zuständigkeit dahingehend, dass über solche Anträge das mit der Sache befasste Gericht befindet. Erwogen wurde, die Zuständigkeitsregelung in Satz 3 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 letztlich nicht ratsam.

Satz 4 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. 5 StPO-E). Die Möglichkeit der Erlangung nachträglichen Rechtsschutzes ist eine unabdingbare Voraussetzung für die rechtsstaatliche Ausgestaltung verdeckter Ermittlungsmaßnahmen.

Satz 5 eröffnet dem nach Satz 3 zuständigen Hauptsachegericht die Möglichkeit, über den Antrag des Angeklagten auf nachträglichen Rechtsschutz auch in der das Verfahren abschließenden Entscheidung (z. B. dem Urteil) zu befinden. Anders als nach dem bisherigen § 100d Abs. 10 Satz 4 StPO ist das Hauptsachegericht damit nicht mehr gehalten, seine Entscheidung über ein nachträgliches Rechtsschutzbegehren stets in der das Verfahren abschließenden Entscheidung zu treffen. Entscheidet das Hauptsachegericht über den Antrag

auf nachträglichen Rechtsschutz durch Beschluss außerhalb der das Verfahren abschließenden Entscheidung, so bleibt damit auch die – insbesondere bei problematischen Fallgestaltungen sinnvoll erscheinende – Möglichkeit der sofortigen Beschwerde nach Satz 3 erhalten.

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 aller-

dings 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 – 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 zugangsberechtigt 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 diese Vorschrift hingegen der heimliche Online-Zugriff auf zugangsgeschützte Datenbestände im Sinne eines so genannten „staatlichen Hackings“. Der Online-Zugriff auf öffentlich zugängliche Datenbestände, die keiner besonderen Zugangsberechtigung bedürfen, erfordert hingegen keine besondere Ermächtigungsgrundlage.

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 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 (Satz 1). Durch diese praktisch bedeutsame Regelung wird die Bestimmung der ermittlungsrichterlichen 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 richterlichen Bereitschaftsdienstes (vgl. BVerfGE 100, 313, 401; 103, 142, 152; 105, 239, 248; 109, 279, 358; BVerfGK 2, 176, 179) besser sichergestellt werden, der bei Gerichten in kleineren Amtsgerichtsbezirken aufgrund der dort typischerweise gegebenen Personalsituation mit zumutbarem Aufwand oftmals nicht gewährleistet werden kann. Durch die Konzentration der ermittlungsrichterlichen 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 richterliche 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).

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 Absatz 3

Um einen effektiven vorbeugenden Rechtsschutz der von einer längerfristige Observation nach § 163f StPO Betroffenen zu gewährleisten, wird die Anordnung einer solchen Maßnahme 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.

Zu Absatz 4

Die in Satz 1 enthaltene Verpflichtung der Staatsanwaltschaft oder ihrer Ermittlungspersonen, die Anordnung unter Angabe der maßgeblichen Gründe aktenkundig zu machen, entfällt als Folgeänderung zu Absatz 3 (Richtervorbehalt), weil für gerichtliche Anordnungen die Begründungspflicht aus § 34 StPO gilt. Der neue Satz 1 gibt daher – entsprechend dem bisherigen Recht – nur noch vor, dass die Anordnung der längerfristigen Observation auf einen Monat zu befristen ist.

Die bisher in Satz 2 bestimmte Anforderung, dass eine Verlängerung der Maßnahme nur durch den Richter getroffen werden kann, bedarf es nicht mehr, da dies nunmehr bereits aus dem in Absatz 3 enthaltenen Richtervorbehalt folgt. Der neu gefasste Satz stellt nunmehr klar, dass eine Verlängerungen der Anordnung um jeweils maximal einen Monat zulässig sind, wenn die Anordnungsvoraussetzungen unter Berücksichtigung der zwischenzeitlich gewonnenen Ermittlungsergebnisse fortbestehen.

