Referentenentwurf

des Bundesministeriums der Justiz und für Verbraucherschutz

Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten

A. Problem und Ziel

Bei der Aufklärung schwerer Straftaten und bei der Gefahrenabwehr sind Verkehrsdaten ein wichtiges Hilfsmittel für die staatlichen Behörden. Unter Verkehrsdaten im Sinne des § 96 des Telekommunikationsgesetzes (TKG) versteht man die Daten, die bei einer Telekommunikation anfallen, also zum Beispiel die Rufnummer der beteiligten Anschlüsse sowie Zeit und Ort eines Gesprächs. Es geht nicht um die Inhalte der Telekommunikation, sondern um die Frage, ob und wann überhaupt Telekommunikation stattgefunden hat. Gegenwärtig können die Strafverfolgungsbehörden auf Grundlage von § 100g der Strafprozessordnung (StPO) Verkehrsdaten bei den Telekommunikationsunternehmen bei Vorliegen eines Anfangsverdachts und entsprechender richterlicher Anordnung erheben. Dies gilt jedoch nur für zukünftig anfallende Daten sowie für Daten, die zum Zeitpunkt der Anfrage noch gespeichert sind, zum Beispiel, weil sie aus geschäftlichen Gründen noch benötigt werden. Die Speicherpraxis ist bei den einzelnen Unternehmen unterschiedlich und reicht von sehr wenigen Tagen bis zu vielen Monaten. Es ist daher vom Zufall abhängig, ob Verkehrsdaten zum Zeitpunkt der Anfrage noch vorhanden sind oder nicht. Dies führt zu Lücken bei der Strafverfolgung und bei der Gefahrenabwehr und kann im Einzelfall dazu führen, dass strafrechtliche Ermittlungen ohne Erfolg bleiben, weil weitere Ermittlungsansätze nicht vorhanden sind.

Dieser Zustand ist mit der Bedeutung, die einer effektiven Strafverfolgung zukommt, nur schwer zu vereinbaren. Das Bundesverfassungsgericht hat wiederholt das verfassungsrechtliche Gebot einer effektiven Strafverfolgung hervorgehoben, das Interesse an einer möglichst vollständigen Wahrheitsermittlung im Strafverfahren betont und die wirksame Aufklärung gerade schwerer Straftaten als einen wesentlichen Auftrag eines rechtsstaatlichen Gemeinwesens bezeichnet (BVerfGE 129, 208 <260> m. w. N.). Um diesen Zustand zu ändern, ist die Einführung einer gesetzlichen Pflicht zur Speicherung von Verkehrsdaten durch die Erbringer öffentlich zugänglicher Telekommunikationsdienste erforderlich. Allerdings unterliegt eine entsprechende Regelung wegen der mit ihr verbundenen Grundrechtseingriffe strengen Anforderungen hinsichtlich des Umfangs der gespeicherten Daten sowie der Datenverwendung. Sie ist auf das absolut Notwendige zu beschränken. Hinsichtlich der Datensicherheit muss ein hoher Standard normenklar und verbindlich vorgegeben werden.

Dies war bei den bisherigen Regelungen zur Einführung einer Speicherpflicht zur Strafverfolgungsvorsorge und zur Gefahrenabwehr auf europäischer wie auf nationaler Ebene nicht der Fall. Daher hat das Bundesverfassungsgericht mit Urteil vom 2. März 2010 (BVerfGE 125, 260) die §§ 113a und 113b TKG und auch § 100g Absatz 1 Satz 1 StPO, soweit danach Verkehrsdaten nach § 113a TKG erhoben werden durften, wegen Verstoßes gegen Artikel 10 Absatz 1 des Grundgesetzes (GG) für nichtig erklärt und damit im Ergebnis die maßgeblichen Regelungen zur 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. L 105 vom 13.4.2006, S. 54) aufgehoben. Der Gerichtshof der Europäischen Union hat am 8. April 2014 die Richtlinie 2006/24/EG

für ungültig erklärt (verbundene Rechtssachen C-293/12 und C-594/12, EuZW 2014, 459), weil sie die Grundrechte aus den Artikeln 7 und 8 der Grundrechtecharta der Europäischen Union in unverhältnismäßigem Umfang einschränkte.

B. Lösung

Es wird eine Regelung zur zeitlich befristeten Speicherung von Verkehrsdaten zur Strafverfolgungsvorsorge und zur Gefahrenabwehr geschaffen. Diese soll die Eingriffe in das Telekommunikationsgeheimnis aus Artikel 10 GG und die Grundrechte auf Datenschutz nach den Artikeln 7 (Achtung der Privatsphäre) und 8 (Schutz personenbezogener Daten) der Grundrechtecharta der Europäischen Union aus Gründen der effektiven Strafverfolgung in zulässiger Weise gestalten. Dies geschieht dadurch, dass zwar eine Pflicht der Telekommunikationsanbieter vorgesehen wird, im Einzelnen bezeichnete Verkehrsdaten für eine beschränkte Zeit zu speichern, die Erhebung der Daten durch staatliche Stellen aber nur unter sehr engen Voraussetzungen ermöglicht wird. Die Eingriffsintensität wird durch ein deutlich reduziertes Datenvolumen (keine verpflichtende Speicherung von Daten von Diensten der elektronischen Post) und eine sehr kurze Speicherfrist (vier bzw. zehn Wochen) im Vergleich zur vorhergehenden Ausgestaltung deutlich reduziert.

Für die Erhebung der Daten zum Zweck der Verfolgung von besonders schweren Straftaten sieht der neu formulierte § 100g StPO-E nach Eingriffsintensität abgestufte Befugnisse vor, die zwischen den bei den Erbringer öffentlich zugänglicher Telekommunikationsdienste zu geschäftlichen Zwecken gespeicherten Verkehrsdaten (§ 100g Absatz 1 StPO-E) und den nach Maßgabe der §§ 113a ff. TKG-E verpflichtend gespeicherten Verkehrsdaten (§ 100g Absatz 2 StPO-E) differenzieren. Den grundrechtlichen Vorgaben entsprechend wird eine Erhebung der verpflichtend zu speichernden Verkehrsdaten nur unter sehr engen Voraussetzungen möglich sein, nämlich zur Verfolgung der in § 100g Absatz 2 StPO-E bezeichneten besonders schweren Straftaten, die auch im Einzelfall schwer wiegen müssen. Die Erhebung von gespeicherten Standortdaten ist nur unter denselben engen Voraussetzungen möglich. Außerdem werden die Anforderungen an eine Funkzellenabfrage präzisiert, um zu gewährleisten, dass auch bei diesen Datenerhebungen die Verhältnismäßigkeit gewahrt ist.

Dem Anliegen, in einer immer stärker von Informations- und Kommunikationstechnologie geprägten Gesellschaft effektive Strafverfolgung zu ermöglichen, steht die Notwendigkeit gegenüber, den strafrechtlichen Schutz von Informationssystemen und der in ihnen gespeicherten Daten vor Angriffen und Ausspähungen ausreichend zu gewährleisten. Dieser Schutz muss sich auch gegen Tathandlungen richten, mit denen ausgespähte, abgefangene oder in anderer Weise rechtswidrig erlangte Daten gehandelt und damit die durch die Vortat erfolgte Beeinträchtigung der formellen Verfügungsbefugnis des Berechtigten über seine Daten fortgesetzt und vertieft wird. Die geltenden strafrechtlichen Regelungen gegen den Handel mit illegal erlangten Daten sind unzureichend und weisen Schutzlücken auf. Der Entwurf sieht daher die Einführung eines neuen Straftatbestands der Datenhehlerei (§ 202d des Strafgesetzbuches (StGB)) vor. Danach soll sich strafbar machen, wer sich oder einem anderen nicht öffentlich zugängliche Daten, die ein anderer durch eine rechtswidrige Tat erlangt hat, verschafft, wer sie einem anderen überlässt, wer sie verbreitet oder in sonstiger Weise zugänglich macht, um sich oder einen Dritten zu bereichern oder einen anderen zu schädigen.

C. Alternativen

Keine.

D. Haushaltsausgaben ohne Erfüllungsaufwand

Keine.

E. Erfüllungsaufwand

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Erfüllungsaufwand für die Bürgerinnen und Bürger entsteht nicht.

E.2 Erfüllungsaufwand für die Wirtschaft

Für die betroffenen Telekommunikationsunternehmen entsteht durch die Erfüllung der in § 113b TKG-E vorgesehenen Speicherpflicht und die damit verbundenen – wegen der Vorgaben des Bundesverfassungsgerichts unvermeidbaren – Regelungen zur Verwendung der Daten, zur Gewährleistung der Datensicherheit und Datenqualität, zur Protokollierung der Zugriffe auf die Daten sowie zur Aufnahme bestimmter Angaben in das zu erstellende Sicherheitskonzept ein zusätzlicher Aufwand.

Zusätzlicher Aufwand entsteht auch durch die mit der in § 113b TKG-E vorgesehenen Speicherpflicht im Zusammenhang stehenden Verpflichtungen zur Übermittlung von Verkehrsdaten nach § 100g Absatz 2 StPO-E und zur Auskunftserteilung über Bestandsdaten nach § 100j StPO-E.

Dieser Aufwand kann nur geschätzt werden: Die 2007 eingeführte Verpflichtung zur Vorratsdatenspeicherung führte nach Angaben des Branchenverbandes BITKOM bei den dort organisierten Telekommunikationsunternehmen zu erforderlichen Investitionen in Höhe von ca. 75 Millionen Euro. Hinzu kamen jährliche Betriebskosten in zweistelliger Millionenhöhe. Der Verband der deutschen Internetwirtschaft e. V. (eco) hat demgegenüber dargelegt, dass die Internetwirtschaft bei der Vorratsdatenspeicherung in der ursprünglich von der Europäischen Union vorgegebenen Form mehr als 300 Millionen Euro in die notwendige Technik investiert habe. Durch die erhöhten Datensicherheitsanforderungen und Veränderungen aufgrund der technischen Entwicklung dürften sich zusätzliche Kosten ergeben. Andererseits sollten die Unternehmen zumindest teilweise auf die bereits getätigten Investitionen zurückgreifen können. Bezogen auf konkrete Unternehmen wurden seinerzeit jeweils Investitionen in Höhe von drei bis neun Millionen Euro erforderlich. Nachdem die Speicherpflicht unterschiedslos alle Telekommunikationsunternehmen betrifft, sind ca. 1 000 Unternehmen betroffen. Bei den voraussichtlichen Kosten muss man den Investitionsaufwand für die erstmalige Einrichtung sowie die laufenden Kosten für die stetige Aktualisierung der Sicherungsmaßnahmen unterscheiden. Da sich die Lage bei den einzelnen Unternehmen sehr unterschiedlich gestalten dürfte, ist der Aufwand derzeit nicht bezifferbar.

Der Aufwand, der für die Übermittlung von Verkehrsdaten und die Auskunftserteilung über Bestandsdaten entsteht, wird nach § 23 Justizvergütungs- und -entschädigungsgesetzes (JVEG) entschädigt. Darüber hinaus sieht der Entwurf für die zur Erfüllung der Speicherpflichten nach den §§ 113b ff. TKG-E erforderlichen Investitionen und gegebenenfalls gesteigerten Betriebskosten eine Entschädigungsregelung vor, wenn die Kosten für einzelne Unternehmen erdrosselnde Wirkung haben könnten.

Davon Bürokratiekosten aus Informationspflichten

Der Entwurf führt vier neue Informationspflichten im Sinne des Gesetzes zur Einsetzung eines Nationalen Normenkontrollrates für Unternehmen ein.

E.3 Erfüllungsaufwand der Verwaltung

Durch die Änderung der Vorschriften des Telekommunikationsgesetzes in Artikel 2 entsteht bei der Bundesnetzagentur Vollzugsaufwand, der in Sachinvestitionen und Personalkosten aufzugliedern ist. Dieser – wegen der Vorgaben des Bundesverfassungsgerichts in seinem Urteil zur Vorratsdatenspeicherung unvermeidbare – Mehraufwand entsteht unter anderem durch die Verpflichtung nach § 113f TKG-E, einen Anforderungskatalog zu erstellen, diesen fortlaufend zu überprüfen und bei Bedarf unverzüglich anzupassen. Zudem resultiert aus der Verpflichtung zur Verkehrsdatenspeicherung ein erhöhter Kontrollaufwand im Rahmen der Aufsicht nach § 115 TKG sowie der Anwendung der neuen Bußgeldtatbestände. Diese neuen Aufgaben führen bei der Bundesnetzagentur zu einem Bedarf von 25 Planstellen/Stellen mit jährlichen Personalkosten in Höhe von 2,9 Millionen Euro. Des Weiteren entstehen Kosten für Sachmittel in Höhe von einmalig 150 000 Euro im ersten Jahr.

Noch nicht abzuschätzen ist, wie sich die Entschädigungsregelung in § 113a Absatz 2 TKG-E auswirken wird. Von den vorhandenen ca. 1000 Erbringer öffentlich zugänglicher Telekommunikationsdienste sind 20 so groß, dass sie 98 Prozent des Marktes abdecken, die übrigen sind kleine bis mittlere Unternehmen, die sich voraussichtlich häufig auf eine unbillige Härte berufen werden. Dies kann jedoch erst geschehen, wenn der entsprechende Anforderungskatalog (§ 113f TKG-E) durch die Bundesnetzagentur erstellt wurde.

Für die Kommunen entsteht kein Erfüllungsaufwand.

F. Weitere Kosten

Die Verkehrsdatenabfrage stellt kein neues Ermittlungsinstrument dar. Kosten für die Judikative werden voraussichtlich nicht in nennenswertem Umfang entstehen, da die Abfragen voraussichtlich in dem gleichen Umfang erfolgen wie bisher, aber zu besseren Ergebnissen führen. Die nach dem JVEG zu gewährenden Kostenpauschalen werden die Haushalte der Länder belasten; es ist aber nicht zu erwarten, dass dies in erheblich höherem Maße der Fall ist als bei den bestehenden Regelungen.

Durch die Einführung eines neuen Straftatbestandes der Datenhehlerei (§ 202d StGB-E) können den Landeshaushalten Verfahrens- und Vollzugskosten entstehen, deren genaue Höhe sich nicht näher beziffern lässt.

Für den Bund entstehen allenfalls in geringem Umfang Mehrausgaben. Etwaiger Mehrbedarf an Sach- und Personalmitteln kann innerhalb der vorhandenen Kapazitäten und der verfügbaren Mittel aufgefangen werden und soll finanziell und stellenmäßig im Einzelplan 07 (Einzelplan des Bundesministeriums der Justiz und für Verbraucherschutz) ausgeglichen werden.

Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz

Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten

Vom ...

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1

Änderung der Strafprozessordnung

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

1. In der Inhaltsübersicht werden nach der Angabe zu § 101 folgende Angaben eingefügt:

„§ 101a Gerichtliche Entscheidung, Datenkennzeichnung und -auswertung, Benachrichtigungspflichten bei der Erhebung von Verkehrsdaten

§ 101b Statistische Erfassung der Erhebung von Verkehrsdaten“.

2. § 100g wird wie folgt gefasst:

„§ 100g

Erhebung von Verkehrsdaten

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

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

2. eine Straftat mittels Telekommunikation begangen hat,

so dürfen Verkehrsdaten (§ 96 Absatz 1 des Telekommunikationsgesetzes) erhoben werden, soweit dies für die Erforschung des Sachverhalts erforderlich ist und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht. Im Fall des Satzes 1 Nummer 2 ist die Maßnahme nur zulässig, wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos wäre. Die Erhebung von Standortdaten ist nach diesem Absatz nur für künftig anfallende Verkehrsdaten oder in Echtzeit und nur im Fall des Satzes 1 Nummer 1 zulässig, soweit sie für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich ist.

(2) Begründen bestimmte Tatsachen den Verdacht, dass jemand als Täter oder Teilnehmer eine der in Satz 2 bezeichneten, besonders schweren Straftaten begangen hat oder in Fällen, in denen der Versuch strafbar ist, eine solche Straftat zu begehen versucht hat, und die Tat auch im Einzelfall besonders schwer wiegt, dürfen die nach § 113b des Telekommunikationsgesetzes gespeicherten Verkehrsdaten erhoben werden, soweit die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht. Besonders schwere Straftaten im Sinne des Satzes 1 sind:

1. aus dem Strafgesetzbuch:

   a) Straftaten des Friedensverrats, des Hochverrats und der Gefährdung des demokratischen Rechtsstaates sowie des Landesverrats und der Gefährdung der äußeren Sicherheit nach den §§ 80, 81, 82, 89a, nach den §§ 94, 95 Absatz 3 und § 96 Absatz 1, jeweils auch in Verbindung mit § 97b, sowie nach den §§ 97a, 98 Absatz 1 Satz 2, § 99 Absatz 2 und den §§ 100, 100a Absatz 4,

   b) besonders schwerer Fall des Landfriedensbruchs nach § 125a, Bildung krimineller Vereinigungen nach § 129 Absatz 1 in Verbindung mit Absatz 4 Halbsatz 2 und Bildung terroristischer Vereinigungen nach § 129a Absatz 1, 2, 4, 5 Satz 1 Alternative 1, jeweils auch in Verbindung mit § 129b Absatz 1,

   c) Straftaten gegen die sexuelle Selbstbestimmung in den Fällen der §§ 176a, 176b, 177 Absatz 2 Satz 2 Nummer 2 und des § 179 Absatz 5 Nummer 2,

   d) Verbreitung, Erwerb und Besitz kinder- und jugendpornographischer Schriften in den Fällen des § 184b Absatz 2, § 184c Absatz 2,

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

   f) Straftaten gegen die persönliche Freiheit in den Fällen der §§ 234, 234a Absatz 1, 2, §§ 239a, 239b und Menschenhandel zum Zweck der sexuellen Ausbeutung und zum Zweck der Ausbeutung der Arbeitskraft nach § 232 Absatz 3, 4 oder 5, § 233 Absatz 3, jeweils soweit es sich um Verbrechen handelt,

   g) schwerer Bandendiebstahl nach § 244a Absatz 1, schwerer Raub nach § 250 Absatz 1 oder Absatz 2, Raub mit Todesfolge nach § 251, räuberische Erpressung nach § 255 und besonders schwerer Fall einer Erpressung nach § 253 unter den in § 253 Absatz 4 Satz 2 genannten Voraussetzungen, gewerbsmäßige Bandenhehlerei nach § 260a Absatz 1, besonders schwerer Fall der Geldwäsche und der Verschleierung unrechtmäßig erlangter Vermögenswerte nach § 261 unter den in § 261 Absatz 4 Satz 2 genannten Voraussetzungen,

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

2. aus dem Aufenthaltsgesetz:

   a) Einschleusen von Ausländern nach § 96 Absatz 2,

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

3. aus dem Betäubungsmittelgesetz:

a) besonders schwerer Fall einer Straftat nach § 29 Absatz 1 Satz 1 Nummer 1, 5, 6, 10, 11 oder 13, Absatz 3 unter der in § 29 Absatz 3 Satz 2 Nummer 1 genannten Voraussetzung,

b) eine Straftat nach den §§ 29a, 30 Absatz 1 Nummer 1, 2, 4, § 30a,

4. aus dem Grundstoffüberwachungsgesetz:

eine Straftat nach § 19 Absatz 1 unter den in § 19 Absatz 3 Satz 2 genannten Voraussetzungen,

5. aus dem Gesetz über die Kontrolle von Kriegswaffen:

a) eine Straftat nach § 19 Absatz 2 oder § 20 Absatz 1, jeweils auch in Verbindung mit § 21,

b) besonders schwerer Fall einer Straftat nach § 22a Absatz 1 in Verbindung mit Absatz 2,

6. aus dem Völkerstrafgesetzbuch:

a) Völkermord nach § 6,

b) Verbrechen gegen die Menschlichkeit nach § 7,

c) Kriegsverbrechen nach den §§ 8 bis 12,

7. aus dem Waffengesetz:

a) besonders schwerer Fall einer Straftat nach § 51 Absatz 1 in Verbindung mit Absatz 2,

b) besonders schwerer Fall einer Straftat nach § 52 Absatz 1 Nummer 1 in Verbindung mit Absatz 5.

(3) Die Erhebung aller in einer Funkzelle angefallenen Verkehrsdaten (Funkzellenabfrage) ist nur unter den Voraussetzungen des Absatzes 1 Satz 1 Nummer 1 zulässig, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre. Auf nach § 113b des Telekommunikationsgesetzes gespeicherte Verkehrsdaten darf nur unter den Voraussetzungen des Absatzes 2 zurückgegriffen werden.

(4) Die Erhebung von Verkehrsdaten, die sich gegen eine der in § 53 Absatz 1 Satz 1 Nummer 1 bis 5 genannten Personen richtet und die voraussichtlich Erkenntnisse erbringen würde, über die diese das Zeugnis verweigern dürfte, ist unzulässig. Dennoch erlangte Erkenntnisse dürfen nicht verwendet werden. Aufzeichnungen hierüber sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und der Löschung der Aufzeichnungen ist aktenkundig zu machen. Die Sätze 2 bis 4 gelten entsprechend, wenn durch eine Ermittlungsmaßnahme, die sich nicht gegen eine in § 53 Absatz 1 Satz 1 Nummer 1 bis 5 genannte Person richtet, von dieser Person Erkenntnisse erlangt werden, über die sie das Zeugnis verweigern dürfte. § 160a Absatz 3 und 4 gilt entsprechend.