Zu Nummer 19 (§ 304 StPO-E)

Der an § 304 Abs. 5 neu angefügte Satz 5 stellt klar, dass im Falle des nachträglichen Rechtsschutzes nach § 101 Abs. 9 StPO-E die dort in Satz 3 eröffnete sofortige Beschwerde auch gegen Entscheidungen des Ermittlungsrichters beim Bundesgerichtshof oder beim Oberlandesgericht statthaft 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 die Verwendung von personenbezogenen Daten, die aus Maßnahmen erlangt worden sind, welche nur bei Verdacht bestimmter Straftaten zulässig sind. Im Einzelnen:

Der bisherige Satz 1 wird unverändert übernommen.

Als Satz 2 wird eine Regelung 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 Satz 3 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 die Verwendung der 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 Maß-

nahmen 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.

In Satz 4 wird zum einen klargestellt, dass Auskünfte nach § 406e StPO von den Verwendungsbeschränkungen nicht berührt werden. Diese Klarstellung ist aus Gründen des Opferschutzes notwendig. Ferner wird durch die Bezugnahme auf § 100d Abs. 5 StPO-E klargestellt, 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.

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 (§ 96 TKG-E)

Die Vorgaben der Richtlinie 2006/24/EG werden im Bereich des TKG in Bezug auf die Speicherung und Verwendung von Verkehrsdaten durch die neu einzufügenden Vorschriften der §§ 110a, 110b TKG-E umgesetzt. Die Aufzählung der zulässigen Verwendungszwecke für gespeicherte Verkehrsdaten in § 96 Abs. 2 TKG-E ist durch einen Verweis auf die vorgenannten Vorschriften anzupassen.

Zu Nummer 2 (§ 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 Spei-

cherungsdauer werden in § 110a TKG-E festgelegt. § 97 Abs. 3 Satz 2 Halbsatz 1 TKG-E stellt klar, dass Verkehrsdaten, die nicht von der Speicherungspflicht des § 110a TKG-E erfasst sind, weiterhin grundsätzlich unverzüglich zu löschen sind. Die bisherigen Sätze 2 und 3 in Absatz 3 werden aus sprachlichen Gründen zusammengefasst. Der Verweis in Absatz 3 Satz 3 ist daher entsprechend anzupassen.

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 § 110a Abs. 2 Nr. 1 TKG-E widersprechen, nach der Rufnummern 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 wird systematisch richtig in § 99 Abs. 1 Satz 7 TKG-E eingestellt und ist 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 3 (§ 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, und dass ihm, wenn er eine Entscheidung nicht trifft, die Rufnummern ungekürzt mitgeteilt werden. Eine Beschränkung auf die Mitteilung gekürzter Rufnummer 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.

Bei den geänderten Verweisungen in Absatz 1 Satz 5 und 8 handelt es sich um redaktionelle Folgeanpassungen an die vorgenannten Änderungen.

Zu Buchstabe b (Absatz 3)

Es handelt sich um Folgeänderungen zu den Änderungen in Absatz 1.

Zu Nummer 4 (§ 110 Abs. 8 TKG-E)

§ 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 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 5 (§§ 110a, 110b TKG-E)

Zu § 110a TKG-E

§ 110a TKG-E dient als Kernregelung der Umsetzung der Artikel 3, 5 und 6 der Richtlinie 2006/24/EG, indem sie die Adressaten sowie die Grundvoraussetzungen der Speicherungspflichten bestimmt und die zu speichernden Datenarten sowie die Speicherungsdauer festlegt. 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 Systemstruk-