(5) Erfolgt die Erhebung von Verkehrsdaten nicht beim Erbringer öffentlich zugänglicher Telekommunikationsdienste, bestimmt sie sich nach Abschluss des Kommunikationsvorgangs nach den allgemeinen Vorschriften.“

3. In § 100j Absatz 2 werden die Wörter „§ 113 Absatz 1 Satz 3“ durch die Wörter „§§ 113 Absatz 1 Satz 3, 113c Absatz 1 Nummer 3“ ersetzt.

4. § 101 wird wie folgt geändert:

   a) In Absatz 1 wird die Angabe „100c bis 100i“ durch die Angabe „100c bis 100f, 100h, 100i“ ersetzt.

   b) Absatz 4 wird wie folgt geändert:

      aa) Satz 1 wird wie folgt geändert.

         aaa) Nummer 6 wird aufgehoben.

         bbb) Die Nummern 7 bis 12 werden die Nummern 6 bis 11.

      bb) In Satz 4 werden die Wörter „Satz 1 Nr. 2, 3 und 6“ durch die Wörter „Satz 1 Nummer 2 und 3“ ersetzt.

5. Nach § 101 werden die folgenden §§ 101a und 101b eingefügt:

„§ 101a

Gerichtliche Entscheidung, Datenkennzeichnung und -auswertung, Benachrichtigungspflichten bei der Erhebung von Verkehrsdaten

(1) Bei Erhebungen von Verkehrsdaten nach § 100g StPO gelten § 100a Absatz 3 und § 100b Absatz 1 bis 4 entsprechend mit der Maßgabe, dass

1. in der Entscheidungsformel nach § 100b Absatz 2 Satz 2 auch die zu übermittelnden Daten und der Zeitraum, für den sie übermittelt werden sollen, eindeutig anzugeben sind,

2. der nach § 100b Absatz 3 Satz 1 zur Auskunft Verpflichtete auch mitzuteilen hat, welche der von ihm übermittelten Daten nach § 113b des Telekommunikationsgesetzes gespeichert wurden.

In den Fällen des § 100g Absatz 2 findet § 100b Absatz 1 Satz 2 und 3 keine Anwendung. Bei Funkzellenabfragen nach § 100g Absatz 3 genügt abweichend von § 100b Absatz 2 Satz 2 Nummer 2 eine räumlich und zeitlich eng begrenzte und hinreichend bestimmte Bezeichnung der Telekommunikation.

(2) Wird eine Maßnahme nach § 100g angeordnet oder verlängert, sind in der Begründung einzelfallbezogen insbesondere die wesentlichen Erwägungen zur Erforderlichkeit und Angemessenheit der Maßnahme, auch hinsichtlich des Umfangs der zu erhebenden Daten und des Zeitraums, für den sie erhoben werden sollen, darzulegen.

(3) Personenbezogene Daten, die durch Maßnahmen nach § 100g erhoben wurden, sind entsprechend zu kennzeichnen und unverzüglich auszuwerten. Bei der Kennzeichnung ist erkennbar zu machen, ob es sich um Daten handelt, die nach § 113b des Telekommunikationsgesetzes gespeichert waren. Nach Übermittlung an

eine andere Stelle ist die Kennzeichnung durch diese aufrechtzuerhalten. Für die Löschung personenbezogener Daten gilt § 101 Absatz 8 entsprechend.

(4) Die Beteiligten der betroffenen Telekommunikation sind von der Erhebung der Verkehrsdaten nach § 100g zu benachrichtigen. § 101 Absatz 4 bis 7 gilt entsprechend mit der Maßgabe, dass

1. das Unterbleiben der Benachrichtigung nach § 101 Absatz 4 Satz 3 der gerichtlichen Anordnung bedarf;

2. abweichend von § 101 Absatz 6 Satz 1 die Zurückstellung der Benachrichtigung nach § 101 Absatz 5 Satz 1 stets der Anordnung des zuständigen Gerichts bedarf und eine erstmalige Zurückstellung auf höchstens zwölf Monate zu befristen ist.

§ 101b

Statistische Erfassung der Erhebung von Verkehrsdaten

Über Maßnahmen nach § 100g ist entsprechend § 100b Absatz 5 jährlich eine Übersicht zu erstellen, in der anzugeben sind

1. unterschieden nach Maßnahmen nach den § 100g Absatz 1, 2 und 3

   a) die Anzahl der Verfahren, in denen diese Maßnahmen durchgeführt wurden;

   b) die Anzahl der Erstanordnungen, mit denen diese Maßnahmen angeordnet wurden;

   c) die Anzahl der Verlängerungsanordnungen, mit denen diese Maßnahmen angeordnet wurden;

2. unterschieden für die Bereiche Festnetz-, Mobilfunk- und Internetdienste und jeweils untergliedert nach der Anzahl der zurückliegenden Wochen, für die die Erhebung von Verkehrsdaten angeordnet wurde, jeweils bemessen ab dem Zeitpunkt der Anordnung

   a) die Anzahl der Anordnungen nach § 100g Absatz 1;

   b) die Anzahl der Anordnungen nach § 100g Absatz 2;

   c) die Anzahl der Anordnungen nach § 100g Absatz 3;

   d) die Anzahl der Anordnungen, die teilweise ergebnislos geblieben sind, weil die abgefragten Daten teilweise nicht verfügbar waren;

   e) die Anzahl der Anordnungen, die ergebnislos geblieben sind, weil keine Daten verfügbar waren.“

6. § 160a wird wie folgt geändert:

   a) In Absatz 4 Satz 1 wird vor dem Wort „Begünstigung“ das Wort „Datenhehlerei,“ eingefügt.

   b) In Absatz 5 wird die Angabe „§§ 97 und 100c Abs. 6“ durch die Angabe „§§ 97, 100c Absatz 6 und § 100g Absatz 4“ ersetzt.

7. In § 304 Absatz 4 Satz 2 Nummer 1 wird nach der Angabe „§ 101 Abs. 1“ die Angabe „und § 101a Absatz 1“ eingefügt.

8. In den §§ 3, 60 Nummer 2, 68b Absatz 1 Satz 4 Nummer 1, 97 Absatz 2 Satz 3, 102 und 138a Absatz 1 Nummer 3 wird jeweils vor dem Wort „Begünstigung“ das Wort „Datenhehlerei,“ eingefügt.

Artikel 2

Änderung des Telekommunikationsgesetzes

Das Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch … geändert worden ist, wird wie folgt geändert:

1. In der Inhaltsübersicht werden die Angaben zu den §§ 113a und 113b durch die folgenden Angaben ersetzt:

„§ 113a Verpflichtete, Entschädigung

§ 113b Pflichten zur Speicherung von Verkehrsdaten

§ 113c Verwendung der Daten

§ 113d Gewährleistung der Sicherheit der Daten

§ 113e Protokollierung

§ 113f Anforderungskatalog

§ 113g Sicherheitskonzept“.

2. Die §§ 113a und 113b werden durch die folgenden §§ 113a bis 113g ersetzt:

„§ 113a

Verpflichtete; Entschädigung

(1) Die Verpflichtungen zur Speicherung von Verkehrsdaten, zur Verwendung der Daten und zur Datensicherheit nach den §§ 113b bis 113g beziehen sich auf Erbringer öffentlich zugänglicher Telekommunikationsdienste. Wer öffentlich zugängliche Telekommunikationsdienste erbringt, aber nicht alle der nach Maßgabe der nachstehenden Regelungen zu speichernden Daten selbst erzeugt oder verarbeitet, hat

1. sicherzustellen, dass die nicht von ihm selbst bei der Erbringung seines Dienstes erzeugten oder verarbeiteten Daten gemäß § 113b Absatz 1 gespeichert werden, und

2. der Bundesnetzagentur auf deren Verlangen unverzüglich mitzuteilen, wer diese Daten speichert.

(2) Für notwendige Aufwendungen, die den Verpflichteten durch die Umsetzung der Vorgaben aus den §§ 113b, 113d bis 113g entstehen, ist eine angemessene Entschädigung zu zahlen, soweit dies zur Abwendung oder zum Ausgleich unbilliger Härten geboten erscheint. Für die Bemessung der Entschädigung sind die tatsächlich

entstandenen Kosten maßgebend. Über Anträge auf Entschädigung entscheidet die Bundesnetzagentur.

§ 113b

Pflichten zur Speicherung von Verkehrsdaten

(1) Die in § 113a Absatz 1 Genannten sind verpflichtet, Daten nach Absatz 2 und 3 für zehn Wochen und Standortdaten nach Absatz 4 für vier Wochen im Inland zu speichern.

(2) Die Erbringer öffentlich zugänglicher Telefondienste speichern:

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

2. Datum und Uhrzeit von Beginn und Ende der Verbindung unter Angabe der zugrunde liegenden Zeitzone,

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

4. im Fall mobiler Telefondienste ferner

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

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

   c) Datum und Uhrzeit der ersten Aktivierung des Dienstes, wenn Dienste im Voraus bezahlt wurden,

5. im Fall von Internet-Telefondiensten auch die Internetprotokoll-Adressen des anrufenden und des angerufenen Anschlusses und zugewiesene Benutzerkennungen.

Satz 1 gilt entsprechend

1. bei der Übermittlung einer Kurz-, Multimedia- oder ähnlichen Nachricht; hierbei treten an die Stelle der Angaben nach Satz 1 Nummer 2 die Zeitpunkte der Versendung und des Empfangs der Nachricht;

2. für unbeantwortete oder wegen eines Eingriffs des Netzwerkmanagements erfolglose Anrufe, soweit der Erbringer die in Satz 1 genannten Verkehrsdaten für die in § 96 Absatz 1 Satz 2 genannten Zwecke speichert oder protokolliert.

(3) Die Erbringer öffentlich zugänglicher Internetzugangsdienste speichern

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

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

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

(4) Im Fall der Nutzung mobiler Telefondienste sind die Bezeichnungen der Funkzellen zu speichern, die durch den anrufenden und den angerufenen Anschluss bei Beginn der Verbindung genutzt wurden. Bei öffentlich zugänglichen Internetzugangsdiensten ist die Bezeichnung der bei Beginn der Internetverbindung genutzten Funkzelle zu speichern. Zusätzlich sind die Daten zu speichern, aus denen sich die geografische Lage und die Hauptstrahlrichtungen der die jeweilige Funkzelle versorgenden Funkantennen ergeben.

(5) Der Inhalt der Kommunikation, Daten über aufgerufene Internetseiten und Daten von Diensten der elektronischen Post dürfen auf Grund dieser Vorschrift nicht gespeichert werden.

(6) Daten, die den in § 99 Absatz 2 genannten Verbindungen zugrunde liegen, dürfen auf Grund dieser Vorschrift nicht gespeichert werden. Dies gilt entsprechend für Telefonverbindungen, die von den in § 99 Absatz 2 genannten Stellen ausgehen. § 99 Absatz 2 Satz 2 bis 7 gilt entsprechend.

(7) Die Speicherung der Daten hat so zu erfolgen, dass Auskunftsersuchen der berechtigten Stellen unverzüglich beantwortet werden können.

(8) Der nach § 113a Absatz 1 Verpflichtete hat die auf Grund dieser Vorschrift gespeicherten Daten unverzüglich, spätestens jedoch binnen einer Woche nach Ablauf der Speicherfristen nach Absatz 1, irreversibel zu löschen oder die irreversible Löschung sicherzustellen.

§ 113c

Verwendung der Daten

(1) Die auf Grund des § 113b gespeicherten Daten dürfen

1. an eine Strafverfolgungsbehörde übermittelt werden, soweit diese die Übermittlung unter Berufung auf eine gesetzliche Bestimmung, die ihr eine Erhebung der in § 113b genannten Daten zur Verfolgung besonders schwerer Straftaten erlaubt, verlangt;

2. an eine Gefahrenabwehrbehörde der Länder übermittelt werden, soweit diese die Übermittlung unter Berufung auf eine gesetzliche Bestimmung, die ihr eine Erhebung der in § 113b genannten Daten zur Abwehr einer konkreten Gefahr für Leib, Leben oder Freiheit einer Person oder für den Bestand des Bundes oder eines Landes erlaubt, verlangt wird;

3. durch den Erbringer öffentlich zugänglicher Telekommunikationsdienste für eine Auskunft nach § 113 Absatz 1 Satz 3 verwendet werden.

(2) Für andere Zwecke als die in Absatz 1 genannten dürfen die auf Grund des § 113b gespeicherten Daten nicht verwendet werden.

(3) Die Übermittlung der Daten erfolgt nach Maßgabe der Rechtsverordnung nach § 110 Absatz 2 und der Technischen Richtlinie nach § 110 Absatz 3. Die Daten sind so zu kennzeichnen, dass erkennbar ist, dass es sich um Daten handelt, die nach § 113b gespeichert waren. Nach Übermittlung an eine andere Stelle ist die Kennzeichnung durch diese aufrechtzuerhalten.

§ 113d

Gewährleistung der Sicherheit der Daten

Der nach § 113a Absatz 1 Verpflichtete hat sicherzustellen, dass die auf Grund der Speicherungsverpflichtung nach § 113b Absatz 1 gespeicherten Daten durch technische und organisatorische Maßnahmen nach dem Stand der Technik gegen unbefugte Kenntnisnahme und Verwendung geschützt werden. Die Maßnahmen umfassen insbesondere:

1. den Einsatz eines besonders sicheren Verschlüsselungsverfahrens,

2. die Speicherung in gesonderten, von den für die üblichen betrieblichen Aufgaben getrennten Speichereinrichtungen,

3. die Speicherung mit einem hohen Schutz vor dem Zugriff aus dem Internet auf vom Internet entkoppelten Rechnern,

4. die Beschränkung des Zutritts zu den Datenverarbeitungsanlagen auf Personen die durch den Verpflichteten besonders ermächtigt sind und

5. die notwendige Mitwirkung von mindestens zwei Personen beim Zugriff auf die Daten, die dazu durch den Verpflichteten besonders ermächtigt worden sind.

§ 113e

Protokollierung

(1) Der nach § 113a Absatz 1 Verpflichtete hat sicherzustellen, dass für Zwecke der Datenschutzkontrolle jeder Zugriff, insbesondere das Lesen, Kopieren, Ändern, Löschen und Sperren der auf Grund der Speicherungsverpflichtung nach § 113b Absatz 1 gespeicherten Daten protokolliert wird. Zu protokollieren sind

1. der Zeitpunkt des Zugriffs,

2. die auf die Daten zugreifenden Personen ,

3. Zweck und Art des Zugriffs.

(2) Für andere als die in Absatz 1 Satz 1 genannten Zwecke dürfen die Protokolldaten nicht verwendet werden.

(3) Der nach § 113a Absatz 1 Verpflichtete hat sicherzustellen, dass die Protokolldaten nach einem Jahr gelöscht werden.

§ 113f

Anforderungskatalog

(1) Bei der Umsetzung der Verpflichtungen gemäß §§ 113b bis 113e ist ein besonders hoher Standard der Datensicherheit und Datenqualität zu gewährleisten. Die Einhaltung dieses Standards wird vermutet, wenn alle Anforderungen des Katalogs der technischen Vorkehrungen und sonstigen Maßnahmen erfüllt werden, den die Bundesnetzagentur unter Beteiligung des Bundesamtes für Sicherheit in der Informa-

tionstechnik und der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit erstellt.

(2) Die Bundesnetzagentur überprüft fortlaufend die im Katalog nach Absatz 1 Satz 1 enthaltenen Anforderungen; hierbei berücksichtigt sie den Stand der Technik und der Fachdiskussion. Stellt die Bundesnetzagentur Änderungsbedarf fest, ist der Katalog unter Beteiligung des Bundesamtes für Sicherheit in der Informationstechnik und der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit unverzüglich anzupassen.

(3) § 109 Absatz 6 Satz 2 und 3 gilt entsprechend. § 109 Absatz 7 gilt mit der Maßgabe, dass an die Stelle der Anforderungen nach § 109 Absatz 1 bis 3 die Anforderungen nach Absatz 1 Satz 1, § 113b Absatz 7 und 8, § 113d und § 113e Absatz 1 und 3 treten.

§ 113g

Sicherheitskonzept

Der nach § 113a Absatz 1 Verpflichtete hat in das Sicherheitskonzept nach § 109 Absatz 4 zusätzlich aufzunehmen

1. welche Systeme zur Erfüllung der Verpflichtungen der §§ 113b bis 113e betrieben werden,

2. von welchen Gefährdungen für diese Systeme auszugehen ist und

3. welche technischen Vorkehrungen oder sonstigen Maßnahmen getroffen oder geplant sind, um diesen Gefährdungen entgegenzuwirken die Verpflichtungen aus den §§ 113b bis 113e zu erfüllen.

Der nach § 113a Verpflichtete hat der Bundesnetzagentur das Sicherheitskonzept unverzüglich nach dem Beginn der Speicherung nach § 113b und erneut bei jeder Änderung vorzulegen. Bleibt das Sicherheitskonzept unverändert, hat der nach § 113a Verpflichtete dies gegenüber der Bundesnetzagentur im Abstand von jeweils zwei Jahren schriftlich zu erklären.“

3. Dem § 121 Absatz 1 wird folgender Satz angefügt:

„Ferner teilt die Bundesnetzagentur in dem Bericht mit,

1. in welchem Umfang und mit welchen Ergebnissen sie Sicherheitskonzepte nach § 113g und deren Einhaltung überprüft hat und

2. ob und welche Beanstandungen und weiteren Ergebnisse die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit an die Bundesnetzagentur übermittelt hat (§ 115 Absatz 4 Satz 2).“

4. § 149 wird wie folgt geändert:

a) Absatz 1 wird wie folgt geändert:

aa) In Nummer 35 wird das Wort „oder“ durch ein Komma ersetzt.

bb) Nach Nummer 35 werden die folgenden Nummern 36 bis 44 eingefügt:

„36. entgegen § 113b Absatz 1, auch in Verbindung mit § 113b Absatz 7, Daten nicht, nicht richtig, nicht vollständig, nicht in der vorgeschriebenen Weise, nicht für die vorgeschriebene Dauer oder nicht rechtzeitig speichert,

37. entgegen § 113b Absatz 1 in Verbindung mit § 113a Absatz 1 Satz 2 nicht sicherstellt, dass die dort genannten Daten gespeichert werden, oder eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,

38. entgegen § 113b Absatz 8 Daten nicht oder nicht rechtzeitig löscht oder nicht sicherstellt, dass die Daten rechtzeitig gelöscht werden,

39. entgegen § 113c Absatz 2 Daten für andere als die genannten Zwecke verwendet,

40. entgegen § 113d Satz 1 nicht sicherstellt, dass Daten gegen unbefugte Kenntnisnahme und Verwendung geschützt werden,

41. entgegen § 113e Absatz 1 nicht sicherstellt, dass jeder Zugriff protokolliert wird,

42. entgegen § 113e Absatz 2 Protokolldaten für andere als die genannten Zwecke verwendet,

43. entgegen § 113e Absatz 3 nicht sicherstellt, dass Protokolldaten rechtzeitig gelöscht werden,

44. entgegen § 113g Satz 2 das Sicherheitskonzept nicht oder nicht rechtzeitig vorlegt oder“.

cc) Die bisherige Nummer 36 wird Nummer 45.

b) Absatz 2 Satz 1 wird wie folgt gefasst:

„Die Ordnungswidrigkeit kann wie folgt geahndet werden:

1. in den Fällen des Absatzes 1 Nummer 4 Buchstabe a, Nummer 6, 10, 22, 27, 31 und 36 bis 40 mit einer Geldbuße bis zu fünfhunderttausend Euro,

2. in den Fällen des Absatzes 1 Nummer 7a, 16 bis 17a, 18, 26, 29, 30a, 33 und 41 bis 43 mit einer Geldbuße bis zu dreihunderttausend Euro,

3. in den Fällen des Absatzes 1 Nummer 4 Buchstabe b, Nummer 7b bis 7d, 7g, 7h, 12, 13 bis 13b, 13d bis 13o, 15, 17c, 19, 19a, 20, 21, 21b, 30 und 44 sowie des Absatzes 1a Nummer 1 bis 5 mit einer Geldbuße bis zu hunderttausend Euro,

4. in den Fällen des Absatzes 1 Nummer 7, 8, 9, 11, 17b, 21a, 21c, 23 und 24 mit einer Geldbuße bis zu fünfzigtausend Euro und

5. in den übrigen Fällen des Absatzes 1 sowie im Fall des Absatzes 1a Nummer 6 mit einer Geldbuße bis zu zehntausend Euro.“

5. Dem § 150 wird folgender Absatz 13 angefügt:

„(13) Die Speicherverpflichtung und die damit verbundenen Verpflichtungen nach den §§ 113b bis 113e und 113g sind spätestens ab dem … [einsetzen: Datum

des ersten Tages des 19. auf die Verkündung dieses Gesetzes folgenden Kalendermonats] zu erfüllen. Die Bundesnetzagentur veröffentlicht den nach § 113f Absatz 1 zu erstellenden Anforderungskatalog spätestens am … [einsetzen: Datum des ersten Tages des 13. auf die Verkündung dieses Gesetzes folgenden Kalendermonats].“

Artikel 3

Änderung des Einführungsgesetzes zur Strafprozessordnung

Dem Einführungsgesetz zur Strafprozessordnung in der im Bundesgesetzblatt Teil III, Gliederungsnummer 312-1, veröffentlichten bereinigten Fassung, das zuletzt durch … geändert worden ist, wird folgender § 12 angefügt:

„§ 12

Übergangsregelung zum Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten

(1) Nach § 96 Absatz 1 Satz 1 Nummer 1 des Telekommunikationsgesetzes gespeicherte Standortdaten dürfen bis zum [einsetzen: Datum des Tages, der vier Wochen nach dem in § 150 Absatz 13 Satz 1 TKG bezeichneten Tag liegt] auf der Grundlage des § 100g Absatz 1 in der bis zum Inkrafttreten des Gesetzes zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten geltenden Fassung erhoben werden.

(2) Die Übersicht nach § 101b der Strafprozessordnung in der Fassung des Gesetzes zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten …[einsetzen: Ausfertigungsdatum und Fundstelle] ist erstmalig für das Berichtsjahr anzuwenden, das dem Beginn der Speicherpflicht nach § 113b in Verbindung mit § 150 Absatz 13 Satz 1 des Telekommunikationsgesetzes folgt. Für die vorangehenden Berichtsjahre ist § 100g Absatz 4 der Strafprozessordnung in der bis zum Inkrafttreten des Gesetzes zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten geltenden Fassung anzuwenden.“

Artikel 4

Änderung des Justizvergütungs- und -entschädigungsgesetzes

Das Justizvergütungs- und -entschädigungsgesetz vom 5. Mai 2004 (BGBl. I S. 718, 776), das zuletzt durch ... geändert worden ist, wird wie folgt geändert:

1. Der Inhaltsübersicht wird folgende Angabe angefügt:

   „Anlage 3 (zu § 23 Absatz 1)“.

2. In § 6 Absatz 1 werden die Wörter „§ 4 Abs. 5 Satz 1 Nr. 5 Satz 2 des Einkommensteuergesetzes bestimmt“ durch die Wörter „der Verpflegungspauschale zur Abgeltung tatsächlich entstandener, beruflich veranlasster Mehraufwendungen im Inland nach dem Einkommensteuergesetz bemisst“ ersetzt.

3. In § 23 Absatz 2 Satz 1 wird jeweils in dem Satzteil vor Nummer 1 und in Nummer 1 das Wort „Strafverfolgungsbehörde“ durch die Wörter „Strafverfolgungs- oder Verfolgungsbehörde“ ersetzt.

4. Der Vorbemerkung nach der Überschrift von Abschnitt 1 der Anlage 2 wird folgende Überschrift vorangestellt:

   „Vorbemerkung 1:“.

5. Anlage 3 wird wie folgt geändert:

   a) In Absatz 2 der Allgemeinen Vorbemerkung werden die Wörter „300 bis 312, 400 und 401“ durch die Wörter „300 bis 321 und 400 bis 402“ ersetzt.

   b) Nach Nummer 201 wird folgende Nummer 202 eingefügt:

Nr.	Tätigkeit	Höhe
„202	Es muss auf Verkehrsdaten nach § 113b Abs. 2 bis 4 TKG zurückgegriffen werden: Die Pauschale 201 beträgt	40,00 €.“

   c) Abschnitt 3 wird wie folgt gefasst:

Nr.	Tätigkeit	Höhe
	„Abschnitt 3 Auskünfte über Verkehrsdaten	
300	Auskunft über gespeicherte Verkehrsdaten: für jede Kennung, die der Auskunftserteilung zugrunde liegt	30,00 €
	Die Mitteilung der die Kennung betreffenden Standortdaten ist mit abgegolten.	
301	Für die Auskunft muss auf Verkehrsdaten nach § 113b Abs. 2 bis 4 TKG zurückgegriffen werden Die Pauschale 300 beträgt	35,00 €
302	Die Auskunft wird im Fall der Nummer 300 aufgrund eines einheitlichen Ersuchens auch oder ausschließlich für künftig anfallende Verkehrsdaten zu bestimmten Zeitpunkten erteilt: für die zweite und jede weitere in dem Ersuchen verlangte Teilauskunft.....	10,00 €
303	Auskunft über gespeicherte Verkehrsdaten zu Verbindungen, die zu einer bestimmten Zieladresse hergestellt wurden, durch Suche in allen Datensätzen der abgehenden Verbindungen eines Betreibers (Zielwahlsuche): je Zieladresse	90,00 €
	Die Mitteilung der Standortdaten der Zieladresse ist mit abgegolten.	
304	Für die Auskunft muss auf Verkehrsdaten nach § 113b Abs. 2 bis 4 TKG zurückgegriffen werden: Die Pauschale 303 beträgt	110,00 €
305	Die Auskunft wird im Fall der Nummer 303 aufgrund eines einheitlichen Ersuchens auch oder ausschließlich für künftig anfallende Verkehrsdaten zu bestimmten Zeitpunkten erteilt: für die zweite und jede weitere in dem Ersuchen verlangte Teilauskunft	70,00 €
306	Auskunft über gespeicherte Verkehrsdaten für eine von der Strafverfolgungsbehörde benannte Funkzelle (Funkzellenabfrage)	30,00 €
307	Für die Auskunft muss auf Verkehrsdaten nach § 113b Abs. 2 bis 4 TKG zurückgegriffen werden: Die Pauschale 306 beträgt	35,00 €
308	Auskunft über gespeicherte Verkehrsdaten für mehr als eine von der Strafverfolgungsbehörde benannte Funkzelle: Die Pauschale 306 erhöht sich für jede weitere Funkzelle um	4,00 €

Nr.	Tätigkeit	Höhe
309	Auskunft über gespeicherte Verkehrsdaten für mehr als eine von der Strafverfolgungsbehörde benannte Funkzelle und für die Auskunft muss auf Verkehrsdaten nach § 113b Abs. 2 bis 4 TKG zurückgegriffen werden: Die Pauschale 306 erhöht sich für jede weitere Funkzelle um	5,00 €
310	Auskunft über gespeicherte Verkehrsdaten in Fällen, in denen lediglich Ort und Zeitraum bekannt sind: Die Abfrage erfolgt für einen bestimmten, durch eine Adresse bezeichneten Standort	60,00 €
311	Für die Auskunft muss auf Verkehrsdaten nach § 113b Abs. 2 bis 4 TKG zurückgegriffen werden: Die Pauschale 310 beträgt	70,00 €
	Die Auskunft erfolgt für eine Fläche:	
312	- Die Entfernung der am weitesten voneinander entfernten Punkte beträgt nicht mehr als 10 Kilometer: Die Pauschale 310 beträgt	190,00 €
313	- Die Entfernung der am weitesten voneinander entfernten Punkte beträgt mehr als 10 und nicht mehr als 25 Kilometer: Die Pauschale 310 beträgt	490,00 €
314	- Die Entfernung der am weitesten voneinander entfernten Punkte beträgt mehr als 25, aber nicht mehr als 45 Kilometer: Die Pauschale 310 beträgt ..... Liegen die am weitesten voneinander entfernten Punkte mehr als 45 Kilometer auseinander, ist für den darüber hinausgehenden Abstand die Entschädigung nach den Nummern 312 bis 314 gesondert zu berechnen.	930,00 €
	Die Auskunft erfolgt für eine Fläche und es muss auf Verkehrsdaten nach § 113b Abs. 2 bis 4 TKG zurückgegriffen werden:	
315	- Die Entfernung der am weitesten voneinander entfernten Punkte beträgt nicht mehr als 10 Kilometer: Die Pauschale 310 beträgt	230,00 €
316	- Die Entfernung der am weitesten voneinander entfernten Punkte beträgt mehr als 10 und nicht mehr als 25 Kilometer: Die Pauschale 310 beträgt	590,00 €
317	- Die Entfernung der am weitesten voneinander entfernten Punkte beträgt mehr als 25, aber nicht mehr als 45 Kilometer: Die Pauschale 310 beträgt ..... Liegen die am weitesten voneinander entfernten Punkte mehr als 45 Kilometer auseinander, ist für den darüber hinausgehenden Abstand die Entschädigung nach den Nummern 315 bis 317 gesondert zu berechnen.	1 120,00 €
318	Die Auskunft erfolgt für eine bestimmte Wegstrecke: Die Pauschale 310 beträgt für jeweils angefangene 10 Kilometer Länge	110,00 €
319	Die Auskunft erfolgt für eine bestimmte Wegstrecke und es muss auf Verkehrsdaten nach § 113b Abs. 2 bis 4 TKG zurückgegriffen werden: Die Pauschale 310 beträgt für jeweils angefangene 10 Kilometer Länge	130,00 €
320	Umsetzung einer Anordnung zur Übermittlung künftig anfallender Verkehrsdaten in Echtzeit: je Anschluss ..... Mit der Entschädigung ist auch der Aufwand für die Abschaltung der Übermittlung und die Mitteilung der den Anschluss betreffenden Standortdaten entgolten.	100,00 €
321	Verlängerung der Maßnahme im Fall der Nummer 320	35,00 €
	Leitungskosten für die Übermittlung der Verkehrsdaten in den Fällen der Nummern 320 und 321:	
322	- wenn die angeordnete Übermittlung nicht länger als eine Woche dauert ...	8,00 €
323	- wenn die angeordnete Übermittlung länger als eine Woche, jedoch nicht länger als zwei Wochen dauert	14,00 €

Nr.	Tätigkeit	Höhe
324	- wenn die angeordnete Übermittlung länger als zwei Wochen dauert: je angefangenen Monat	25,00 €
325	Übermittlung der Verkehrsdaten auf einem Datenträger	10,00 €.“

d) Nach Nummer 400 wird folgende Nummer 401 eingefügt:

Nr.	Tätigkeit	Höhe
„401	Im Fall der Nummer 400 muss auf Verkehrsdaten nach § 113b Abs. 2 bis 4 TKG zurückgegriffen werden: Die Pauschale 400 beträgt	110,00 €.“

e) Die bisherige Nummer 401 wird Nummer 402.

Artikel 5

Änderung des Strafgesetzbuches

Das Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), das zuletzt durch … geändert worden ist, wird wie folgt geändert:

1. In der Inhaltsübersicht wird nach der Angabe zu § 202c folgende Angabe eingefügt:

„§ 202d Datenhehlerei“.

2. Nach § 202c wird folgender § 202d eingefügt:

„§ 202d

Datenhehlerei

(1) Wer Daten (§ 202a Absatz 2), die nicht allgemein zugänglich sind und die ein anderer durch eine rechtswidrige Tat erlangt hat, sich oder einem anderen verschafft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, um sich oder einen Dritten zu bereichern oder einen anderen zu schädigen, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Die Strafe darf nicht schwerer sein als die für die Vortat angedrohte Strafe.

(3) Absatz 1 gilt nicht für Handlungen, die ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen. Dazu gehören insbesondere solche Handlungen von Amtsträgern oder deren Beauftragten, mit denen Daten ausschließlich der Verwertung in einem Besteuerungsverfahren, einem Strafverfahren oder einem Ordnungswidrigkeitenverfahren zugeführt werden sollen.“

3. § 205 wird wie folgt geändert:

a) In Absatz 1 Satz 2 wird die Angabe „und 202b“ durch ein Komma und die Angabe „202b und 202d“ ersetzt.

b) In Absatz 2 Satz 1 wird die Angabe „§§ 202a und 202b“ durch die Angabe „§§ 202a, 202b und 202d“ ersetzt.

Artikel 6

Einschränkung eines Grundrechts

Durch die Artikel 1 und 2 dieses Gesetzes wird das Fernmeldegeheimnis (Artikel 10 des Grundgesetzes) eingeschränkt.

Artikel 7

Inkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

Begründung

A. Allgemeiner Teil

I. Anlass und Ziel des Gesetzentwurfs

Die 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 erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (ABl. L 105 vom 13.4.2006, S. 54; im Folgenden: Richtlinie Vorratsdatenspeicherung) sah die Einführung einer Pflicht zur Speicherung solcher Daten vor. Sie wurde mit dem Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007 (BGBl. I S. 3198) in das deutsche Recht umgesetzt. Es sah in den §§ 113a und b TKG eine Verpflichtung für Diensteanbieter vor, Verkehrsdaten ihrer Teilnehmer für sechs Monate zu speichern und diese Daten auf Anforderung den Strafverfolgungsbehörden zur Verfügung zu stellen. Die Strafverfolgungsbehörden waren nach der Neuregelung des § 100g StPO u.a. bei einem Verdacht des Vorliegens einer Straftat von auch im Einzelfall erheblicher Bedeutung zum Abruf der Daten befugt.

Mit Urteil vom 2. März 2010 (1 BvR 256/08; BVerfGE 125, 260) hat das Bundesverfassungsgericht die §§ 113a und 113b des TKG und auch § 100g Absatz 1 Satz 1 der Strafprozessordnung (StPO), soweit danach Verkehrsdaten nach § 113a TKG erhoben werden durften, wegen Verstoßes gegen Artikel 10 Absatz 1 des GG für nichtig erklärt. Mit Urteil vom 8. April 2014 hat der Gerichtshof der Europäischen Union die dem Umsetzungsgesetz zugrundeliegende Richtlinie Vorratsdatenspeicherung wegen Verstoßes gegen Artikel 7 und 8 der Grundrechtecharta für unwirksam erklärt. Eine europarechtliche Pflicht zur gesetzlichen Einführung einer Pflicht der Erbringer öffentlich zugänglicher Telekommunikationsdienste, Verkehrsdaten für einen bestimmten Zeitraum zu speichern, besteht damit nicht mehr.

Die jetzige Gesetzeslage führt jedoch zu Unzulänglichkeiten bei der Strafverfolgungsvorsorge und bei der Gefahrenabwehr. Zwar können die Strafverfolgungsbehörden auf der Grundlage von § 100g Absatz 1 StPO bei Vorliegen eines Anfangsverdachts und entsprechender richterlicher Anordnung auf Verkehrsdaten Zugriff nehmen, die bei den Erbringern öffentlich zugänglicher Telekommunikationsdienste aus geschäftlichen Gründen zum Zeitpunkt der Anfrage noch gespeichert sind. Die Erbringer öffentlich zugänglicher Telekommunikationsdienste dürfen im Einzelnen im Telekommunikationsgesetz bezeichnete Verkehrsdaten nämlich auch nach Beendigung des einzelnen Kommunikationsvorgangs speichern, wenn sie diese für – im Einzelnen im TKG festgelegte – eigene Bedürfnisse benötigen (zum Beispiel Aufbau weiterer Verbindungen, Rechnungsstellung, Störungsbeseitigung oder Schutz vor belästigenden Anrufen, § 96 TKG). Da die Speicherpraxis der Erbringer öffentlich zugänglicher Telekommunikationsdienste sehr unterschiedlich ist, ist es jedoch derzeit vom Zufall abhängig, welche Daten bei einer Abfrage nach § 100g StPO abgerufen werden können.

Eine Änderung dieses Zustandes ist auch im Hinblick auf die Bedeutung einer effektiven Strafverfolgung angezeigt. Das Bundesverfassungsgericht hat wiederholt das verfassungsrechtliche Gebot einer effektiven Strafverfolgung hervorgehoben, das Interesse an einer möglichst vollständigen Wahrheitsermittlung im Strafverfahren betont und die wirksame Aufklärung gerade schwerer Straftaten als einen wesentlichen Auftrag eines rechtsstaatlichen Gemeinwesens bezeichnet (BVerfGE 129, 208 <260> mwN). Der Europäische Gerichtshof für Menschenrechte hat aus Artikel 8 der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten (EMRK) positive Pflichten für die Staa-

ten abgeleitet, das materielle Strafrecht in der Praxis durch effektive Ermittlung und Verfolgung anzuwenden (EGMR, Nr. 2872/02, 2. Dezember 2008 – K.U. v. Finnland). Auch der Gerichtshof der Europäischen Union hat die Bedeutung der Bekämpfung schwerer Kriminalität zur Gewährleistung der öffentlichen Sicherheit betont (EuGH-Urteil Digital Rights, C-293/12 und C-564/12, EuZW 2014, 459 <462>, Rn. 42).

Der Gesetzentwurf behebt die beschriebenen Unzulänglichkeiten in der Strafverfolgungsvorsorge und der Gefahrenabwehr. Durch die Speicherung der Verkehrsdaten für eine begrenzte Zeit werden zusätzliche Aufklärungsmöglichkeiten geschaffen, die der zunehmenden Bedeutung der Telekommunikation für die Vorbereitung und Begehung von Straftaten Rechnung tragen. Gleichzeitig wird der Gesetzentwurf Anforderungen des Artikels 10 Absatz 1 GG gerecht, wie sie das Bundesverfassungsgericht in dem oben genannten Urteil präzisiert hat. Eine vorsorglich anlasslose Datenspeicherung unterliegt sowohl hinsichtlich ihrer Begründung als auch ihrer Ausgestaltung, insbesondere auch in Bezug auf die vorgesehenen Verwendungszwecke, besonders strengen Anforderungen (BVerfGE 125, 260 <316 f.>).

Diese betreffen zum einen die Datensicherheit. Das Bundesverfassungsgericht hat ausgeführt, dass die Sicherheit der Daten sowohl bei der Aufbewahrung als auch bei der Übermittlung gewährleistet sein müsse; zudem bedürfe es effektiver Sicherungen zur Gewährleistung der Löschung der Daten. Die Verfassung gebe nicht detailgenau vor, welche Sicherheitsmaßgaben im Einzelnen geboten seien. Es müsse aber ein hoher Standard gewahrt werden, der sich an dem Stand der Technik orientiere und neue Erkenntnisse und Einsichten fortlaufend aufnehme. Es liege nahe, dass grundsätzlich eine getrennte Speicherung der Daten, eine anspruchsvolle Verschlüsselung, ein gesichertes Zugriffsregime unter Nutzung etwa des Vier-Augen-Prinzips sowie eine revisionssichere Protokollierung sichergestellt sein müssten. Die technische Konkretisierung des gesetzlich vorzugebenden Sicherheitsstandards könne der Gesetzgeber einer Aufsichtsbehörde anvertrauen. Der Gesetzgeber habe sicherzustellen, dass die Entscheidung über Art und Maß der zu treffenden Schutzvorkehrungen nicht letztlich unkontrolliert in den Händen der Anbieter liege. Verfassungsrechtlich geboten sei eine für die Öffentlichkeit transparente Kontrolle unter Einbeziehung des unabhängigen Datenschutzbeauftragten sowie ein ausgeglichenes Sanktionensystem, das auch Verstößen gegen die Datensicherheit ein angemessenes Gewicht beimesse.

Auch die Verwendung der Daten müsse verhältnismäßig ausgestaltet sein. Für die Strafverfolgung dürfe ein Abruf nur für den Fall eines durch bestimmte Tatsachen begründeten Verdachts einer schweren Straftat erfolgen, die auch im Einzelfall schwer wiege. Die zum Abruf berechtigenden Straftaten müsse der Gesetzgeber abschließend in Form eines Katalogs festlegen. Zudem sei gesetzlich zu gewährleisten, dass die Daten nach Übermittlung unverzüglich ausgewertet und, sofern sie für die Erhebungszwecke unerheblich seien, gelöscht würden. Eine Weitergabe der Daten an andere Stellen dürfe nur erfolgen, soweit sie zur Wahrnehmung von Aufgaben erfolge, derentwegen ein Zugriff auch unmittelbar zulässig wäre. Um dies zu gewährleisten müssten die vorsorglich anlasslos gespeicherten Daten besonders gekennzeichnet werden. Hinsichtlich des Umfangs der abzurufenden Daten habe der Gesetzgeber einen Gestaltungsspielraum. Verfassungsrechtlich sei es jedoch geboten, zumindest für einen engen Kreis von auf besondere Vertraulichkeit angewiesenen Telekommunikationsverbindungen ein grundsätzliches Übermittlungsverbot vorzusehen. Zu denken sei hier etwa an Verbindungen zu Anschlüssen von Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen, die grundsätzlich anonym bleibenden Anrufern ganz oder überwiegend telefonische Beratung in seelischen oder sozialen Notlagen anbieten und die selbst oder deren Mitarbeiter insoweit anderen Verschwiegenheitsverpflichtungen unterliegen (vgl. § 99 Absatz 2 TKG).

Schließlich müsse der Gesetzgeber hinreichende Vorkehrungen zur Transparenz der Datenverwendung treffen. Soweit dies möglich sei, müsse die Verwendung der Daten offen erfolgen. Ansonsten bedürfe es grundsätzlich zumindest nachträglich einer Benachrichti-

gung der Betroffenen. Unterbleibe ausnahmsweise auch diese, bedürfe die Nichtbenachrichtigung einer richterlichen Entscheidung. Ein effektiver Rechtsschutz setze voraus, dass der Abruf der Daten unter einem Richtervorbehalt stehe und es ein Rechtsschutzverfahren zur nachträglichen Kontrolle der Verwendung der Daten gebe. Wirksame Sanktionen bei Rechtsverletzungen seien ein weiteres notwendiges Element einer verhältnismäßigen Regelung.

Neben den Vorgaben des Grundgesetzes sind aber auch die Vorgaben der Grundrechtecharta, wie sie der Gerichtshof der Europäischen Union in seinem Urteil vom 8. April 2014 zur Richtlinie 2006/24/EG präzisiert hat, zu beachten. Nach Artikel 51 Absatz 1 der Grundrechtecharta sind die Mitgliedstaaten bei der Durchführung des Rechts der Union an die Grundrechtecharta gebunden. Das ist der Fall, wenn eine nationale Regelung in den Anwendungsbereich des Unionsrechts fällt. Die grundsätzliche Anwendbarkeit der Grundrechtecharta für nationale Regelungen zur Vorratsdatenspeicherung folgt aus der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation): Nachdem der Gerichtshof der Europäischen Union die Richtlinie 2006/24/EG für ungültig erklärt hat, ist für nationale Regelungen zur Speicherung von Telekommunikationsdaten der Anwendungsbereich des Artikels 15 Absatz 1 der Richtlinie 2002/58/EG wieder eröffnet. Danach sind nationale Regelungen zur Vorratsdatenspeicherung zur Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten zulässig, wenn sie den Anforderungen des Artikels 6 Absatz 1 und 2 EUV genügen. Aus Artikel 15 Absatz 1 folgt demnach die Bindung etwaiger nationaler Regelungen an die Charta. Darüber hinaus bewirkt die Anwendbarkeit des Artikels 15, dass nationale Regelungen in den Geltungsbereich des Unionsrechts fallen.