turen 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 Telekommunikationsdienste für die Öffentlichkeit erbringen oder an der Erbringung solcher Dienste mitwirken. 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 die Speicherungspflichten auch dann bestehen, wenn für die Erbringung der Telekommunikationsdienste oder für die Mitwirkung daran keine eigenen Telekommunikationsanlagen genutzt, sondern solche anderer Anbieter in Anspruch genommen werden. Auch in diesem Fall hat der Anbieter des Telekommunikationsdienstes die Speicherung der in dieser Vorschrift im Einzelnen aufgeführten Daten sicherzustellen, wobei ihm die Entscheidung überlassen bleibt, ob er die Daten selbst speichert oder durch den Betreiber der von ihm genutzten Telekommunikationsanlage speichern lässt. Auf welche Weise ein solcher Anbieter die Erfüllung der Speicherungspflichten sicherstellt, hat er gegenüber der Bundesnetzagentur nachzuweisen.

Einen Telekommunikationsdienst für die Öffentlichkeit im Sinne dieser Vorschrift erbringt auch, wer einen Anonymisierungsdienst betreibt und hierbei die Ausgangskennung des Telekommunikationsnutzers durch eine andere ersetzt.

Satz 1 bestimmt zudem, dass die betroffenen Diensteanbieter die in § 110a TKG-E genannten Daten nur dann zu speichern haben, wenn diese von ihnen gerade bei der Nutzung des von ihnen bereitgestellten Telekommunikationsdienstes erzeugt oder verarbeitet werden. Diese – gleichsam „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 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, nicht zur Speicherung der von anderen Diensteanbietern über die bereitgestellten Übertragungswege übermittelten Daten verpflichtet sind.

Satz 1 legt überdies die Speicherungsdauer fest. Die in § 110a TKG-E im Einzelnen aufgeführten Daten sind danach für die Dauer von sechs Monaten ab ihrer Entstehung zu speichern. Dies entspricht der nach Artikel 6 der Richtlinie 2006/24/EG zulässigen 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.

Schließlich bestimmt Satz 1 den Zweck der Speicherung, nämlich die Sicherstellung der Verfügbarkeit der in die Kategorien der Absätze 2 bis 4 fallenden Daten für die Zwecke der Strafverfolgung. Hieraus folgt zugleich, dass eine Verwendung der nach Maßgabe dieser Vorschrift gespeicherten Daten für die Zwecke der Strafverfolgung zulässig ist. Ergänzende Verwendungsregelungen enthält § 110b TKG-E. Um sicher zu stellen, dass die Daten auch unverzüglich den berechtigten Stellen zur Verfügung gestellt werden können, bestimmt Satz 1 zudem, dass die Daten im Inland zu speichern sind.

Zu Absatz 2

Absatz 2 regelt die einzelnen Speicherungspflichten für Anbieter öffentlicher Telefondienste und umfasst die Bereiche der Festnetz-, Mobilfunk- und Internettelefonie. Die Kenntnis dieser Daten ist für Strafverfolgungsbehörden unverzichtbar, um zurückliegende Telekommuni-

kationsvorgänge zuverlässig nachvollziehen zu können. Besonders hinzuweisen ist auf folgende Regelungen:

- Nummer 3 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. Nach Buchstabe a sind die Kennungen der verwendeten Mobilfunkkarten des anrufenden und des angerufenen Anschlusses zu speichern (so genannte IMSI). Nach Buchstabe b sind die Kennungen der anrufenden und der angerufenen Endgeräte zu speichern (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, in denen sich die Telekommunikationsteilnehmer beim Verbindungsaufbau befinden. Nach Buchstabe d sind der Zeitpunkt der Aktivierung einer im Voraus bezahlten Guthabenkarte (so genannte Prepaidkarte) sowie die Angabe der Funkzelle zu speichern, in der sich das Mobiltelefon bei Aktivierung der Guthabenkarte befindet. Diese Daten werden bei dem derzeit üblichen Verfahren zur Aktivierung einer Prepaidkarte mittels Anrufs beim Telekommunikationsdiensteanbieter bereits durch die Nummern 1, 2 und 4 Buchstabe a bis c erfasst, so dass auf der Grundlage der derzeitigen Aktivierungsverfahren Buchstabe d zu keiner zusätzlichen Datenspeicherung führt. Die Aufnahme von Buchstabe d ist gleichwohl geboten, um bei etwaigen Änderungen der derzeitigen Aktivierungsverfahren weiterhin den Vorgaben der Richtlinie zu entsprechen.