Das Urteil des Gerichtshofs der Europäischen Union zeigt auf, warum die Vorratsdatenspeicherung, wie sie in der Richtlinie 2006/24/EG vorgesehen war, nicht mit der Grundrechtecharta vereinbar ist. Der Gerichtshof kritisiert, dass die Richtlinie in umfassender Weise alle Personen, elektronischen Kommunikationsmittel und Verkehrsdaten betreffe, ohne irgendeine Differenzierung oder Einschränkung aufgrund des Ziels der Verfolgung schwerer Straftaten vorzunehmen. Sie gelte etwa auch für Personen, deren Kommunikationsvorgänge nach den nationalen Rechtsvorschriften dem Berufsgeheimnis unterliegen. Außerdem enthalte die Richtlinie kein objektives Kriterium, das es ermögliche, den Zugang nationaler Behörden zu den Daten und deren Nutzung auf solche schwerwiegenden Fälle zu beschränken, die einen Eingriff rechtfertigen, sondern überlasse dies den Mitgliedstaaten. Die Richtlinie sehe keinen Mechanismus für eine vorherige Kontrolle des Zugriffs nationaler Behörden auf die gespeicherten Daten durch Gerichte oder unabhängige Verwaltungsstellen vor. Die Richtlinie sehe zudem eine Speicherdauer von mindestens sechs Monaten vor, ohne dass eine Unterscheidung anhand der Datenkategorie nach Maßgabe ihres etwaigen Nutzens für das verfolgte Ziel oder anhand der betroffenen Personen getroffen werde. Es fehle an objektiven Kriterien, die gewährleisteten, dass die zwischen sechs und 24 Monaten liegende Speicherfrist auf das Notwendigste beschränkt werde. Zudem biete die Richtlinie keine hinreichenden Garantien, um die gespeicherten Daten hinreichend vor Missbrauchsrisiken zu schützen. Stattdessen gestatte sie es den Erbringern öffentlich zugänglicher Telekommunikationsdienste, bei der Bestimmung des angewandten Sicherheitsniveaus wirtschaftliche Kriterien zu berücksichtigen. Schließlich rügt der Gerichtshof, dass die Richtlinie keine Speicherung der Daten im Unionsgebiet vorschreibe, so dass die Einhaltung der unionsrechtlichen Datenschutzerfordernisse nicht vollständig gewährleistet werden könne.

Soweit teilweise die Auffassung vertreten wird, der Gerichtshof der Europäischen Union halte eine anlasslose Speicherung von Verkehrsdaten per se für mit der Grundrechtecharta unvereinbar, kann dem nicht gefolgt werden. Die der Prüfung des Gerichtshofs der Europäischen Union zugrundliegende Richtlinie 2006/24/EG weist eine Vielzahl von Kritikpunkten auf, die in ihrer Gesamtbetrachtung die Unverhältnismäßigkeit der Vorratsdaten-

speicherung nach der Richtlinie 2006/24/EG begründet haben. Vor allem die Kombination der umfassenden Datenspeicherung für einen Zeitraum zwischen sechs und 24 Monaten ohne Differenzierungsmöglichkeit für Datenarten oder die Zwecke der Speicherung führen nach dem Urteil des Gerichtshofs zu einer unverhältnismäßigen Regelung in der Richtlinie 2006/24/EG. Zudem ist zu berücksichtigen, dass die Richtlinie Vorratsdatenspeicherung ausschließlich Regelungen zur Speicherung der Verkehrsdaten enthielt; die Regelung der Abrufvoraussetzungen war mangels einer unionsrechtlichen Kompetenzgrundlage den Mitgliedstaaten vorbehalten (Artikel 4 der Richtlinie). De facto sah die Richtlinie demnach eine Sammlung von personenbezogenen Daten auf Vorrat zu noch nicht bestimmbaren Zwecken vor. Eine solche Datensammlung hält auch das Bundesverfassungsgericht für unzulässig (BVerfGE 125, 260 <320 f.>). Die Speicherung kann der Entscheidung zufolge aber verhältnismäßig und damit zulässig sein, wenn sie zu bestimmten Zwecken erfolgt und in eine dem Eingriff adäquate gesetzliche Ausgestaltung eingebettet ist. Die verhältnismäßige Ausgestaltung der Regelungen zur Verwendung der Daten wirke auf die Verfassungsmäßigkeit schon der Speicherung als solcher zurück. Vor diesem Hintergrund wird das Urteil des Gerichtshofs der Europäischen Union so verstanden, dass bei einer Differenzierung der zu speichernden Daten und zugleich einer Reduzierung des Datenkranzes, bei der konkreten und restriktiven Benennung der Speicher- und Verwendungszwecke, der erheblichen Verkürzung des Speicherzeitraums sowie bei der Schaffung zusätzlicher, sachlicher und technischer Voraussetzungen eine Speicherung von Telekommunikationsdaten zur Strafverfolgungsvorsorge und zur Gefahrenabwehr unionsgrundrechtskonform ausgestaltet werden kann.

Den genannten verfassungs- und europarechtlichen Vorgaben wird der Gesetzentwurf dadurch gerecht, dass er eine möglichst begrenzte Speicherpflicht mit strengen Abrufregelungen kombiniert. Er sieht einerseits eine zehnwöchige Speicherung von genau bezeichneten Verkehrsdaten, bei Standortdaten sogar nur eine vierwöchige Speicherung, bei den Erbringern öffentlich zugänglicher Telekommunikationsdienste zu Zwecken der Strafverfolgungsvorsorge und zur Gefahrenabwehr und, ermöglicht den Abruf der Daten durch staatliche Stellen andererseits nur unter sehr engen Voraussetzungen.

Schon die Verpflichtung zur Speicherung wird – entsprechend den Anforderungen des Gerichtshofs der Europäischen Union, auf das absolut Notwendige beschränkt. Daten von Diensten der elektronischen Post sind vollständig von der Speicherpflicht ausgenommen. Zum Schutz des besonderen Vertrauensverhältnisses sind Verkehrsdaten, die sich auf Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen beziehen, die grundsätzlich anonym bleibenden Anrufern ganz oder überwiegend telefonische Beratung in seelischen oder sozialen Notlagen anbieten und die selbst oder deren Mitarbeiter insoweit besonderen Verschwiegenheitsverpflichtungen unterliegen, grundsätzlich von der Speicherpflicht ausgenommen. Detaillierte und normenklare Regeln begrenzen die Verwendung der Daten und gewährleisten ihre Sicherheit.

Auch die Erhebung der verpflichtend gespeicherten Verkehrsdaten ist eng begrenzt. Ein Abruf dieser Daten ist nur zur Verfolgung der in § 100g Absatz 2 StPO-E aufgeführten besonders schweren Straftaten zulässig, die auch im Einzelfall besonders schwer wiegen müssen. Im Hinblick auf die hohe Grundrechtsrelevanz des Abrufs verpflichtend gespeicherter Daten ist der Katalog des § 100g Absatz 2 StPO-E im Vergleich zu dem nach der vorhergehenden Regelung (Straftaten von erheblicher Bedeutung) deutlich reduziert. Damit wird dem Umstand Rechnung getragen, dass der Gerichtshof der Europäischen Union die Speicherung von Verkehrsdaten nur für zulässig gehalten hat, soweit die Bekämpfung schwerer Kriminalität in Rede steht. Der Katalog enthält Straftaten, die der Bekämpfung des Terrorismus oder dem Schutz höchstpersönlicher Rechtsgüter, insbesondere Leib, Leben, Freiheit und sexuelle Selbstbestimmung, dienen. Außerdem sind besonders schwere Straftaten umfasst, bei denen die gespeicherten Verkehrsdaten nach kriminalistischer Erfahrung besonders wertvolle Dienste leisten können.

Darüber hinaus ist festgelegt, dass die Strafverfolgungsbehörden Verkehrsdaten in Bezug auf alle nach § 53 StPO zeugnisverweigerungsberechtigten Personen nicht erheben dürfen. Zufallsfunde unterliegen einem Verwertungsverbot. Für den Abruf der Daten ist ein umfassender Richtervorbehalt vorgesehen; eine Eilkompetenz der Staatsanwaltschaft besteht nicht. Zudem ist die Datenerhebung als offene Maßnahme ausgestaltet. Die betroffenen Personen sind grundsätzlich vor dem Abruf der Daten zu benachrichtigen. Die Benachrichtigung kann ausnahmsweise zurückgestellt werden; dies erfordert jedoch eine richterliche Entscheidung.

Zum Zwecke der Gefahrenabwehr ist die Erhebung der Daten ebenfalls nur unter engen Voraussetzungen möglich; der Abruf muss der Abwehr schwerster Gefahren, das heißt Gefahren für Leib, Leben oder Freiheit oder für den Bestand des Bundes oder eines Landes dienen.

Die Erhebung der besonders sensiblen Standortdaten wird im Vergleich zum geltenden Recht stark eingeschränkt. Auf zu geschäftlichen Zwecken gespeicherte Verkehrsdaten darf – anders als bislang – zur Ermittlung des Aufenthaltsortes nicht zurückgegriffen werden; eine Erhebung von Standortdaten ist nur unter den strengen Voraussetzungen des Absatzes 2 zulässig.

Mit dem Gesetzentwurf werden auch die bislang in § 100g Absatz 2 Satz 2 StPO geregelten Voraussetzungen zur Funkzellenabfrage präzisiert. Durch Funkzellenabfragen werden regelmäßig unvermeidbar Verkehrsdaten Dritter, namentlich solcher Personen erhoben, die – ohne Beschuldigte oder Nachrichtenmittler zu sein – in der abgefragten Funkzelle mit ihrem Mobiltelefon kommuniziert haben. Verkehrsdaten Unbeteiligter dürfen nicht über das zur Strafverfolgung unerlässliche Maß hinaus erhoben werden. Zu diesem Zweck wird die Funkzellenabfrage legal definiert und die strenge Subsidiaritätsklausel des § 100a Absatz 1 Nummer 3 StPO übernommen. Außerdem muss die Funkzellenabfrage wie bisher die zu erfassende Telekommunikation räumlich und zeitlich eng begrenzt und hinreichend bestimmt bezeichnen. Damit wird die Erstellung von Bewegungsprofilen unbescholtener Bürgerinnen und Bürger wirksam verhindert.

Gleichbedeutend neben dem Anliegen, in einer immer stärker von Informations- und Kommunikationstechnologie geprägten Gesellschaft effektive Strafverfolgung zu ermöglichen, steht der strafrechtliche Schutz von Informationssystemen und der in ihnen gespeicherten Daten vor Angriffen und Ausspähungen. Dieser Schutz muss sich auch gegen Tathandlungen richten, mit denen ausgespähte, abgefangene oder in anderer Weise rechtswidrig erlangte Daten gehandelt werden und damit die durch die Vortat erfolgte Beeinträchtigung der formellen Verfügungsbefugnis des Berechtigten über seine Daten fortgesetzt und vertieft wird.

Das Ausspähen und Abfangen von Daten sowie die Vorbereitung dieser Taten sind bereits heute nach den §§ 202a, 202b und 202c des Strafgesetzbuches (StGB) unter Strafe gestellt, die die entsprechenden Vorgaben des von der Bundesrepublik Deutschland ratifizierten Übereinkommens des Europarates über Computerkriminalität vom 23. November 2001, des Rahmenbeschlusses 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme (ABl. L 69 vom 16.3.2005, S. 67) sowie der Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12. August 2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates (ABl. L 218 vom 14.8.2013, S. 8) umsetzen. Zur vollständigen Umsetzung der Richtlinie über Angriffe auf Informationssysteme ist darüber hinaus eine Erhöhung des Strafrahmens von § 202c StGB (Vorbereitung des Ausspähens und Abfangens von Daten) erforderlich, die durch das von der Bundesregierung vorgelegte Gesetz zur Bekämpfung der Korruption (Bundestagsdrucksache 18/4350) erfolgen soll.

Auch der Handel mit Daten, die durch Ausspähen und Abfangen bzw. durch andere rechtswidrige Taten erlangt worden sind, kann schon heute bestimmten Straftatbeständen

unterfallen. Die geltenden strafrechtlichen Regelungen sind aber unzureichend und weisen Schutzlücken auf, die durch einen eigenständigen Straftatbestand der Datenhehlerei geschlossen werden sollen.

Nach geltendem Recht kommt beim An- und Verkauf von gestohlenen Daten insbesondere eine Strafbarkeit nach § 202c Absatz 1 Nummer 1 StGB (Vorbereiten des Ausspähens und Abfangens von Daten) in Betracht. Danach macht sich strafbar, wer Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten ermöglichen, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wenn er dadurch eine Straftat des Ausspähens oder Abfangens von Daten (§§ 202a, 202b StGB) vorbereitet. Die Strafbarkeit erfasst damit auch den Handel mit bestimmten Daten, die aus strafbaren Handlungen erlangt worden sind. Sie ist aber beschränkt auf Passwörter und sonstige Sicherungscodes, die den Zugang zu Daten ermöglichen, und erfasst damit beispielsweise den Handel mit Konto- und Kreditkartendaten jedenfalls dann nicht, wenn diese Daten unmittelbar zur Zahlung eingesetzt werden sollen, ohne dass dem Täter dabei Zugang zu Daten, die nicht für ihn bestimmt sind und die gegen unberechtigten Zugang besonders gesichert sind, verschafft wird (Golla/von zur Mühlen, JZ 2014, 668, 672). Auch beim Vorliegen von Passwörtern und Sicherungscodes scheidet eine Strafbarkeit nach der Vorschrift aus, wenn der Täter die Daten zum Weiterverkauf erwirbt und noch keinen hinreichend konkreten Vorsatz hinsichtlich der Vorbereitung einer Tat nach §§ 202a, 202b StGB hat (vgl. Leipziger Kommentar/Hilgendorf, 12. Auflage, § 202c Rz. 26ff.).

Auch eine Beteiligung des Täters der Datenhehlerei an den vorangegangenen Straftaten des Ausspähens oder Abfangens von Daten nach den §§ 202a, 202b StGB scheidet aus, wenn diese Straftaten, was regelmäßig der Fall sein wird, zum Zeitpunkt des Erwerbs der Daten bereits beendet sind. Ebenso wenig kommt eine Beteiligung an einer möglicherweise nachfolgenden strafbaren Nutzung der Daten, wie etwa einem Computerbetrug (§ 263a StGB) und einer Fälschung beweiserheblicher Daten (§ 269 StGB), in Betracht, solange der Täter die Daten lediglich erwirbt und weiterveräußert, ohne dass es zu einem späteren strafbaren Gebrauch durch den Aufkäufer gekommen ist bzw. dies festgestellt werden kann.

Nach dem Bundesdatenschutzgesetz (BDSG) ist es strafbar, unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, zu erheben, zu verarbeiten, abzurufen, sich oder einem anderen aus automatisierten Verarbeitungen oder nicht automatisierten Dateien zu verschaffen, wenn die Tat gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, begangen wird (§ 44 in Verbindung mit § 43 Absatz 2 Nummer 1 und 3 BDSG). Die Strafbarkeit besteht unabhängig davon, ob die Daten zuvor durch eine rechtswidrige Tat erlangt worden sind. Sie kann daher auch nicht den besonderen Unrechtsgehalt des Handels mit Daten erfassen, die von einem Vortäter ausgespäht oder abgefangen oder sonst durch eine rechtswidrige Tat erlangt worden sind. Bei der Datenhehlerei macht sich der Täter die durch die Vortat erfolgte strafwürdige Rechtsverletzung zunutze und handelt damit verwerflicher als bei einem lediglich unbefugten Umgang mit persönlichen Daten wie er vom BDSG- erfasst wird. Der anders geartete und dahinter zurückbleibende Unrechtsgehalt der Straftaten nach dem Bundesdatenschutzgesetz schlägt sich insbesondere in einer geringen Strafandrohung (Freiheitsstrafe bis zu zwei Jahren) und in der Ausgestaltung der Norm als absolutes Antragsdelikt nieder, wobei neben dem datenschutzrechtlich Betroffenen auch die verantwortliche Stelle sowie die Datenschutzaufsichtsbehörden antragsbefugt sind. Beides wird dem Unrechtsgehalt der Datenhehlerei nicht gerecht. Insbesondere bei Fällen von massiven Angriffen auf Informationssysteme mit einer Vielzahl von Verletzten, die individuell aber jeweils nur geringfügig in ihren Rechtsgütern beeinträchtigt sind und daher möglicherweise von einer nach dem Bundesdatenschutzgesetz erforderlichen Strafantragstellung absehen, kann der auf den Angriff folgende massenhafte Handel mit den ausgespähten Daten strafrechtlich nicht adäquat verfolgt und geahndet werden. Die Vorschriften des Bundesdatenschutzgesetzes gelten zudem nur für personenbezogene Da-

ten, also für Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (§ 3 Absatz 1 BDSG), und erfassen beispielsweise nicht den Handel mit Daten juristischer Personen. Beim Handel mit nicht personenbezogenen Daten kommt zwar eine Strafbarkeit wegen des Verrats von Geschäfts- und Betriebsgeheimnissen nach der Vorschrift des § 17 des Gesetzes gegen den unlauteren Wettbewerb (UWG) in Betracht. Die Norm gilt – ihrem Schutzzweck entsprechend – jedoch ebenfalls nicht umfassend.

Nach § 17 Absatz 2 Nummer 2 UWG macht sich strafbar, wer ein Geschäfts- oder Betriebsgeheimnis, das er sich unbefugt verschafft oder gesichert hat, unbefugt verwertet oder jemandem mitteilt. Geschäfts- und Betriebsgeheimnisse liegen nur dann vor, wenn eine Beziehung des Geheimnisses zum Geschäftsbetrieb besteht, die betreffenden Daten nicht offenkundig sind und der Geschäftsinhaber einen Geheimhaltungswillen und ein Geheimhaltungsinteresse an diesen Daten hat. Daran kann es beispielsweise bei Daten von Kreditkarten fehlen, die im Rahmen des täglichen Geschäftsverkehrs verwendet werden. Der An- und Verkauf solcher Daten, die zuvor ausgespäht oder durch eine andere rechtswidrige Tat erlangt worden sind, ist in diesen Fällen nicht nach § 17 UWG strafbar.

Aufgrund der bestehenden Strafbarkeitslücken hat sich 2012 auch der 69. Deutsche Juristentag für die Einführung eines Straftatbestands zur „Datenhehlerei“ ausgesprochen. Ein entsprechender Gesetzentwurf wurde vom Bundesrat in den Deutschen Bundestag eingebracht (Bundestagsdrucksache 18/1288). Der vorliegende Regelungsvorschlag ist hieran angelehnt.

Als Hehlerware stehen Daten insbesondere aufgrund von Straftaten zur Verfügung, bei denen Täter in fremde Computersysteme eindringen und sich Zugang zu Daten verschaffen (sogenanntes Hacking, § 202a StGB) oder bei denen Daten bei ihrer Übermittlung abgefangen werden (§ 202b StGB). Die Vortäter umgehen dabei beispielsweise mit Hilfe technischer Mittel den Passwortschutz oder nutzen Sicherheitslücken aus, um unerkannt Schadsoftware aufzuspielen. Sie können durch solche Angriffe auf Informationssysteme etwa von Erbringern von Telekommunikationsdienstleistungen, sozialen Netzwerken oder E-Mail-Diensten und von Banken enorme Mengen an dort gespeicherten Daten erbeuten, die von ihnen anschließend nicht unbedingt selbst zur Begehung weiterer Straftaten eingesetzt, sondern Dritten zum Verkauf angeboten werden. Daten können außerdem durch eine nach § 269 StGB (Fälschung beweiserheblicher Taten) strafbare Täuschung des Berechtigten erlangt werden, etwa durch das sogenannte Phishing, bei dem der Nutzer einen vermeintlich vertrauenswürdigen Kontakt, der – in der Regel mittels E-Mail – eine gefälschte Identität vorgibt, vertrauliche Zugangsdaten wie Benutzername, Passwörter, PIN- und TAN-Nummern übermittelt (Sieber, Gutachten C zum 69. Deutschen Juristentag, 2012, S. 20). Der Handel mit den so erbeuteten Daten erfolgt auch durch internationale, arbeitsteilig strukturierte Gruppen, die dafür spezielle – meist nicht öffentlich zugängliche – Diskussionsforen und Chat-Dienste nutzen (Sieber, Gutachten C zum 69. Deutschen Juristentag, 2012, S. 22).

Ausweislich der Polizeilichen Kriminalstatistik des Bundeskriminalamtes und der Strafverfolgungsstatistik des Statistischen Bundesamtes ist nach einem vorausgegangen erheblichen Anstieg in den letzten Jahren von einer nahezu gleichbleibend hohen Zahl der Straftaten gegen die Integrität, Vertraulichkeit und Verfügbarkeit informationstechnischer Systeme auszugehen (siehe auch Bundeskriminalamt, Bundeslagebild Cybercrime 2013), durch die der Schwarzmarkt für den Handeln mit gestohlenen Daten versorgt wird.

Mit dem Erwerb und der Weitergabe gestohlener Daten müssen die Täter nicht zwingend nur finanzielle Interessen verfolgen. Tatmotiv kann auch eine Schädigung Dritter sein, etwa durch Angriffe auf Informationssysteme.

Der neue Straftatbestand der Datenhehlerei schützt das formelle Datengeheimnis, das durch die Vortat bereits verletzt worden ist, vor einer Aufrechterhaltung und Vertiefung

dieser Verletzung. Bereits mit der Erlangung der Daten durch den Vortäter sind die formelle Verfügungsbefugnis desjenigen, der aufgrund seines Rechts an dem gedanklichen Inhalt über eine Weitergabe und Übermittlung der Daten entscheidet (Münchener Kommentar/Graf, 2. Auflage, § 202a Rz. 2), und damit das Interesse an der Aufrechterhaltung des Herrschaftsverhältnisses über eine Information (Leipziger Kommentar/Hilgendorf, 12. Auflage, § 202a Rz. 6) beeinträchtigt worden. Dem Berechtigten wird mit der Vortat die ihm zustehende Entscheidung, wem seine Daten zugänglich sein sollen, aus der Hand genommen.

Diese Rechtsgutsverletzung wird aufrechterhalten und vertieft, wenn sich im Anschluss daran ein Dritter die gestohlenen Daten verschafft und damit die Daten weiterverbreitet werden. Mit dem Datenhehler erhält eine weitere Person die Möglichkeit, über die Zugänglichmachung der Daten anstelle des Berechtigten zu entscheiden. Zugleich kann es für den Berechtigten schwieriger werden, seine Daten nachzuverfolgen und die alleinige Verfügungsbefugnis über sie zurückzugewinnen.

Nach der Rechtsprechung des Bundesgerichtshofs verletzt die Sachhehlerei nicht nur das durch die Vortat bereits verletzte Eigentum oder Vermögen, indem sie den durch die Vortat herbeigeführten rechtswidrigen Vermögenszustand aufrechterhält und befestigt, sondern auch vor allem allgemeine Sicherheitsinteressen, die durch den von der Hehlerei geschaffenen Anreiz zur Verübung von Vortaten beeinträchtigt werden (BGH, Beschluss vom 25. Juli 1996 - 4 StR 202/96, BGH St 7, 142, Beschluss vom 20. Dezember 1954 - GSSt 1/5; vgl. Münchener Kommentar, 2. Auflage, § 259 Rz. 3). Dies gilt entsprechend für die Datenhehlerei. Hieraus ergibt sich einerseits die Beschränkung des Hehlereistraftatbestands auf rechtswidrige Vortaten unter Ausschluss von sonstigen (nicht strafbaren) rechtswidrigen Handlungen des Vortäters. Zugleich erklärt sich daraus die Einbeziehung auch solcher Vortaten, die sich im Einzelfall gegen die formelle Verfügungsbefugnis des Berechtigten richten, deren Strafbarkeit (anders als beispielsweise bei den §§ 202a, 202b StGB) aber nicht auf einer Verletzung des Rechtsguts der formellen Verfügungsbefugnis über Daten beruht, sondern die andere Rechtsgüter schützen.

Strafwürdig ist die Hehlerei mit gestohlenen Daten allerdings nur, wenn es sich um Daten handelt, die nicht allgemein zugänglich sind. Daten können beliebig häufig vervielfältigt werden und dem parallelen Zugriff beliebig vieler Personen ausgesetzt sein (Golla/von zur Mühlen, JZ 2014, 668. 671). Die vom Vortäter erlangten Daten werden dem Berechtigten in der Regel weder durch die Vortat noch durch die anschließende Hehlereihandlung vollständig entzogen, sondern stehen ihm weiter zur Verfügung. Seine formelle Verfügungsbefugnis wird durch einen An- und Verkauf der ihm gestohlenen Daten nicht in strafwürdiger Weise beeinträchtigt, wenn es sich um Daten handelt, die aus allgemein zugänglichen Quellen entnommen werden können und bei denen die Entscheidung, wem die Daten zugänglich sein sollen, daher nicht mehr alleine in der Hand des Berechtigten liegt.

II. Die wesentlichen Änderungen

Der Gesetzentwurf sieht im Wesentlichen Änderungen in der Strafprozessordnung (Artikel 1), des Telekommunikationsgesetzes (Artikel 2) und des Strafgesetzbuches (Artikel 5) vor.

1. Neuregelung der Erhebung von Verkehrsdaten nach § 100g StPO-E

Die Vorgaben des Bundesverfassungsgerichts sowie des Gerichtshofs der Europäischen Union in den Entscheidungen zur Vorratsdatenspeicherung machen eine grundlegende Neuregelung des § 100g StPO erforderlich. Bei dieser Gelegenheit werden auch die Voraussetzungen der Funkzellenabfrage präzisiert.

Während in Absatz 1 die Erhebung von Verkehrsdaten geregelt wird, die aus geschäftlichen Gründen bei den Erbringern öffentlich zugänglicher Telekommunikationsdienste ge-

speichert werden, legt Absatz 2 fest, unter welchen Voraussetzungen die nunmehr durch die neue Speicherpflicht gespeicherten Daten erhoben werden dürfen. Diese Differenzierung hat das Bundesverfassungsgericht ausdrücklich verlangt (BVerfGE 125, 260 <328>):

„Die Verwendung der durch eine anlasslos systematische Speicherung praktisch aller Telekommunikationsverkehrsdaten gewonnenen Datenbestände unterliegt dementsprechend besonders hohen Anforderungen. Insbesondere ist diese nicht in gleichem Umfang verfassungsrechtlich zulässig wie die Verwendung von Telekommunikationsverkehrsdaten, die die Erbringer öffentlich zugänglicher Telekommunikationsdienste in Abhängigkeit von den jeweiligen betrieblichen und vertraglichen Umständen – von den Kunden teilweise beeinflussbar – nach § 96 TKG speichern dürfen. Angesichts der Unausweichlichkeit, Vollständigkeit und damit gesteigerten Aussagekraft der über sechs Monate systematisch vorsorglich erhobenen Verkehrsdaten hat ihr Abruf ein ungleich größeres Gewicht."

Die Erhebung der nach § 113b TKG-E gespeicherten Verkehrsdaten soll nach Maßgabe des § 100g Absatz 2 StPO-E nur unter sehr engen Voraussetzungen möglich sein, nämlich zur Verfolgung besonders schwerer, in § 100g Absatz 2 Satz 2 StPO-E im Einzelnen benannter Straftaten, die auch im Einzelfall besonders schwer wiegen müssen. Der Katalog des § 100g Absatz 2 StPO-E ist dabei im Vergleich zu dem nach der vorhergehenden Regelung deutlich reduziert.

Die Erhebung von gespeicherten Standortdaten ist besonders sensibel, weil aus ihnen Bewegungsprofile erstellt werden können. Sie wird deshalb nur nach Absatz 2 unter den dort geregelten strengen Voraussetzungen zugelassen. In Absatz 1 wird die Erhebung von aus geschäftlichen Gründen gespeicherten Standortdaten grundsätzlich ausgeschlossen, indem die Ermittlung des Aufenthaltsortes des Beschuldigten nicht mehr zu den zulässigen Zwecken einer Verkehrsdatenerhebung nach dieser Vorschrift gehört. Die Erhebung von Standortdaten in Echtzeit greift hingegen nicht auf gespeicherte Daten zurück und ist zur Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsortes des Beschuldigten unter den Voraussetzungen des Absatzes 1 Satz 1 Nummer 1 wie bisher zulässig.

Bei der Erhebung von Verkehrsdaten sind in der Begründung ihrer Anordnung oder Verlängerung die wesentlichen Erwägungen zur Verhältnismäßigkeit gesondert darzulegen (§ 101a Absatz 1 StPO-E). Dies gilt auch für Funkzellenabfragen, die im neuen Absatz 3 legal definiert werden.

2. Änderungen im Telekommunikationsgesetz

§ 113a bestimmt den Kreis der zur Speicherung von Verkehrsdaten Verpflichteten und sieht aus Gründen der Verhältnismäßigkeit eine Entschädigungsregelung vor, wenn die Speicherpflicht zu unbilligen Härten führen würde.

In § 113b TKG-E wird die Speicherung von genau bezeichneten Verkehrsdaten angeordnet. Dabei wird hinsichtlich der Speicherdauer differenziert. Während die Verbindungsdaten für zehn Wochen zu speichern sind, ist die Speicherung der besonders sensiblen Standortdaten auf vier Wochen beschränkt.

Im Übrigen dienen die Änderungen im Telekommunikationsgesetz im Wesentlichen der Umsetzung der Vorgaben des Bundesverfassungsgerichts und des Gerichtshofes der Europäischen Union in ihren Urteilen zur Vorratsdatenspeicherung und regeln dementsprechend die Einzelheiten zu den Speicherpflichten, zur Verwendung und Gewährleistung der Sicherheit der Daten sowie zur Protokollierung der Zugriffe auf die Daten. Zudem werden Einzelheiten für den von der Bundesnetzagentur zu erstellenden Anforderungskatalog der technischen Vorkehrungen und sonstigen Schutzmaßnahmen und für das von den verpflichteten Unternehmen zu erstellende Sicherheitskonzept geregelt.

3. Änderungen im Strafgesetzbuch

Der Entwurf sieht die Einführung eines neuen Straftatbestands der Datenhehlerei (§ 202d StGB-E) vor. Danach soll sich strafbar machen, wer nicht öffentlich zugängliche Daten, die ein anderer durch eine rechtswidrige Tat erlangt hat, sich oder einem anderen verschafft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, um sich oder einen Dritten zu bereichern oder einen anderen zu schädigen. Die Tat soll mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bedroht werden, wobei die Strafe nicht schwerer sein darf als die für die Vortat angedrohte Strafe.

Die Tat soll nur auf Antrag verfolgt werden, es sei denn, dass die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält (§ 205 Absatz 1 Satz 2 StGB-E).

Als Folgeänderungen sollen die Regelungen der Strafprozessordnung, die sich auf Anschlussdelikte wie insbesondere die Hehlerei beziehen, auf den neuen Straftatbestand der Datenhehlerei erstreckt werden.

III. Gesetzgebungskompetenz

Die Gesetzgebungskompetenz des Bundes folgt aus Artikel 74 Absatz 1 Nummer 1 GG (gerichtliches Verfahren, Strafrecht) sowie aus Artikel 73 Absatz 1 Nummer 7 GG (Telekommunikation). Bei der Einführung der §§ 113a bis 113g im Telekommunikationsgesetz handelt es sich nicht um Vorschriften, die eine Zustimmungsbedürftigkeit des Gesetzes nach Artikel 87f Absatz 1 GG auslösen würden. Sie betreffen nicht die „flächendeckend angemessene und ausreichende Dienstleistung“ im Sinne des Artikels 87f Absatz 1 GG.

IV. Vereinbarkeit mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen, die die Bundesrepublik Deutschland abgeschlossen hat

Der Gesetzentwurf ist mit europäischem Recht und völkerrechtlichen Verträgen, die die Bundesrepublik Deutschland abgeschlossen hat, vereinbar.

V. Gesetzesfolgen

1. Rechts- und Verwaltungsvereinfachung

Durch die gesetzliche Regelung einer Speicherpflicht für Verkehrsdaten ist davon auszugehen, dass die Erhebung von Verkehrsdaten häufiger erfolgreich sein wird, als dass gegenwärtig der Fall ist; dies gilt auch für Bestandsdatenabfragen.

2. Nachhaltigkeitsaspekte

Der Gesetzentwurf steht im Einklang mit den Leitgedanken der Bundesregierung zur nachhaltigen Entwicklung im Sinne der Nationalen Nachhaltigkeitsstrategie. Die beabsichtigten Regelungen begrenzen die Einschränkung grundrechtlich geschützter Interessen der Bürgerinnen und Bürger auf das zur Sicherung der Belange der Strafverfolgung unabdingbare Maß und tragen gleichzeitig den wesentlichen Bedürfnissen der Strafverfolgungsbehörden angemessen Rechnung. Der Gesetzentwurf dient darüber hinaus der Verbesserung der Bekämpfung von Delikten im Zusammenhang mit dem Handel illegal erlangter Daten und damit der Bekämpfung von Kriminalität (Nachhaltigkeitsindikator 15). Wegen der erheblichen sozialen und wirtschaftlichen Bedeutung der Datensicherheit ist dem rechtswidrigen Handel mit illegal erlangten Daten auch mit den Mitteln des Strafrechts entgegenzutreten.

3. Haushaltsausgaben ohne Erfüllungsaufwand

Es entstehen keine Haushaltsausgaben ohne Erfüllungsaufwand.

3. Erfüllungsaufwand

a) Erfüllungsaufwand für die Bürgerinnen und Bürger

Für die Bürgerinnen und Bürger entsteht kein Erfüllungsaufwand.

b) Erfüllungsaufwand für die Wirtschaft

Für die jeweils betroffenen Erbringer öffentlich zugänglicher Telekommunikationsdienste entsteht ein zusätzlicher Aufwand durch die Erfüllung der in § 113b TKG-E vorgesehenen Speicherpflicht und die damit verbundenen Regelungen zur Verwendung der Daten, zur Gewährleistung der Datensicherheit und Datenqualität, zur Protokollierung der Zugriffe auf die Daten sowie zur Aufnahme bestimmter Angaben in das zu erstellende Sicherheitskonzept. § 113a Absatz 2 TKG-E sieht daher aus Verhältnismäßigkeitsgründen eine Entschädigungsregelung vor, die vor allem Kleinunternehmer vor unbilligen Härten schützen soll.

Der Aufwand dürfte in Abhängigkeit von der bisherigen – sehr unterschiedlichen und dem Wandel unterzogenen – Handhabung bei der Speicherung der Daten und der Unternehmensgröße verschieden groß sein. Die erforderliche Umstellung wird zum Teil allerdings im Rahmen von ohnehin regelmäßig anstehenden technischen Anpassungen erfolgen und damit den allein durch die Speicherpflicht ausgelösten Aufwand reduzieren können.

Der insgesamt für die Telekommunikationswirtschaft entstehende zusätzliche Aufwand kann zurzeit nicht geschätzt werden. Während der Aufwand für die Verkehrsdatenerhebung und die Beauskunftung nach § 23 JVEG-E entschädigt wird, sieht der Entwurf für die zur Erfüllung der Speicherpflichten erforderlichen Investitionen und gegebenenfalls gesteigerten Betriebskosten nur dann eine Entschädigung vor, wenn es sonst zu unbilligen Härten kommen würde.

Weil es sich bei den meisten der ca. 1 000 betroffenen Unternehmen um kleine bis mittlere Erbringer öffentlich zugänglicher Telekommunikationsdienste handelt, für welche die voraussichtlichen Kosten bei der Umstellung eine erhebliche Härte darstellen, werden voraussichtlich viele von ihnen eine Entschädigung geltend machen. Es ist davon auszugehen, dass die übrigen betroffenen Unternehmen diese Kosten bei ihrer Preisgestaltung einkalkulieren und an ihre Kunden weitergeben werden.

Der Entwurf führt folgende neue Informationspflichten im Sinne des Gesetzes zur Einsetzung eines Normenkontrollrates für Unternehmen und die Verwaltung ein:

– § 113b Absatz 1 TKG-E verpflichtet Erbringer öffentlich zugänglicher Telekommunikationsdiensten, Daten nach Maßgabe der Absätze 2 und 3 für zehn Wochen zu speichern; bei Standortdaten nach Absatz 4 beträgt die Speicherpflicht vier Wochen.

– § 113e Absatz 1 TKG-E bestimmt, dass der nach § 113a TKG-E Verpflichtete jeden Zugriff auf die gespeicherten Daten für Zwecke der Datenschutzkontrolle revisionssicher zu protokollieren hat.

– § 113g Satz 1 TKG-E bestimmt, dass der nach § 113a TKG-E Verpflichtete bestimmte Angaben in das zu erstellende Sicherheitskonzept aufzunehmen hat.

– § 113g Satz 2 TKG-E bestimmt die Zeitpunkte, zu denen der nach § 113a TKG-E Verpflichtete der Bundesnetzagentur das Sicherheitskonzept vorzulegen hat. § 121

Absatz 1 TKG-E erweitert die Mitteilungspflichten der Bundesnetzagentur in dem zu erstellenden Tätigkeitsbericht.

Durch die in diesem Gesetz vorgenommene Änderung des Strafgesetzbuches durch dieses Gesetz entstehen für die Wirtschaft bei normgerechtem Verhalten keine Kosten. Das Gesetz zielt auf eine effektive Bekämpfung des Umgangs mit illegal erlangten Daten ab und kann daher dazu beitragen, dass Schäden und damit auch Kosten für die Wirtschaft vermieden werden.

c) Erfüllungsaufwand der Verwaltung

§ 101b baut die sich derzeit aus § 100g Absatz 4 StPO ergebenden Pflichten zur Erhebung statistischer Daten durch die Strafverfolgungsbehörden und das Bundesamt für Justiz aus.

Durch die Änderung der Vorschriften des Telekommunikationsgesetzes in Artikel 2 entsteht bei der Bundesnetzagentur sich in Sachinvestitionen und Personalkosten aufgliedernder zusätzlicher Vollzugsaufwand. Der – wegen der Vorgaben des Bundesverfassungsgerichts in seinem Urteil zur Vorratsdatenspeicherung unvermeidbare – Mehraufwand entsteht u. a. durch die Verpflichtung nach § 113f TKG-E, einen Anforderungskatalog zu erstellen, diesen fortlaufend zu überprüfen und bei Bedarf unverzüglich anzupassen. Zudem resultiert aus der Verpflichtung zur Verkehrsdatenspeicherung ein erhöhter Kontrollaufwand im Rahmen der Aufsicht nach § 115 TKG einschließlich der Anwendung der neuen Bußgeldtatbestände.

Die nach dem JVEG zu gewährenden Kostenpauschalen werden die Haushalte der Länder belasten; es ist aber nicht zu erwarten, dass dies in erheblich höherem Maße der Fall ist als bei den bestehenden Regelungen.

Noch nicht abzuschätzen ist, wie sich die Entschädigungsregelung in § 113a Absatz 2 TKG-E auswirken wird. Von den vorhandenen ca. 1 000 Anbietern sind zwanzig so groß, dass die 98 Prozent des Marktes abdecken, die übrigen sind kleine bis mittlere Unternehmen, von denen voraussichtlich viele ein unbillige Härte geltend machen werden. Dies kann jedoch erst geschehen, wenn der entsprechende Anforderungskatalog (§ 113f TKG-E) durch die Bundesnetzagentur erstellt wurde.

Auswirkungen auf die Haushalte der Kommunen sind nicht zu erwarten.

4. Weitere Kosten

Die Verkehrsdatenabfrage stellt kein neues Ermittlungsinstrument dar. Kosten für die Judikative werden durch die mit diesem Gesetz eingeführten Änderungen voraussichtlich nicht in nennenswertem Umfang entstehen, da die Abfragen im Großen und Ganzen im gleichen Umfang erfolgen wie bisher, aber zu besseren Ergebnissen führen. In diesen Fällen müssen allerdings nach dem JVEG Kostenpauschalen bezahlt werden, die insgesamt zu erhöhten Kosten führen können.

Durch die Einführung eines neuen Straftatbestandes können den Länderhaushalten Verfahrens- und Vollzugskosten entstehen, deren genaue Höhe sich nicht näher beziffern lässt. Für den Bund entstehen allenfalls in geringem Umfang Mehrausgaben. Etwaiger Mehrbedarf an Sach- und Personalmitteln kann innerhalb der vorhandenen Kapazitäten und der verfügbaren Mittel aufgefangen werden und soll finanziell und stellenmäßig im Einzelplan 07 ausgeglichen werden.

Im Übrigen entstehen für die Wirtschaft, insbesondere für mittelständische Unternehmen, keine weiteren Kosten. Auswirkungen auf Einzelpreise und das allgemeine Preisniveau, insbesondere auf das Verbraucherpreisniveau, sind nicht zu erwarten.

5. Weitere Gesetzesfolgen

Die Regelungen sind inhaltlich geschlechtsneutral und berücksichtigen die Vorschrift des § 1 Absatz 2 des Bundesgleichstellungsgesetzes, der zufolge die Rechts- und Verwaltungsvorschriften des Bundes die Gleichstellung von Frauen und Männern auch sprachlich zum Ausdruck bringen sollen. Auswirkungen von gleichstellungspolitischer Bedeutung sind nicht zu erwarten.

Demographische oder verbraucherpolitische Auswirkungen sind nicht ersichtlich.

VI. Befristung; Evaluierung

Eine Befristung der Regelungen ist nicht sachgerecht. Eine Evaluierung ist entbehrlich; der Entwurf sieht allerdings eine statistische Erfassung der vorgenommenen Ermittlungsmaßnahmen vor. Sollte weiterer Änderungsbedarf erkennbar werden, werden die Strafverfolgungsbehörden die Justizressorts informieren.

B. Besonderer Teil

Zu Artikel 1 (Änderung der Strafprozessordnung)

Zu Nummer 1 (Inhaltsübersicht)

Die mit Gesetz vom …[hier einfügen: BGBl. …] neu eingeführte Inhaltsübersicht mit Paragraphenbezeichnungen in der Strafprozessordnung wird um die neu geschaffenen Vorschriften ergänzt.