- Nummer 5 regelt für den Bereich der Internettelefonie die besondere Pflicht zur Speicherung der Internetprotokolladressen 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 regelt die einzelnen Speicherungspflichten für Anbieter öffentlicher E-Mail-Dienste. Diese Daten sind für eine Rückverfolgbarkeit einer erfolgten Telekommunikation mittels E-Mail unverzichtbar. Die Speicherung der Benutzerkennung (etwa der IP-Adresse) des Absenders einer E-Mail ist erforderlich, weil dieser seine E-Mail-Adresse selbst ohne größeren

Aufwand oder besondere technische Kenntnisse ändern kann und manche Betreiber Server einsetzen, die die Richtigkeit der Absenderangaben nicht überprüfen, wodurch die Rückverfolgbarkeit von E-Mails erheblich erschwert wird.

Zu Absatz 4

Absatz 4 regelt die einzelnen Speicherungspflichten für Anbieter von Internetzugängen. Die Verfügbarkeit dieser Daten 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 § 110a Abs. 4 TKG-E. 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 § 110a TKG-E nicht verpflichtet. Keinesfalls besteht eine Speicherungspflicht in den Fällen, in denen schon der Verbindungsaufbau scheitert.

Zu Absatz 6

Absatz 6 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 dient der Ermöglichung einer genaueren Ermittlung des Standorts, von dem aus oder zu dem eine Telekommunikationsverbindung aufgebaut wurde.

Zu Absatz 7

Absatz 7 stellt klar, dass Daten, die Aufschluss über den Kommunikationsinhalt geben, nach dieser Vorschrift nicht gespeichert werden dürfen. Dies erlangt insbesondere 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 § 110a TKG-E nicht gespeichert werden.

Zu Absatz 8

Mit der Regelung in Absatz 8 soll sichergestellt werden, 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 § 110b TKG-E

Die Vorschrift regelt die Verwendung der nach Maßgabe von § 110a TKG-E gespeicherten Verkehrsdaten. Im Einzelnen:

Zu Absatz 1

Absatz 1 Satz 1 enthält die Verpflichtung des Telekommunikationsdiensteanbieters, die nach § 110a TKG-E gespeicherten Daten unverzüglich den für die Strafverfolgung zuständigen Stellen für die Zwecke der Strafverfolgung zu übermitteln, wenn diese Stellen die Übermittlung anordnen. Ob die Strafverfolgungsbehörden ein solches Verlangen an den Telekommunikationsdiensteanbieter richten dürfen, ist nicht Regelungsgegenstand von Absatz 1, sondern bestimmt sich nach den für die Strafverfolgungsbehörden geltenden Vorschriften und damit nach der Strafprozessordnung (§ 100g i. V. m. § 100b StPO-E). Ob die Voraussetzun-

gen für ein Übermittlungsverlangen vorliegen, haben die für die Strafverfolgung zuständigen Stellen in eigener Verantwortung zu prüfen. Dem Telekommunikationsdiensteanbieter kommt insoweit weder eine inhaltliche Prüfungspflicht noch -befugnis zu. Der Telekommunikationsdiensteanbieter hat sich allerdings zu vergewissern, ob es sich bei dem die Übermittlung Verlangenden um eine für die Strafverfolgung zuständige Stelle handelt, die zur Ausübung des Übermittlungsverlangens legitimiert ist. Soweit das Verlangen auf die Übermittlung von § 100g Abs. 1 StPO-E i. V. m. § 96 TKG unterfallenden Verkehrsdaten - und nicht etwa nur auf Angaben zur geographischen Lage von Funkzellen (vgl. § 110a Abs. 6 TKG-E) - gerichtet ist, muss die zuständige Stelle sich durch eine gerichtliche oder staatsanwaltschaftliche (Eil-)Anordnung legitimeren können, vgl. § 100g Abs. 2 Satz 1 i. V. m. § 100b Abs. 1 StPO-E. § 110b Abs. 1 TKG-E ist damit der Regelung des § 113 TKG nachgebildet, die ebenfalls eine Verpflichtung des Telekommunikationsdiensteanbieters zur Auskunftserteilung u. a. an die Strafverfolgungsbehörden enthält, nicht aber eine Erhebungsbefugnis dieser Stellen begründet.

Nach Absatz 1 Satz 2 ist die Regelung des § 113 Abs. 1 Satz 4 TKG entsprechend anzuwenden. Dies bedeutet, dass der zur Auskunft Verpflichtete gegenüber seinen Kundinnen und Kunden sowie gegenüber Dritten Stillschweigen über die Auskunftserteilung zu wahren hat, und dient mithin dazu, dass verdeckt geführte Ermittlungen nicht vorzeitig bekannt werden.

Eine Übermittlung der allein aufgrund des § 110a TKG-E gespeicherten Daten für andere Zwecke als zur Verfolgung von Straftaten ist in Absatz 1 Satz 1 nicht vorgesehen und damit nicht zulässig. Dies stellt Absatz 1 Satz 3 ausdrücklich klar. Ausgeschlossen ist damit insbesondere eine Übermittlung der allein auf der Grundlage des § 110a TKG-E gespeicherten Daten für Zwecke der Gefahrenabwehr, der Aufgabenerfüllung der Dienste oder auch zur Erfüllung zivilrechtlicher Auskunftsansprüche. Diese eng begrenzte Übermittlungsregelung in Absatz 1 ist nicht durch die Richtlinie 2006/24/EG vorgegeben (s. o., S. 62), sondern entspricht dem hierauf gerichteten rechtspolitischen Willen.

Absatz 1 Satz 4 enthält eine Verwendungsbeschränkung im Hinblick auf unternehmensinterne Zwecke des nach § 110a TKG-E zur Speicherung Verpflichteten: Der Verpflichtete darf die allein aufgrund der Speicherverpflichtung nach § 110a TKG-E gespeicherten Daten außer zur Übermittlung für die in Satz 1 bestimmten Zwecke nur verwenden für Zwecke der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes der Datenverarbeitungsanlage.

Zu Absatz 2

Absatz 2 bestimmt, dass die nach § 110a 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 Absatz 3

Absatz 3 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 Nummer 6 (§ 111 TKG-E)

Zu Buchstabe a (Absatz 1)

Die Untergliederung des Satzes 1 in die Nummern 1 bis 6 in Satz 1 dient der besseren Übersichtlichkeit; dabei entsprechen die Nummern 1 bis 4 und 6 der bisherigen Rechtslage, lediglich 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 den Kunden überlassenen Mobilfunkgeräte (IMEI) zu erfassen und zu speichern, um Auskünfte an die nach den §§ 112 und 113 TKG berechtigten Stellen erteilen zu können. Diese Informationen sind in den Fällen unverzichtbar, in denen die Täter 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 Artikel 5 der Richtlinie 2006/24/EG und schreibt die Erhebung von Kundendaten auch für den Bereich so genannter E-Mail-Konten vor.

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 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 7 (§ 112 TKG-E)

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. Die Änderung in Absatz 1 Satz 4 Nr. 2 dient der Richtigstellung eines redaktionellen Versehens, da die Möglichkeit einer Suche mittels einer Ähnlichenfunktion sichergestellt sein soll. Die bisherige Fassung war in der Literatur bereits „berichtigend“ verstanden worden (vgl. Klesczewski, a. a. O., § 112, Rn. 11).