Zu Nummer 2 (§ 100g StPO-E)

Das Bundesverfassungsgericht hat mit seinem Urteil zur Vorratsdatenspeicherung die §§ 113a und 113b des TKG und auch § 100g Absatz 1 Satz 1 StPO, soweit danach Verkehrsdaten nach § 113a TKG erhoben werden dürfen, wegen Verstoßes gegen Artikel 10 Absatz 1 GG für nichtig erklärt. Darüber hinaus hat das Bundesverfassungsgericht die Vorschrift des § 100g StPO in seinem Urteil nicht beanstandet, insbesondere auch nicht die Erhebung von Verkehrsdaten, welche die Telekommunikationsunternehmen nach Maßgabe der §§ 96 ff. TKG zu geschäftlichen Zwecken speichern. Die Einführung einer Speicherpflicht in das TKG macht jedoch eine grundlegende Neuregelung des § 100g StPO erforderlich, um die Einhaltung der mit einer solchen Speicherpflicht verbundenen verfassungs- und europarechtlichen Vorgaben zu gewährleisten. Dies schließt ausdifferenzierte und systematische Bestimmungen zu den Benachrichtigungspflichten und den Möglichkeiten des nachträglichen Rechtsschutzes (§ 101a Absätze 3 bis 4 StPO-E) ein.

Zu Absatz 1

100g Absatz 1 StPO-E findet ausschließlich auf die Erhebung von Verkehrsdaten Anwendung, welche die Erbringer öffentlich zugänglicher Telekommunikationsdienste nach dem abschließenden Katalog in § 96 Absatz 1 TKG zu geschäftlichen Zwecken speichern dürfen. Durch die Streichung der Worte „auch ohne Wissen des Betroffenen“ wird deutlich gemacht, dass es sich bei der Verkehrsdatenerhebung nach § 100g StPO-E grundsätzlich nicht um eine heimliche Maßnahme handelt. Soweit möglich muss die Verwendung der Daten offen erfolgen. Zudem wird die Voraussetzung eines angemessenen Verhältnisses

zwischen der Erhebung der Daten und der Bedeutung der Sache auch für die Fälle des Absatzes 1 Nummer 1 ausdrücklich aufgenommen.

Die Erhebung von Standortdaten ist nach diesem Absatz nur für künftig anfallende Verkehrsdaten oder in Echtzeit und nur im Fall des Satzes 1 Nummer 1 zulässig, soweit sie für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich ist. Damit wird bezüglich der besonders sensiblen Standortdaten, die grundsätzlich die Erstellung von Bewegungsprofilen ermöglichen, differenziert: Nicht gespeicherte Standortdaten stehen den Behörden nach wie vor im gleichen Umfang wie vor der Neufassung zur Verfügung; auf gespeicherte Standortdaten ist der Zugriff nur noch unter den Bedingungen des Absatzes 2 möglich.

Zu Absatz 2

§ 100g Absatz 2 StPO-E regelt die Erhebung der Verkehrsdaten, die nach § 113b TKG-E verpflichtend zu speichern sind. Eine Einschränkung im Vergleich zu Absatz 1 ergibt sich zum einen daraus, dass eine Erhebung dieser Daten nur bei bestimmten, besonders schweren, im Einzelnen aufgezählten Straftaten zulässig ist.

Sowohl das Bundesverfassungsgericht wie der Gerichtshof der Europäischen Union haben in ihren Urteilen zur Vorratsdatenspeicherung die Verwendung der gespeicherten Verkehrsdaten für die Strafverfolgung auf den Bereich der schweren Kriminalität beschränkt:

Für die Strafverfolgung bedeutet dies, dass ein Abruf der Daten zumindest den durch bestimmte Tatsachen begründeten Verdacht einer schweren Straftat voraussetzt. Welche Straftatbestände hiervon umfasst sein sollen, hat der Gesetzgeber abschließend mit der Verpflichtung zur Datenspeicherung festzulegen. Ihm kommt hierbei ein Beurteilungsspielraum zu. Er kann dabei entweder auf bestehende Kataloge zurückgreifen oder einen eigenen Katalog schaffen, etwa um Straftaten, für die die Telekommunikationsverkehrsdaten besondere Bedeutung haben, zu erfassen. Die Qualifizierung einer Straftat als schwer muss aber in der Strafnorm – insbesondere etwa durch deren Strafrahmen – einen objektivierten Ausdruck finden (vgl. BVerfGE 109, 279 <343 ff., insbesondere 347 f.>). Eine Generalklausel oder lediglich die Verweisung auf Straftaten von erheblicher Bedeutung reichen hingegen nicht aus. (BVerfGE 125, 260 <328 f.>)

Auch der Gerichtshof der Europäischen Union hat objektive Kriterien gefordert, die den Eingriff in Artikel 7 und 8 der Charta der Grundrechte auf Straftaten beschränken, die im Hinblick auf die betroffenen Grundrechte als hinreichend schwer angesehen werden können, um den Eingriff zu rechtfertigen (Urteil Digital Rights, C-294/13 und C-594/12, Rn. 60).

Diesen Vorgaben entsprechend, sollen die nach § 113b TKG-E gespeicherten Verkehrsdaten nur dann erhoben werden dürfen, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in § 100g Absatz 2 Satz 2 StPO-E katalogmäßig bezeichnete, auch im Einzelfall besonders schwere Straftat begangen oder in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat.

In Ausprägung des Verhältnismäßigkeitsgrundsatzes ist ferner eine – § 100g Absatz 1 Satz 1 StPO-E entsprechende – Subsidiaritätsklausel vorgesehen, nach der eine Erhebung dieser Daten nur erfolgen darf, soweit dies für die Erforschung des Sachverhalts erforderlich ist und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht.

Für die enumerative Aufzählung der als besonders schwer einzustufenden Straftaten in § 100g Absatz 2 Satz 2 StPO-E wurde auf eine Teilmenge der im Katalog des § 100a Absatz 2 StPO enthaltenen Straftaten zurückgegriffen. Dass der Straftatenkatalog des

§ 100a Absatz 2 StPO verfassungsgemäß ist, hat das Bundesverfassungsgericht mit Beschluss vom 12. Oktober 2011 (2 BvR 236/08) festgestellt, in dem es Verfassungsbeschwerden, mit denen u. a. eine Verletzung von Grundrechten durch § 100a Absatz 2 StPO gerügt wurde, zurückgewiesen hat (BVerfGE 129, 208 <241 f.>).

Im Hinblick auf die hohe Grundrechtsrelevanz des Abrufs verpflichtend gespeicherter Daten wurde der Katalog deutlich reduziert. Es handelt sich um Straftaten, die der Bekämpfung des Terrorismus oder dem Schutz höchstpersönlicher Rechtsgüter, insbesondere Leib, Leben, Freiheit und sexuelle Selbstbestimmung, dienen. Außerdem sind besonders schwere Straftaten umfasst, bei denen die gespeicherten Verkehrsdaten nach kriminalistischer Erfahrung besonders wertvolle Dienste leisten können.

Eine Erhebung von Standortdaten zur Ermittlung des Aufenthaltsortes des Beschuldigten ist nach Absatz 2 unter den dort genannten Voraussetzungen möglich.

Zu Absatz 3

Absatz 3 enthält eine Sonderregelung zu Funkzellenabfragen. Bei diesen handelt es sich nicht um Standortdatenerhebungen; vielmehr werden bei einer solchen Abfrage alle Verkehrsdaten erhoben, die in einer bestimmten Funkzelle angefallen sind, um festzustellen, welche Mobilgeräte zu einer bestimmten Zeit der betreffenden Funkzelle zuzuordnen waren. Der Gesetzentwurf führt eine Legaldefinition der Funkzellenabfrage ein und nennt ihre Voraussetzungen. Auf diese Weise wird eine normenklare Ermächtigungsgrundlage für Funkzellenabfragen geschaffen.

Funkzellenabfragen erfolgen auf der Grundlage von Absatz 3 in Verbindung mit Absatz 1 Nummer 1. Voraussetzung für eine Abfrage ist zum einen, dass die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre. Die Erhebung der Daten muss zudem in einem angemessenen Verhältnis zur Bedeutung der Sache stehen.

Diese im Vergleich zum gegenwärtigen Zustand engeren Zulässigkeitsvoraussetzungen der Funkzellenabfrage sind notwendig, um die unverhältnismäßige Beeinträchtigung einer Vielzahl von Betroffenen zu vermindern. Durch Funkzellenabfragen werden nämlich unvermeidbar Verkehrsdaten Dritter, namentlich solcher Personen erhoben, die – ohne Beschuldigte oder Nachrichtenmittler zu sein – in der abgefragten Funkzelle mit ihrem Mobiltelefon kommuniziert haben. Zwar ist bereits nach geltendem Recht bei der Anordnung zu berücksichtigen, inwieweit dritte Personen von einer Funkzellenabfrage 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, in dem Dritte betroffen sind, als unangemessen erscheint (vgl. Bundestags-Drucksache 16/5846, S. 55). Gleichwohl soll dem Grundsatz der Verhältnismäßigkeit durch eine Präzisierung der Anforderungen für die Anordnung einer Funkzellenabfrage besonders Rechnung getragen werden, um von vornherein zu verhindern, dass Verkehrsdaten Unbeteiligter über das zur Strafverfolgung unerlässliche Maß hinaus erhoben werden und dabei bei den Strafverfolgungsbehörden Bewegungsprofile erstellt werden könnten. Bei den anordnenden Stellen soll das Bewusstsein dafür geschärft werden, dass es im Rahmen der Verhältnismäßigkeitsprüfung stets einer besonderen Abwägung insbesondere im Hinblick darauf bedarf, dass durch die Funkzellenabfrage in regelmäßig unvermeidbarer Weise Verkehrsdaten Dritter erhoben werden.

Die bisherige Regelung zur Ausgestaltung der Funkzellenabfrage in § 100g Absatz 2 Satz 2 StPO findet sich nunmehr in § 101a Absatz 1 Satz 3 StPO-E.

Zu Absatz 4

Sowohl das Bundesverfassungsgericht als auch der Gerichtshof der Europäischen Union (Urteil Digital Rights, C-294/13 und C-594/12, Rn. 58) haben hervorgehoben, dass die Verhältnismäßigkeit einer Speicherung von Verkehrsdaten besondere Regelungen zum Schutz von Personen voraussetzt, die beruflichen Verschwiegenheitspflichten unterliegen.

Flankierend zur Regelung des § 113b Absatz TKG-E, der die in § 99 Absatz 2 Satz 2 TKG genannten Verbindungen von der Speicherpflicht des § 113b Absatz 2 TKG-E ausnimmt, sieht Absatz 4 daher ein grundsätzliches Verbot der Erhebung von Verkehrsdaten vor, die sich gegen die in § 53 Absatz 1 Nummer 1 bis 5 genannten Personen richtet. Damit wird die Regelung des § 160a Absatz 1 für den Abruf von nach § 113b TKG-E gespeicherten Daten dahingehend erweitert, dass ein Erhebungsverbot in Bezug auf alle in § 53 Absatz 1 genannten Berufsgruppen besteht.

Die Berufsgeheimnisträger in ihrer Gesamtheit schon von der Speicherung ihrer Verkehrsdaten auszunehmen, ist nicht möglich. Dazu müsste sämtlichen Telekommunikationsanbietern, von denen es in Deutschland ca. 1 000 gibt, mitgeteilt werden, wer Berufsgeheimnisträger im Sinne des § 53 StPO ist; diese Liste müsste dauernd aktualisiert werden. Ihre Erstellung, Übermittlung und Aktualisierung birgt auch im Falle des Einverständnisses der Betroffenen ein erhebliches Missbrauchsrisiko. Hinzu kommt, dass Berufsgeheimnisträger in vielen Fällen nicht über statische, sondern über dynamische IP-Adressen verfügen, so dass eine Liste der verwendeten Adressen gar nicht erstellt werden könnte. Der bessere Schutz ergibt sich daher bei einer Regelung, die die Verwendung der gespeicherten Daten ausschließt. Dieser Schutzmechanismus hat sich in der StPO auch an anderer Stelle bewährt.

Zu Absatz 5

Die Regelung in Absatz 5 entspricht dem geltenden Recht (§ 100g Absatz 3) und stellt klar, dass sich die Erhebung von Verkehrsdaten nach den allgemeinen Vorschriften, also insbesondere nach den §§ 94 ff. StPO richtet, wenn sie – etwa durch Sicherstellung von Gegenständen (zum Beispiel elektronische Datenträger, aber auch Verbindungsnachweise in Papierform) nach Abschluss des Kommunikationsvorgangs in anderer Weise als durch eine Auskunftsanordnung an den Erbringer öffentlich zugänglicher Telekommunikationsdienste erfolgt.

Zu Nummer 3 (§ 100j StPO-E)

Die vorgeschlagene Ergänzung in § 100j Absatz 2 StPO sieht vor, dass für Bestandsdatenauskünfte zu Internetprotokoll-Adressen auf nach § 113b TKG gespeicherte Verkehrsdaten zurückgegriffen werden darf.

Weiterer Ergänzungen bedarf § 100j StPO nicht. Insbesondere enthält er in Absatz 4 bereits Bestimmungen zur Benachrichtigung der betroffenen Person und entspricht damit den verfassungsrechtlichen Vorgaben auch insoweit, als künftig eine Auskunftserteilung nach § 100j Absatz 2 StPO anhand von nach § 113b TKG-E gespeicherten Daten (Internetprotokoll-Adressen) erfolgen kann.

Zu Nummer 4 (§ 101 StPO-E)

Es handelt sich um eine Folgeänderung, die sich aus Qualifizierung der Verkehrsdatenabfrage als offene Maßnahme ergibt.

Zu Nummer 5 (§§ 101a und 101b StPO-E)

Zu § 101a StPO-E

Mit dem Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007 (BGBl. I S. 3198) hat der Gesetzgeber in § 101 StPO für die Ermittlungsbefugnisse nach den §§ 98a, 99, 100a, 100c, 100f bis 100i, 110a und 163d ff. StPO all jene Verfahrensvorschriften zusammengefasst, die bis dahin jeweils gesondert geregelt waren. Die Vorschrift regelt damit einheitlich für alle speziellen verdeckten Maßnahmen unter anderem Kennzeichnungspflichten, Benachrichtigungspflichten und deren Zurückstellung nebst gerichtlicher Überprüfung. Zur Stärkung des Grundrechts auf rechtliches Gehör nach Artikel 103 Absatz 1 GG und des Gebots der Gewährleistung eines effektiven Rechtsschutzes nach Artikel 19 Absatz 4 GG wird zudem nachträglicher Rechtsschutz gewährt.

Die Erhebung von Verkehrsdaten nach § 100g StPO-E ist aus systematischen Gründen aus dem Anwendungsbereich dieser einheitlichen Vorschrift über grundrechtssichernde Verfahrensregelungen bei verdeckten Ermittlungsmaßnahmen herauszunehmen, da die Regelung nunmehr den Vorgaben des Bundesverfassungsgerichts entspricht, das festgelegt hatte, dass die Erhebung von Verkehrsdaten jedenfalls für den Bereich der Strafverfolgung künftig grundsätzlich als offene Maßnahme auszugestalten ist: „Zu den Transparenzanforderungen zählt der Grundsatz der Offenheit der Erhebung und Nutzung von personenbezogenen Daten. Eine Verwendung der Daten ohne Wissen des Betroffenen ist verfassungsrechtlich nur dann zulässig, wenn andernfalls der Zweck der Untersuchung, dem der Datenabruf dient, vereitelt wird. Für die Gefahrenabwehr und die Wahrnehmung der Aufgaben der Nachrichtendienste darf der Gesetzgeber dies grundsätzlich annehmen. Demgegenüber kommt im Rahmen der Strafverfolgung auch eine offene Erhebung und Nutzung der Daten in Betracht (vgl. § 33 Absatz 3 und 4 StPO). Ermittlungsmaßnahmen werden hier zum Teil auch sonst mit Kenntnis des Beschuldigten und in seiner Gegenwart durchgeführt (vgl. zum Beispiel §§ 102, 103, 106 StPO). Dementsprechend ist der Betroffene vor der Abfrage beziehungsweise Übermittlung seiner Daten grundsätzlich zu benachrichtigen. Eine heimliche Verwendung der Daten darf nur vorgesehen werden, wenn sie im Einzelfall erforderlich und richterlich angeordnet ist.“ (BVerfGE 125, 260 <335 f.>)

In § 101a StPO-E wird das Verfahren zur Erhebung von Verkehrsdaten an Verfahren zur Anordnung offener Maßnahmen angeglichen.

Zu Absatz 1

Absatz 1 enthält den für Verkehrsdatenerhebungen nach § 100g bedeutsamen Richtervorbehalt. Dabei wird nach der Art der gespeicherten Daten differenziert. In Absatz 1 Satz 1 wird für die Fälle des § 100g Absatz 1 wie bisher auf § 100a Absatz 3 und § 100b Absatz 1 bis 4 StPO verwiesen. Für die Fälle des § 100g Absatz 2 werden ins Absatz 1 Satz 2 die § 100b Absatz 1 Satz 2 und 3 nicht in Bezug genommen. Für die Erhebung der verpflichtend zu speichernden Daten besteht somit die Möglichkeit einer Eilanordnung durch die Staatsanwaltschaft bei Gefahr im Verzug nicht. Das Verfahren bei Funkzellenabfragen nach § 100g Absatz 3 wird in Absatz 1 Satz 3 geregelt. Abweichend von § 100b Absatz 2 Satz 2 Nummer 2 müssen hier nicht die Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses oder des Endgerätes, sofern sich nicht aus bestimmten Tatsachen ergibt, dass diese zugleich einem anderen Endgerät zugeordnet ist, angegeben werden. Es reicht vielmehr aus, die Telekommunikation räumlich und zeitlich eng begrenzt und hinreichend bestimmt zu bezeichnen. Je nachdem, ob die Funkzellenabfrage unter den Voraussetzungen des § 100g Absatz 1 oder des § 100g Absatz 2 durchgeführt werden soll, sind für die Frage des Richtervorbehalts mit oder ohne Eilkompetenz der

Staatsanwaltschaft die entsprechenden Regelungen in Absatz 1 Satz 1 oder Satz 2 heranzuziehen.

§ 101a Absatz 1 Nummer 1 StPO-E erfüllt die Vorgabe des Bundesverfassungsgerichts, wonach in der Entscheidungsformel die zu übermittelnden Datenarten nach Maßgabe des Verhältnismäßigkeitsgrundsatzes hinreichend selektiv und in klarer Weise zu bezeichnen sind. Auch der Gerichtshof der Europäischen Union hat verfahrensrechtliche Voraussetzungen für den Zugang der zuständigen nationalen Behörden zu den Daten und deren spätere Nutzung als erforderlich angesehen (Urteil Digital Rights, C-294/13 und C-594/12, Rn. 61). Ferner sieht die Neuregelung vor, dass auch der Zeitraum, für den Daten übermittelt werden sollen, eindeutig anzugeben ist. Damit wird klargestellt, dass nicht nur bei der Erhebung zukünftig anfallender Daten zeitliche Angaben zu machen sind, wie es § 100b Absatz 2 Satz 2 Nummer 3 vorsieht, sondern dass auch bei der Erhebung bereits gespeicherter Daten der Zeitraum, für den die Daten erhoben werden sollen, genau bezeichnet werden muss. Auf diese Weise soll gewährleistet werden, dass nicht ohne entsprechende Erforderlichkeit pauschal alle vorhandenen Daten erhoben werden, sondern die Erhebung sich von vornherein auf solche Zeiträume beschränkt, die für die Untersuchung relevant sind.

§ 101a Absatz 1 Nummer 2 StPO-E sieht vor, dass der nach § 100b Absatz 3 Satz 1 zur Auskunft Verpflichtete auch mitzuteilen hat, welche der von ihm mitgeteilten Daten aus den nach § 113b TKG-E zu speichernden Daten herrühren. Diese Mitteilung ist für die von § 101a Absatz 3 StPO-E vorgegebene besondere Kennzeichnung erforderlich, ferner für die Statistik nach § 101b StPO-E.

Zu Absatz 2

Für sämtliche Maßnahmen nach § 100g StPO-E und für deren Verlängerung wird in Absatz 2 in Anlehnung an § 81g Absatz 3 Satz 5 und § 100d Absatz 3 Satz 1 und 2 StPO eine qualifizierte Begründungspflicht vorgesehen.

Die klaren Vorgaben zur Begründung der Erforderlichkeit und Angemessenheit der Maßnahme auch hinsichtlich des Umfangs der zu erhebenden Datenarten und des Zeitraums, für den sie erhoben werden sollen, präzisieren die bereits aus § 34 StPO folgenden Anforderungen für die gerichtliche Anordnung der Verkehrsdatenerhebung und ihre Verlängerung. Die anordnenden Stellen werden besonders angehalten, die maßgeblichen Verhältnismäßigkeitsgesichtspunkte im Anordnungs- und Verlängerungsbeschluss transparent und nachvollziehbar zum Ausdruck zu bringen. Grundsätzlich sollen nur einzelne Standortdaten abgerufen werden, um keine überflüssigen Bewegungsprofile zu erstellen. wenn diese nicht im Einzelfall notwendig sind, zum Beispiel, um eine Serientat aufzuklären oder um Anhaltspunkte für vom Beschuldigten angegebene Bewegungen zu gewinnen. Durch eine solche qualifizierte Begründungspflicht kann eine Stärkung des Richtervorbehaltes, ein verbesserter Rechtsschutz für die durch die Maßnahme Betroffenen (dies gilt vor allem für die unvermeidbar mitbetroffenen Dritten) sowie eine verbesserte Überprüfung der Entscheidung für den Fall einer nachträglichen gerichtlichen Kontrolle erreicht werden (vgl. Bundestags-Drucksache 15/4522, S. 17, für § 100d Absatz 3 StPO).

Zu Absatz 3

Die Vorgabe in Satz 1, nach der personenbezogene Daten, die durch Maßnahmen nach den Absätzen 1, 2 und 4 erhoben wurden, entsprechend zu kennzeichnen sind, entspricht § 101 Absatz 3 Satz 1 StPO.

Zudem sieht Absatz 3 Satz 1 vor, dass die personenbezogenen Daten, die durch Maßnahmen nach § 100g Absatz 1 bis 3 erhoben wurden, unverzüglich auszuwerten sind, um den mit der fortwährenden Speicherung der Daten verbundenen Eingriff nicht zu perpetuieren und damit zu vertiefen. Die erhobenen Verkehrsdaten müssen, soweit sie zur Straf-

verfolgung oder für eine etwaige gerichtliche Überprüfung nicht mehr erforderlich sind, unverzüglich nach § 101 Absatz 8 StPO gelöscht werden. Dies gilt nach Absatz 3 Satz 1 auch für Verkehrsdaten, die nicht nach § 113b TKG gespeichert waren, weil es auch insoweit eine mit der fortwährenden Speicherung der Daten verbundene Perpetuierung des Eingriffs zu vermeiden gilt und dies zudem eine einheitliche und damit für die Praxis einfachere Handhabung ermöglicht.

Absatz 3 Satz 2 gibt vor, dass erkennbar sein muss, ob es sich um Daten handelt, die nach § 113b TKG-E gespeichert waren. Diese besondere Kennzeichnungspflicht ist erforderlich, um die enge Zweckbindung, die für diese Daten gilt, umfassend gewährleisten zu können und dafür sorgen zu können, dass die Verwendung ausschließlich für die Wahrnehmung der Aufgaben erfolgt, derentwegen ein Zugriff auf diese Daten auch unmittelbar zulässig wäre.

Absatz 3 Satz 3 sieht vor, dass die Kennzeichnung auch bei der Übermittlung an andere Stellen aufrechtzuerhalten ist.

Absatz 3 Satz 4 übernimmt mit dem Verweis auf § 101 Absatz 8 StPO die schon bislang auch für Verkehrsdaten geltenden Vorgaben zur Löschung, Veraktung der Löschung und Sperrung.

Zu Absatz 4

Das mit einem Antrag auf Erlass einer Anordnung nach § 100g StPO-E befasste Gericht hat nach Maßgabe des § 33 StPO dem Betroffenen bereits vor der Entscheidung über eine Anordnung Gelegenheit zum rechtlichen Gehör zu geben. Von der Anhörung kann nach § 33 Absatz 4 Satz 1 StPO nur abgesehen werden, wenn die vorherige Anhörung den Zweck der Anordnung gefährden würde. Dies ist in jedem Einzelfall zu begründen.

Erlässt das Gericht die beantragte Anordnung, wird diese, da sie regelmäßig der Vollstreckung bedarf, nach Maßgabe des § 36 StPO der Staatsanwaltschaft übergeben, die das Erforderliche zu veranlassen hat. Hierzu gehört auch, den Betroffenen nach Maßgabe des § 101a Absatz 4 von der (anstehenden) Erhebung der Verkehrsdaten zu benachrichtigen. Stehen einer Benachrichtigung zu diesem Zeitpunkt Gründe entgegen, ist sie mit Zustimmung des Gerichts zurückzustellen. In einem solchen Fall wird das Gericht regelmäßig ohne vorherige Anhörung des Betroffenen die Anordnung getroffen haben; in der Praxis kann sich daher empfehlen, dass bereits mit dem Antrag auf Anordnung einer Verkehrsdatenerhebung zugleich der Antrag auf Zustimmung zur Zurückstellung der Benachrichtigung unterbreitet wird.

§ 101a Absatz 4 verweist für Benachrichtigung und Rechtsschutz auf § 101 Absatz 4 bis 7 StPO. Mit Blick auf die Vorgaben des Bundesverfassungsgerichts wird abweichend von § 101 StPO bestimmt, dass ein Absehen von einer Benachrichtigung nach § 101 Absatz 4 Satz 3 StPO einer gerichtlichen Anordnung bedarf (§ 101a Absatz 4 Nummer 1) und dass auch die erstmalige Zurückstellung einer Benachrichtigung nach § 101 Absatz 5 Satz 1 StPO einer gerichtlichen Anordnung bedarf (§ 101a Absatz 4 Nummer 2).

Zu § 101b StPO-E

Der neue § 101b ersetzt als Folgeänderung die geltenden Vorgaben in § 100g Absatz 4 StPO zur statistischen Erfassung der Verkehrsdatenerhebung nach § 100g StPO. Durch den Verweis auf § 100b Absatz 5 StPO wird bestimmt, dass die Länder und der Generalbundesanwalt dem Bundesamt für Justiz über die in ihrem Geschäftsbereich angeordneten Maßnahmen kalenderjährlich zu berichten haben, damit es eine entsprechende Übersicht zur Veröffentlichung im Internet erstellen kann. Die Statistik soll die Transparenz der Maßnahmen nach § 100g stärken und ihre Evaluierung erleichtern. Der Verweis auf § 100b Absatz 5 StPO entspricht dem Verweis im geltenden § 100g Absatz 4 StPO und

bestimmt unter Nummer 1, dass die Länder und der Generalbundesanwalt dem Bundesamt für Justiz über die in ihrem Geschäftsbereich nach den Absätzen 1, 2 und 3 angeordneten Maßnahmen kalenderjährlich zu berichten haben, damit das Bundesamt eine entsprechende Übersicht zur Veröffentlichung im Internet erstellen kann. Nummer 2 gibt zudem vor, dass die nach Maßgabe der Nummer 2 Buchstabe a bis d differenziert zu erhebende Anzahl von Anordnungen getrennt anzugeben ist für die Bereiche Festnetz-, Mobilfunk- und Internetdienste und jeweils untergliedert – bemessen ab dem Zeitpunkt der Anordnung – nach der Anzahl der zurückliegenden Wochen, für die die Erhebung von Verkehrsdaten angeordnet wurde.

Zu Nummer 6 (§ 160a StPO-E)

Zu Buchstabe a

Es handelt sich um eine Folgeänderung zu Artikel 3 Nummer 2. Da es sich bei der Datenhehlerei um ein Anschlussdelikt handelt, sind die entsprechenden Regelungen in der Strafprozessordnung anzupassen.

Zu Buchstabe b

Es handelt sich um eine Folgeänderung, die sich aus der Regelung der Erhebungs- und Verwertungsverbote zum Schutz der in § 53 Absatz 1 StPO genannten zeugnisverweigerungsberechtigten Personen in Absatz 4 ergibt.

Zu Nummer 7 (§ 304 StPO-E)

Es handelt sich um eine Folgeänderung, die sich aus der Herausnahme des § 100g aus den heimlichen Ermittlungsmaßnahmen in § 101 StPO ergibt.

Zu Nummer 8 (§§ 3, 60, 68b, 97, 102 und 138a StPO-E)

Es handelt sich um eine Folgeänderung zu Artikel 5 Nummer 2. Da es sich bei der Datenhehlerei um ein Anschlussdelikt handelt, sind die entsprechenden Regelungen in der Strafprozessordnung (§§ 3, 60 Nummer 2, 68b Absatz 1 Satz 4 Nummer 1, 97 Absatz 2 Satz 3, 102, 138a Absatz 1 Nummer 3 StPO) anzupassen.

Zu Artikel 2 (Änderung des Telekommunikationsgesetzes)

Zu Nummer 1 (Inhaltsübersicht)

Die Inhaltsübersicht ist an die Überschriften der §§ 113a bis 113g TKG-E anzupassen.

Zu Nummer 2 (§§ 113a bis 113g TKG-E)

Zu § 113a TKG-E

Die Vorschrift beschreibt den Kreis der zur Speicherung Verpflichteten. Nach Absatz 1 richten sich die Speicherungspflichten an diejenigen, die öffentlich zugängliche Telekommunikationsdienste erbringen. Satz 2 bestimmt, dass diejenigen Diensteanbieter, die bei der Erbringung ihres Dienstes andere Unternehmen in Anspruch nehmen und daher nicht alle nach § 113b Absatz 2 bis 4 zu speichernden Daten selbst erzeugen oder verarbeiten, weiteren Verpflichtungen unterliegen. In diesem Fall hat der Erbringer des Telekommunikationsdienstes auch die unverzügliche Speicherung der nicht von ihm selbst bei der Erbringung seines Dienstes erzeugten und verarbeiteten Daten sicherzustellen. Auf welche Weise der Erbringer die Speicherung sicherstellt, hat er gegenüber der Bundesnetzagentur auf deren Verlangen nachzuweisen. Die Regelung des Satzes 2 umfasst im Vergleich

zu § 113a Absatz 1 Satz 2 TKG a. F. nunmehr sowohl den Fall, dass der Erbringer öffentlich zugänglicher Telekommunikationsdienste keine der nach dieser Vorschrift zu speichernden Daten selbst erzeugt und verarbeitet, als auch den Fall, dass er nur einige, aber nicht alle der zu speichernden Daten selbst erzeugt und verarbeitet. Die Verpflichtung zur Sicherstellung der Speicherung nach Satz 2 besteht jedoch nur, soweit die Daten bei der Erbringung des Dienstes erzeugt oder verarbeitet werden.

Außerdem sieht das Gesetz in Absatz 2 Entschädigungsmöglichkeiten für Unternehmen vor, die eine unbillige Härte bei der Durchführung der Speicherverpflichtung nachweisen können. Entsprechende Anträge werden von der Bundesnetzagentur geprüft, wobei die Antragsteller darlegen müssen, dass die Auswirkungen der Speicherpflicht für ihr Unternehmen erdrosselnde Wirkung haben könnte.

Zu § 113b TKG-E

Die Vorschrift des § 113b TKG-E dient als Kernregelung der Umsetzung der Vorgaben der Entscheidungen des Bundesverfassungsgerichts und des Gerichtshofes der Europäischen Union, indem sie die Adressaten sowie die Grundvoraussetzungen der Speicherungspflichten bestimmt, die zu speichernden Datenkategorien sowie die Speicherungsfrist festlegt und Vorgaben macht, wie die Speicherung der Daten und deren Löschung zu erfolgen haben.

Zu Absatz 1

Absatz 1 enthält die Verpflichtung zur Datenspeicherung, differenziert nach Verbindungs- und nach Standortdaten. Für Verbindungsdaten wird eine Speicherungsdauer von zehn Wochen festgelegt; Standortdaten (§ 113b Absatz 4 TKG-E) dürfen nur für vier Wochen gespeichert werden. Dies entspricht dem Gebot einer möglichst grundrechtsschonenden Regelung. Die Speicherungsdauer ist ausreichend, um in der weitaus überwiegenden Anzahl von Ersuchen eine Verfügbarkeit der maßgeblichen Daten sicherzustellen. Abweichend von § 113a TKG a. F. sind die Daten ausschließlich im Inland zu speichern; eine Erfüllung der Speicherpflicht durch die Speicherung in einem anderen Mitgliedstaat der Europäischen Union ist nicht mehr vorgesehen.

Die Beschränkung der Speicherung der Vorratsdaten auf das Inland ist eine Beschränkung der Dienstleistungsfreiheit im Sinne von Artikel 56 AEUV. Eine solche lässt sich rechtfertigen, wenn sie notwendig ist, um zwingenden Gründen des Allgemeininteresses gerecht zu werden, und wenn sie zudem verhältnismäßig ist. Diese Voraussetzungen liegen vor. Eine Beschränkung auf das Inland ist notwendig, um die grundrechtlichen Erfordernisse des Datenschutzes und der Datensicherheit zu gewährleisten, die gespeicherten Vorratsdaten wirksam vor Missbrauch sowie vor jedem unberechtigten Zugang und jeder unberechtigten Nutzung zu schützen und das durch eine unabhängige Stelle zeitnah und effizient überwachen zu können.

Nur im Inland können die in den §§ 113c ff. TKG-E enthaltenen Anforderungen insbesondere an die Verwendung und die Sicherheit der Daten umfassend gewährleistet und überprüft werden. Bei einer Speicherung im europäischen Ausland könnte nicht ausgeschlossen werden, dass entgegen der strengen Verwendungsbeschränkung in § 113c TKG-E der ausländische Staat nach Maßgabe seines (innerstaatlichen) Rechts Zugriff auf die auf seinem Hoheitsgebiet gespeicherten Daten nimmt, was angesichts jüngerer Erfahrungen nicht als nur theoretische Gefahr erscheint.

Zudem hätten die mit der Überprüfung der Einhaltung der Sicherheitsstandards und des Datenschutzes befassten deutschen öffentlichen Stellen in anderen Mitgliedstaaten der EU keine unmittelbaren und gleich wirksamen Möglichkeiten zur Prüfung, da jede Aufsichtsbehörde bei der Ausübung aufsichtsrechtlicher Befugnisse auf ihr eigenes Hoheitsgebiet beschränkt ist. Zwar könnte die deutsche Behörde bei grenzüberschreitender Da-

tenverarbeitung die Aufsichtsbehörde eines anderen Mitgliedstaates im Wege der Amtshilfe um die Ausübung ihrer Befugnisse auf eigenem Boden ersuchen (Art. 28 Absatz 6 Satz 2 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. Nr. L 281 vom 23. 11. 1995, S. 31). Angesichts des Umfangs der Prüfpflichten und der Tatsache, dass es sich nicht um eine einmalige Überprüfung eines Anbieters sondern um die Wahrnehmung dauerhafter Aufgaben (zum Beispiel bei der Anpassung der Sicherheitskonzepte an den jeweiligen Stand der Technik) handelt, erscheint dies aber zu wenig wirksam; im Fall von Einzelbeanstandungen wäre zudem nicht gewährleistet, dass die Überprüfung ausreichend schnell erfolgt.

Zu Absatz 2

Absatz 2 Satz 1 regelt die einzelnen Speicherungspflichten für Erbringer öffentlich zugänglicher Telefondienste und umfasst Ausprägungen wie Festnetz, Mobilfunk und Internettelefonie. Satz 2 stellt klar, dass diese Speicherungspflichten bei der Übermittlung von Kurznachrichten (SMS), Multimedianachrichten (MMS) und ähnliche Nachrichten (zum Beispiel EMS) entsprechend gelten, wobei sich die zu speichernden Zeitangaben mangels bestehender Verbindung auf die Versendung und den Empfang der Nachricht beziehen. Satz 3 erstreckt die Speicherpflicht auf unbeantwortete (das heißt nicht entgegengenommene) oder wegen eines Eingriffs des Netzwerkmanagements erfolglose Anrufe, soweit der Telefonieerbringer die entsprechenden Verkehrsdaten für die in § 96 Absatz 1 Satz 2 genannten Zwecke speichert oder protokolliert. Mit dieser, dem § 113a Absatz 5 TKG a. F. entsprechenden Regelung, werden beispielsweise Fälle erfasst, in denen ein Teilnehmer von seinem Diensteanbieter per Kurznachricht 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 Anrufs außerhalb des Versorgungsbereichs einer Funkzelle befand.

Zu Inhalt und Umfang der Speicherpflichten in Absatz 2 Satz 1 ist im Einzelnen auf Folgendes hinzuweisen:

Nummer 1 stellt sicher, dass – auch im Falle von Um- oder Weiterschaltungen eines Anrufs – die im Bereich der Telefonie zur Identifizierung der Kommunikationsteilnehmer erforderlichen Rufnummern oder anderen Anschlusskennungen verfügbar sind.

Nummer 2 gewährleistet die genaue zeitliche Bestimmbarkeit einer erfolgten Telekommunikation.

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 Speichervorgaben für den Bereich der Mobilfunktelefonie.

– Nach Buchstabe a sind die internationalen Kennungen für mobile Teilnehmer für den anrufenden und den angerufenen Anschluss zu speichern (so genannte IMSI).

– Nach Buchstabe b sind die internationalen Kennungen der anrufenden und der angerufenen Endgeräte zu speichern (so genannte IMEI).

– Nach Buchstabe c ist bei der Inanspruchnahme im Voraus bezahlter anonymer Telefondienste der Zeitpunkt der ersten Aktivierung des Dienstes zu speichern. Sofern die Aktivierung einer solchen so genannten Prepaidkarte mittels Anrufs beim Telekom-

munikationsdiensteerbringer erfolgt, werden diese Daten bereits durch die Nummern 1, 2 und 4 Buchstabe a und b erfasst, so dass auf der Grundlage dieses Aktivierungsverfahrens Buchstabe c zu keiner zusätzlichen Datenspeicherung führt. Soweit die Aktivierung des Dienstes auf eine Weise erfolgt, bei der Verkehrsdaten weder erzeugt noch verarbeitet werden, wie dies etwa der Fall sein kann, wenn die Freischaltung durch eine sofortige Onlineanmeldung bei Vertragsschluss von einem Mitarbeiter des Erbringers öffentlich zugänglicher Telekommunikationsdienste erfolgt, begründet dies nach Maßgabe von Absatz 1 Satz 1 keine Speicherungspflicht.

Nummer 5 regelt für den Bereich der Internettelefonie die Pflicht zur Speicherung der Internetprotokoll-Adressen des anrufenden und des angerufenen Anschlusses, um eine Bestimmung des Anschlusses zu ermöglichen, der Ziel oder Ursprung eines Internettelefonats war. Bei Internet-Telefondiensten sind auch die zugewiesenen Benutzerkennungen zu speichern.

Zu Absatz 3

Absatz 3 regelt die einzelnen Speicherungspflichten für Erbringer öffentlich zugänglicher Internetzugängen. Eine Speicherung der im Internet aufgerufenen Adressen (so genannte URL [Uniform Resource Locator]) findet nicht statt. Es wird somit auch auf Grundlage der zu speichernden Internetdaten nicht das gesamte „Surfverhalten“ von Internetnutzern nachvollziehbar werden.

Um – ebenso wie bei § 113b Absatz 2 Nummer 5 TKG-E – der Praxis die Rückverfolgung und Identifizierung der Quelle eines Kommunikationsvorgangs besser zu ermöglichen, ist nach § 113b Absatz 3 Nummer 2 neben der Kennung des Anschlusses, über den die Internetnutzung erfolgt, auch die zugewiesene Benutzerkennung zu speichern.

Zu Absatz 4

Nach Absatz 4 sind die Standortdaten des anrufenden und des angerufenen Anschlusses bei Beginn der Verbindung, also die konkreten Bezeichnungen der Funkzellen für vier Wochen zu speichern, über die die Telekommunikationsteilnehmer beim Verbindungsaufbau versorgt werden. Bei der Nutzung von öffentlich zugänglichen Internetzugangsdiensten durch Mobilfunk wird die Bezeichnung der Funkzelle gespeichert, die bei Beginn der Internetverbindung genutzt wird.

Absatz 4 Satz 3 bestimmt zudem, dass auch die Daten vorzuhalten sind, aus denen sich die geographischen Lage und die Hauptstrahlrichtungen der die jeweilige Funkzelle versorgenden Funkantennen ergeben. Diese § 113a Absatz 7 TKG a. F. aufgreifende Regelung betrifft Angaben zur Netzplanung der Mobilfunknetzbetreiber, regelt also nicht die Speicherung von Verkehrsdaten. Die Angaben sind erforderlich, um die nach Absatz 1 Nummer 4 und für mobile, öffentlich zugängliche Internetzugangsdienste 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 Erbringern öffentlich zugänglicher Telekommunikationsdienste 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 5

Die Regelung in Absatz 5 stellt klar, dass Kommunikationsinhalte, Daten über aufgerufene Internetseiten und Daten von Diensten der elektronischen Post nach dieser Vorschrift nicht gespeichert werden dürfen.

Zu Absatz 6

Nach Vorgabe des Bundesverfassungsgerichts in seinem Urteil zur Vorratsdatenspeicherung ist als Ausfluss des Verhältnismäßigkeitsgrundsatzes ein grundsätzliches Übermittlungsverbot „für einen engen Kreis von auf besondere Vertraulichkeit angewiesenen Telekommunikationsverbindungen“ verfassungsrechtlich geboten (BVerfGE 125, 260 <334>). Zu denken sei dabei – so das Bundesverfassungsgericht – etwa an die in § 99 Absatz 2 Satz 1 genannten Telekommunikationsverbindungen. Gemäß § 99 Absatz 2 Satz 1 TKG dürfen Einzelverbindungsnachweise nicht Verbindungen zu Anschlüssen von Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen erkennen lassen, die grundsätzlich anonym bleibenden Anrufern ganz oder überwiegend telefonische Beratung in seelischen oder sozialen Notlagen anbieten und die selbst oder deren Mitarbeiter insoweit anderen Verschwiegenheitsverpflichtungen unterliegen. Der Gesetzentwurf geht über die Vorgaben des Bundesverfassungsgerichts hinaus und schließt nicht erst die Übermittlung, sondern schon die Speicherung der Daten aus. Dabei gelten die Regelungen des § 99 Absatz 2 für die Aufnahme dieser Organisationen in Listen, die bei der Bundesnetzagentur geführt und aktualisiert werden, entsprechend.

Zu Absatz 7

Die Regelung in Absatz 7 soll sicherstellen, dass die Daten von den Verpflichteten in einer Weise gespeichert werden, die eine effektive und schnelle Recherche zulässt, so dass Auskunftsersuchen unverzüglich beantwortet werden können.

Zu Absatz 8

Absatz 8 bestimmt, dass die auf Grund des § 113b TKG-E gespeicherten Verkehrsdaten unverzüglich, spätestens jedoch binnen einer Woche nach Ablauf der Speicherfrist nach Absatz 1 Satz 1, zu löschen sind oder deren Löschung sicherzustellen ist. Das Löschen der Daten hat nach dem Stand der Technik zu erfolgen, zu dem der Anforderungskatalog nach § 113f TKG-E Orientierung geben wird. Das Löschen der Daten ist nach § 113e Absatz 1 TKG-E zu protokollieren.