Zu Nummer 8 (§ 115 Abs. 2 TKG-E)

Die Einfügung der §§ 110a, 110b TKG-E in Absatz 2 Satz 1 dient der Sicherstellung der Erfüllung der Speicherungspflichten. Die weiteren Änderungen stellen redaktionelle Folgeanpassungen an die Änderungen in § 111 TKG-E dar.

Zu Nummer 9 (§ 149 TKG-E)

Zu Buchstabe a (Absatz 1)

Die Ergänzung der Ordnungswidrigkeitentatbestände in Absatz 1 um die Nummern 28a bis 28f und 30a 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.

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 10 (§ 150 TKG-E)

Der neu einzufügende Absatz 11a macht Gebrauch von der bei Annahme der Richtlinie 2006/24/EG vorbehaltene Option einer verlängerten Umsetzungsfrist nach Artikel 15 Abs. 3 der Richtlinie für den Bereich des Internets. Die Inanspruchnahme dieser Möglichkeit erscheint im Hinblick auf die zur Erfüllung der Speicherung erforderlichen Umsetzungsmaßnahmen in den betroffenen Unternehmen angemessen. Durch die Bestimmung, dass die Speicherungspflichten in diesem Bereich bis spätestens zum 15. März 2009 zu erfüllen sind, wird zugleich klargestellt, dass die Unternehmen die Speicherungsvorgaben auch vorher umsetzen dürfen, etwa im Rahmen einer allfälligen Anpassung ihrer technischen Einrichtungen.

Zu Artikel 3 (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 4 (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 10 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 StPO-E auch die Kennzeichnungspflicht 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 5 (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 6 (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 7 (Änderung des Einführungsgesetzes zur Strafprozessordnung)

Zu § 12 EGStPO-E

§ 12 gestaltet die statistischen Berichtspflichten der Länder nach § 100b Abs. 5 und 6, § 100e und § 100g Abs. 4 StPO-E abweichungsfest aus (Artikel 84 Abs. 1 Satz 5 und 6 GG). Das hierfür erforderliche besondere Bedürfnis nach einer bundeseinheitlichen Regelung liegt vor: Ohne die Erhebung und Übermittlung der dort genannten statistischen Daten lässt sich die Entwicklung und das Ausmaß der mit erheblichen Grundrechtseingriffen verbundenen Maßnahmen in der Praxis nicht verlässlich beobachten. Eine solche Beobachtung im Sinne einer laufenden Evaluierung ist jedoch erforderlich, damit der Gesetzgeber auf der einer belastbaren Grundlage prüfen, beurteilen und entscheiden kann, ob sich Änderungen der maßgeblichen gesetzlichen Regelungen empfehlen.

Zudem begründet Artikel 10 der Richtlinie 2006/24/EG die Verpflichtung der Mitgliedstaaten, jährlich eine Statistik mit den in Artikel 10 im Einzelnen beschriebenen Angaben an die Kommission zu übermitteln. Diese Verpflichtung Deutschlands bedingt, dass die nach § 100g Abs. 4 StPO-E zu erhebenden Daten einheitlich durch die Länder gemeldet werden müssen, so dass es auch von daher zwingend ist, die entsprechenden Verfahrensregelungen zur Übermittlung abweichungsfest zu gestalten.

Zu § 13 EGStPO-E

§ 13 EGStPO-E trifft Übergangsregelungen für die Statistikpflichten, die vom Telekommunikationsgesetz (§ 110 Abs. 8 TKG) und von der Telekommunikations-Überwachungsverord-

nung (§ 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. Die schon bestehende Statistikregelung in § 100e StPO(-E) bleibt von dieser Übergangsregelung unberührt.

Zu Artikel 8 (Änderung des IStGH-Gesetzes)

Die in der Vorschrift enthaltenen Verweisungen auf § 100a Abs. 1 Satz 1, § 101 Abs. 1, § 100b Abs. 5 und Abs. 6 StPO werden redaktionell an die Neufassung der §§ 100a, 100b, 477 Abs. 2 StPO-E angepasst. Ferner wird das in Absatz 1 Nr. 3 enthaltene Wort „Informationen“ durch die Worte „personenbezogene Daten“ ersetzt und damit an die Begriffe der Strafprozessordnung angeglichen.

Zu Artikel 9 (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 geringeren Eingriffsintensität der in § 16b Abs. 1 Satz 3 WpHG vorgesehene Maßnahme (lediglich Speicherungsanordnung, aber keine Zugriffsregelung) auch künftig nicht geboten erscheint.

Zu Artikel 10 (Änderung des Gesetzes über die Anwendung unmittelbaren Zwanges und die Ausübung besonderer Befugnisse durch Soldaten der Bundeswehr und verbündeter Streitkräfte sowie zivile Wachpersonen – UZwGBw)

§ 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 11 (Änderung des Zollfahndungsdienstgesetzes)

Zu Nummer 1 (§ 22 ZFdG)

Die Änderung trägt dem Umstand Rechnung, dass die Verwendung personenbezogener Information, die durch den Einsatz technischer Mittel zur Eigensicherung nach § 22 ZFdG erlangt wurden, sich nicht allein nach der bislang dort in Absatz 2 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 Nummer 2 (§ 32 ZFdG)

Die Begründung zur Änderung des § 22 ZFdG gilt entsprechend.

Zu Artikel 12 (Änderung der Telekommunikations-Überwachungsverordnung)

Zu Nummern 1, 3 und 4 (§§ 1 und 25 TKÜV sowie Anlage zu § 25 TKÜV)

Die auf die Erstellung der Statistik nach § 110 Abs. 8 TKG bezogenen Regelungen in § 1 Nr. 8, § 25 TKÜV und in der Anlage zu § 25 TKÜV werden in Folge der Aufhebung des § 110 Abs. 8 TKG ebenfalls aufgehoben. Entsprechende statistische Erhebungen werden künftig nach Maßgabe des § 100a Abs. 5 und 6 StPO-E erfolgen. Zu den jeweiligen Übergangsregelungen vgl. Artikel 14 Abs. 2 und 4.

Zu Nummer 2 (§ 3 TKÜV)

§ 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 nicht unerheblichen Aufwendungen befreit werden, die für die Vorhaltung der technischen Einrichtungen und das Treffen der organisatorischen Vorkehrungen für die Umsetzung angeordne-

ter Überwachungsmaßnahmen anfallen. Da man bei der Erstellung der TKÜV 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 angeschlossen sind. Mittlerweile liegen Auswertungen der Bundesnetzagentur (BNetzA) über die Verteilung von Überwachungsmaßnahmen auf Unternehmen unterschiedlicher Größen vor. Daraus geht hervor, dass Netzbetreiber, deren Telekommunikationsanlage nur wenig größer ist als der durch die Verordnung festgelegte Grenzwert nur etwa alle elf Jahre mit der Umsetzung einer Überwachungsmaßnahme rechnen müssen. In Anbetracht dieser sehr seltenen Inanspruchnahme 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 Teilnehmer auf künftig 20.000 Teilnehmer anhebt, was dazu führt, dass Unternehmen von den Vorhalteverpflichtungen befreit werden, die seltener als durchschnittlich einmal in drei Jahren in Anspruch genommen werden.

Über die auf Erfahrungswerten der herkömmlichen Sprachtelefonie beruhenden Erkenntnisse hinaus hat die BNetzA 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.

Zu Artikel 13 (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 14 (Zitiergebot)

Mit der Vorschrift wird dem Zitiergebot des Artikels 19 Abs. 1 Satz 2 GG entsprochen.

Zu Artikel 15 (Inkrafttreten)

Die Vorschrift regelt das Inkrafttreten.