Zu § 113c TKG-E

Die Vorschrift regelt die Verwendung der nach Maßgabe von § 113b TKG-E gespeicherten Verkehrsdaten und enthält eine enge Zweckbegrenzung. Mit dieser ist insbesondere auch eine Verwendung der gespeicherten Daten zur Verfolgung oder Verhinderung von Ordnungswidrigkeiten ausgeschlossen. Eine entsprechende Verwendungsregelung hat das Bundesverfassungsgericht in seinem Urteil zur Vorratsdatenspeicherung im Rahmen der Prüfung der Rechtmäßigkeit der Bestandsdatenauskunft mittels Zuordnung einer (auf Vorrat gespeicherten) dynamischen Internetprotokoll-Adresse zu einem Anschluss zwar nicht grundsätzlich als verfassungswidrig angesehen (BVerfGE 125, 260 <344>). In seinem Beschluss vom 24. Januar 2012 (1 BvR 1299/05) hat das Bundesverfassungsgericht allerdings festgestellt, dass die identifizierende Zuordnung dynamischer Internetprotokoll-Adressen eine besondere Nähe zu konkreten Telekommunikationsvorgängen aufweisen und in den Schutzbereich des Artikels 10 Absatz 1 GG fällt (BVerfGE 130, 151 <181 f.>).

Einer Verwendungsregelung zur Ermöglichung von Bestandsdatenauskünften mittels dynamischer Internetprotokoll-Adressen zur Ermittlung von Ordnungswidrigkeiten steht im Übrigen auch die Vorschrift des § 46 Absatz 3 Satz 1 des Gesetzes über Ordnungswidrig-

keiten entgegen, nach der Auskunftsersuchen über Umstände, die dem Post- und Telekommunikationsgeheimnis unterliegen, unzulässig sind.

Zu Absatz 1

Nach Absatz 1 Nummer 1 dürfen die auf Grund des § 113b TKG-E gespeicherten Daten an eine Strafverfolgungsbehörde übermittelt werden, soweit diese die Übermittlung unter Berufung auf eine gesetzliche Bestimmung verlangt, die eine Erhebung der in § 113b TKG-E genannten Daten erlaubt. Erlaubt ist den Strafverfolgungsbehörden die Erhebung der gespeicherten Daten lediglich unter den engen Voraussetzungen des § 100g Absatz 2 StPO-E.

Absatz 1 Nummer 2 enthält eine Regelung für die Übermittlung von anlasslos gespeicherten Daten an eine Gefahrenabwehrbehörde. Eine solche Übermittlung ist danach zulässig, wenn eine Gefahrenabwehrbehörde, also etwa die Polizei, dies unter Berufung auf eine gesetzliche Befugnis, die ihr eine Erhebung der anlasslos gespeicherten Daten zum Zwecke der Abwehr einer konkreten Gefahr für Leib, Leben oder Freiheit einer Person oder den Bestand des Bundes oder eines Landes erlaubt, verlangt. Damit wird Landespolizeibehörden die Möglichkeit eröffnet, bei Vorliegen entsprechender Befugnisnormen verpflichtend gespeicherte Verkehrsdaten zu erheben.

Absatz 1 Nummer 3 enthält eine Regelung für die Fälle, in denen die verpflichtend gespeicherten Daten vom Erbringer öffentlich zugänglicher Telekommunikationsdienste herangezogen werden dürfen, um für dynamische Internetprotokoll-Adressen Bestandsdatenauskünfte nach § 113 Absatz 1 Satz 3 zu erteilen.

Ob die Behörden berechtigt sind, ein solches Verlangen im Sinne der Nummern 1 bis 3 an den Erbringer öffentlich zugänglicher Telekommunikationsdienste zu richten, ist nicht Regelungsgegenstand von § 113c TKG-E, sondern bestimmt sich nach den für die Strafverfolgungsbehörden maßgeblichen Regelungen des Strafprozessrechts, hier der §§ 100g und 100j StPO. § 100j Absatz 2 StPO verweist deswegen nicht nur auf § 113 Absatz 1 Satz 3 des TKG, sondern bezieht ausdrücklich § 113c Absatz 1 mit ein, um die Auskunftserteilung aus diesen Daten auf Seiten der abrufenden Behörde zu legitimieren. Die Behörden haben in eigener Verantwortung zu prüfen, ob die Voraussetzungen für ein Übermittlungsverlangen vorliegen. Im Fall des § 100g StPO ist zudem grundsätzlich eine entsprechende gerichtliche Anordnung einzuholen. Dem Erbringer kommt insoweit weder eine inhaltliche Prüfungspflicht noch -befugnis zu.

Mit diesen Regelungen wird den Vorgaben des Bundesverfassungsgerichts entsprochen (BVerfGE 125, 260 <329-332> und <355f> bzw. zur mittelbaren Datenverwendung <340-344, 356>).

Zu Absatz 2

Absatz 2 bestimmt, dass die auf Grund des § 113b TKG-E gespeicherten Daten nicht für andere Zwecke als die in Absatz 1 genannten oder zur Protokollierung nach § 113e TKG-E verwendet werden dürfen. Verstöße gegen diese Verpflichtung werden bußgeldbewehrt (§ 149 Absatz 1 Nummer 39 TKG-E).

Zu Absatz 3

Auch an die Übermittlung der Daten an die Berechtigten sind strenge Anforderungen zu stellen, um die Sicherheit der Daten zu gewährleisten. Dies geschieht, indem die in § 110 TKG geregelten Maßnahmen auch für die Übermittlung der nach § 113b TKG-E gespeicherten Daten gelten. Auf die Vorgaben der Rechtsverordnung nach § 110 Absatz 2 und der Technischen Richtlinie nach § 110 Absatz 3 wird Bezug genommen. Das Bundesverfassungsgericht hat zudem verlangt, dass die Daten auch durch die nach dem TKG Ver-

pflichteten zu kennzeichnen sind (BVerfGE 125, 260 <346>), um zu gewährleisten, dass die Zweckbindung auch bei der weiteren Vewendung der Daten aufrechterhalten werden kann.

Zu § 113d TKG-E

§ 113d TKG-E enthält Vorgaben zur Gewährleistung der Sicherheit der nach § 113b Absatz 2 bis 4 TKG-E gespeicherten Daten und soll entsprechende Vorgaben des Bundesverfassungsgerichts umsetzen. Die Regelung des § 113d gibt in Verbindung mit § 113f TKG-E einen besonders hohen Sicherheitsstandard verbindlich vor. Die technische Konkretisierung des vorgegebenen Maßstabs soll mit der Vorschrift des § 113f TKG-E der Bundesnetzagentur anvertraut werden (vgl. BVerfGE 125, 260 <325-327>).

Satz 1 gibt vor, dass die nach § 113b Absatz 2 bis 4 TKG-E gespeicherten Daten durch technische und organisatorische Maßnahmen nach dem Stand der Technik gegen unbefugte Kenntnisnahme und Verwendung geschützt werden. Diese besonderen Sicherungsanforderungen erstrecken sich nicht auf die nach § 113b Absatz 4 zu speichernden Daten über die geografischen Lagen und Hauptstrahlrichtungen der die Funkzellen versorgenden Funkantennen. Solche Daten sind keine Verkehrsdaten und unabhängig von konkreten Telekommunikationsvorgängen, so dass es des besonders hohen Schutzes, an denen die nach § 113b Absatz 2 bis 4 zu speichernden Verkehrsdaten teilhaben, insoweit nicht bedarf.

Satz 2 bestimmt, dass die technischen und organisatorischen Maßnahmen zum Schutze der nach § 113b Absatz 2 bis 4 zu speichernden Daten insbesondere umfassen:

– den Einsatz eines als besonders sicher geltenden Verschlüsselungsverfahrens (Nummer 1),

– die Speicherung in gesonderten, von den für die üblichen betrieblichen Aufgaben getrennten Speichereinrichtungen (Nummer 2),

– die vor dem Zugriff aus dem Internet mit einem hohen Schutz versehene Speicherung, die insbesondere durch eine physische Trennung vom Internet zu gewährleisten ist (Nummer 3),

– die Beschränkung des Zutritts zu den Datenverarbeitungsanlagen auf besonders ermächtigte Personen (Nummer 4) und

– die Gewährleistung des Vier-Augen-Prinzips für den Zugriff auf die Daten (Nummer 5).

Die Regelung in Nummer 3 beruht auf Ausführungen des Bundesverfassungsgerichts in seinem Urteil zur Vorratsdatenspeicherung, in denen an die sachverständigen Äußerungen in der mündlichen Verhandlung sowie in den schriftlichen Stellungnahmen zu möglichen Instrumenten zur Erhöhung der Datensicherheit angeknüpft wird (BVerfGE 125, 260 <325 f.>). Genannt wird in diesem Zusammenhang unter anderem eine getrennte Speicherung der Daten auf „vom Internet entkoppelten Rechnern“.

Das von Nummer 5 vorgegebene Vier-Augen-Prinzip besagt, dass der Zugriff auf die anlasslos gespeicherten Daten nicht einer Person allein möglich sein darf, sondern ablauforganisatorisch so auszugestalten ist, dass für einen Zugriff auf die Daten im Einzelfall die Mitwirkung mindestens einer weiteren Person zwingend erforderlich ist. Vorstellbar ist beispielsweise, dass die Abfragedaten (etwa Aktenzeichen, Name des Anschlussinhabers) ausschließlich durch eine erste Person eingegeben werden, die Ausgabe der anlasslos gespeicherten Daten aus der Datenbank aber erst durch eine im Einzelfall passwortgestützte Freigabe durch eine zweite Person erfolgen kann. Um einen Automatismus

bei der zweiten Person zu vermeiden, könnte aus den von der ersten Person eingegebenen Abfragedaten ein Code generiert werden, der durch die zweite Person zur Freischaltung zusammen mit dem Passwort einzugeben wäre.

Die konkrete Ausgestaltung der Maßnahmen hat nach dem Stand der Technik zu erfolgen. Orientierung gibt der in § 113f TKG-E vorgesehene Anforderungskatalog, in dem konkretisiert werden kann, welches Verschlüsselungsverfahren, welche Schlüssellänge, welches Verfahren des Schlüsselmanagements oder welche organisatorische bzw. technische Ausgestaltung des Vier-Augen-Prinzips dem Stand der Technik entsprechen.

Zu § 113e TKG-E

Die Regelung des § 113e TKG-E orientiert sich am Vorbild des § 112 Absatz 4 Satz 4 bis 6 TKG und setzt entsprechende Vorgaben des Bundesverfassungsgerichts zur Protokollierung um (BVerfGE 125, 260 <325 f>).

Zu Absatz 1

Absatz 1 gibt die revisionssichere Protokollierung jedes Zugriffs auf die auf Grundlage des § 113b TKG-E gespeicherten Daten vor. Das Protokoll soll einer für die Kontrolle der Einhaltung der Vorschriften über den Schutz personenbezogener Daten zuständigen Stelle die Prüfung ermöglichen, ob die Zugriffe rechtmäßig erfolgt sind.

Unter den Begriff des Zugriffs fallen alle lesenden Zugriffe, das Kopieren, das Ändern (zum Beispiel im Rahmen von Fehlerkorrektur- und Plausibilitätsprüfungen), das Löschen und das Sperren der Daten. Zu protokollieren sind der Zeitpunkt, der Zweck und die Art des Zugriffs, Angaben, welche die auf die nach § 113b verpflichtend gespeicherten Daten zugreifenden Personen eindeutig kennzeichnen. Angaben im Zusammenhang mit der Verwendung der Daten nach § 113c Absatz 1 TKG-E werden den Regelungen der Protokollierung in der Rechtsverordnung nach § 110 Absatz 2 folgend protokolliert.

Zu Absatz 2

Absatz 2 bestimmt, dass die Protokolldaten nicht für andere Zwecke als zur Datenschutzkontrolle verwendet werden dürfen.

Zu Absatz 3

Die Löschungsregelung in Absatz 3 folgt dem Vorbild des § 112 Absatz 4 Satz 6 TKG.

Zu § 113f TKG-E

Nach § 113f TKG-E ist ein besonders hoher Sicherheits- und Qualitätsstandard bei der Umsetzung der Verpflichtungen nach den §§ 113b bis 113e TKG-E zu gewährleisten. Die technische Konkretisierung des vorgegebenen Maßstabs soll der Bundesnetzagentur als Aufsichtsbehörde anvertraut werden (vgl. BVerfGE 125, 260 <327>).

Die Regelung des § 113f TKG-E ergänzt die Vorschrift des § 109 Absatz 6 TKG.

Zu Absatz 1

Satz 1 verpflichtet die Erbringer öffentlich zugänglicher Telekommunikationsdienste, bei der Umsetzung der Verpflichtungen der §§ 113b bis 113e TKG-E einen besonders hohen Standard der Datensicherheit und Datenqualität zu gewährleisten.

Satz 2 bestimmt, dass die Bundesnetzagentur unter Beteiligung des Bundesamtes für Sicherheit in der Informationstechnik und der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit einen Katalog von Anforderungen für die technischen Vorkehrungen und sonstigen Maßnahmen zu Erfüllung der Verpflichtungen aus den §§ 113b bis 113e TKG-E erstellt. Die Einhaltung des in Satz 1 vorgegebenen Standards wird vermutet, wenn der Verpflichtete die Anforderungen des Katalogs erfüllt.

Der Katalog soll insbesondere Anforderungen enthalten:

– in Bezug auf die Löschung der Daten nach § 113b Absatz 8 TKG-E, wobei vorzusehen ist, dass die Löschung so zu erfolgen hat, dass eine Wiederherstellung der Daten auch unter Einbeziehung von Sicherungskopien unmöglich ist,

– in Bezug auf die Gewährleistung der Sicherheit der Daten nach § 113d TKG-E,

– für eine revisionssichere Protokollierung nach § 113e TKG-E und

– hinsichtlich der Gewährleistung eines besonders hohen Standards der Datenqualität nach § 113f Absatz 1 Satz 1 TKG-E, zum Beispiel durch den Einsatz von automatisierten Fehlererkennungsverfahren, Plausibilitätsprüfungen und Maßnahmen zur Sicherstellung der Genauigkeit zu speichernder Uhrzeiten.

Zu Absatz 2

Absatz 2 gibt vor, dass die Bundesnetzagentur fortlaufend die im Katalog enthaltenen Anforderungen überprüft und hierbei den Entwicklungsstand der Technik und der Fachdiskussion berücksichtigt, um festzustellen, ob der Katalog geändert werden muss. Besteht Änderungsbedarf, ist der Katalog unter Beteiligung des Bundesamtes für Sicherheit in der Informationstechnik und der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit unverzüglich anzupassen.

Zu Absatz 3

Absatz 3 bestimmt mit der Bezugnahme auf Regelungen des § 109 Absatz 6 Satz 2 und 3 TKG, dass die Bundesnetzagentur bei der Erstellung des Katalogs den Herstellern, den Verbänden der Betreiber öffentlicher Telekommunikationsnetze und den Verbänden der Erbringer öffentlich zugänglicher Telekommunikationsdienste Gelegenheit zur Stellungnahme gibt und den Katalog veröffentlicht.

Die Bundesnetzagentur kann gemäß § 113f Absatz 3 TKG-E in Verbindung mit § 109 Absatz 7 TKG anordnen, dass sich die nach § 113b TKG-E Verpflichteten einer Überprüfung durch eine qualifizierte unabhängige Stelle oder eine zuständige nationale Behörde unterziehen, in der festgestellt wird, ob die Anforderungen aus § 113b Absatz 7 und 8, § 113c, § 113e Absatz 1 sowie § 113f Absatz 1 Satz 1 erfüllt sind. Der Verpflichtete hat eine Kopie des Überprüfungsberichts unverzüglich an die Bundesnetzagentur zu übermitteln. Er soll auch die Kosten dieser Überprüfung tragen.

Zu § 113g TKG-E

Die Regelung des § 113g TKG-E ergänzt die Vorschrift des § 109 Absatz 4 TKG für die nach § 113a Absatz 1 TKG-E Verpflichteten und setzt damit Vorgaben des Bundesverfassungsgerichts hinsichtlich einer nachprüfbaren regelmäßigen Anpassung der Sicherheitsmaßnahmen um (BVerfGE 125, 260 <326, 350 f.>).

Satz 1 bestimmt, dass der nach § 113a Absatz 1 TKG-E Verpflichtete in das von ihm nach § 109 Absatz 4 TKG zu erstellende Sicherheitskonzept auch aufzunehmen hat, welche Systeme zur Erfüllung der Vorgaben der §§ 113b bis 113e TKG-E betrieben werden, von

welchen Gefährdungen für diese Systeme auszugehen ist und welche technischen Vorkehrungen oder sonstigen Maßnahmen zur Erfüllung der Verpflichtungen aus den §§ 113b bis 113e TKG-E getroffen oder geplant sind, um diesen Gefährdungen entgegenzuwirken. Die Bezeichnung „Systeme“ schließt Anlagen und organisatorische Vorkehrungen ein.

Satz 2 enthält Anforderungen in Bezug auf die Vorlage und Wiedervorlage des Sicherheitskonzeptes: Das Sicherheitskonzept ist der Bundesnetzagentur erstmals unverzüglich nach der Aufnahme der Speicherung nach § 113b TKG-E sowie bei jeder Änderung erneut vorzulegen. Werden an dem Sicherheitskonzept keine Änderungen vorgenommen, genügt es, dass der Verpflichtete dies gegenüber der Bundesnetzagentur im Abstand von jeweils zwei Jahren erklärt, eine regelmäßige Neuvorlage des unveränderten Konzeptes ist damit nicht erforderlich.

Zu Nummer 3 (§ 121 Absatz 1 TKG-E)

Die Regelung soll eine für die Öffentlichkeit transparente Kontrolle unter Einbeziehung der oder des unabhängigen Datenschutzbeauftragten gewährleisten und damit eine entsprechende Vorgabe des Bundesverfassungsgerichts umsetzen (BVerfGE 125, 260 <327>).

Vorgegeben wird, dass die Bundesnetzagentur in ihrem Tätigkeitsbericht, der den gesetzgebenden Körperschaften des Bundes alle zwei Jahre vorgelegt wird, mitteilt, in welchem Umfang und mit welchen Ergebnissen sie Sicherheitskonzepte nach § 113g TKG-E und deren Einhaltung überprüft hat und ob und welche Beanstandungen und weiteren Ergebnisse die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit insoweit an die Bundesnetzagentur übermittelt hat.

Zu Nummer 4 (§ 149 TKG-E)

Zu Buchstabe a

Mit der Ergänzung des Katalogs der Ordnungswidrigkeiten in Absatz 1 um die Nummern 36 bis 44 soll die Einhaltung von Verpflichtungen aus den §§ 113b bis 113e und 113g TKG-E und damit insbesondere ein umfassender und wirksamer Schutz der zu speichernden Daten gewährleistet werden.

Zu Buchstabe b

Die Änderung in Absatz 2 trägt dem Urteil des Bundesverfassungsgerichts Rechnung, wonach es nach geltender Rechtslage an einem ausgeglichenen Sanktionensystem fehle, das Verstößen gegen die Datensicherheit kein geringeres Gewicht beimisst als Verstößen gegen die Speicherungspflichten selbst (BVerfGE 125, 260 <351>). Absatz 2 sieht daher vor, dass sämtliche Verstöße gegen die Verpflichtungen, die sich hinsichtlich der nach § 113b TKG-E zu speichernden Daten ergeben, einheitlich mit einer Geldbuße bis zu fünfhunderttausend Euro geahndet werden können. Für Verstöße gegen die Pflicht zur Protokollierung aller Zugriffe auf die gespeicherten Daten (§ 113e TKG-E) ist eine Geldbuße bis zu 300 000 Euro und für die nicht vollständige oder nicht rechtzeitige Vorlage der in § 113g TKG-E aufgeführten Angaben in das Sicherheitskonzept eine Geldbuße bis zu 100 000 Euro vorgesehen.

Zu Nummer 5 (§ 150 Absatz 13 TKG-E)

Der neue Absatz 13 Satz 1 legt fest, dass die Speicherungsverpflichtung nach § 113b TKG-E spätestens 18 Monate nach der Verkündung dieses Gesetzes zu erfüllen ist. Satz 2 bestimmt, dass die Bundesnetzagentur den nach § 113f Absatz 1 TKG-E zu erstellenden Anforderungskatalog spätestens zwölf Monate nach Verkündung dieses Gesetzes veröffentlicht.

Damit soll dem Umstand Rechnung getragen werden, dass sowohl die nach § 113b TKG-E Verpflichteten als auch die weiteren beteiligten Stellen – Bundesnetzagentur, Bundesamt für Sicherheit in der Informationstechnik und der oder die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit – die gesetzlichen Vorgaben nicht ohne weiteres kurzfristig umsetzen können, sondern es hierzu bestimmter technischer, organisatorischer oder sonstiger (Vorbereitungs-)Maßnahmen bedarf. Aus diesem Grunde erscheint es angemessen, die Verpflichtungen zu verschiedenen Zeitpunkten in Kraft treten zu lassen. Die Regelung soll insbesondere die Voraussetzung dafür schaffen, dass der von der Bundesnetzagentur zu erstellende Anforderungskatalog nach § 113f TKG-E vor dem Inkrafttreten der Speicherungs- und damit verbunden Verpflichtungen nach den §§ 113b bis 113e und 113g TKG-E veröffentlicht werden kann.

Zu Artikel 3 (Änderung des Einführungsgesetzes zur Strafprozessordnung - EGStPO)

§ 12 EGStPO-E trifft zwei Übergangsregelungen. Da die Speicherpflicht nach § 150 TKG-E nicht mit Inkrafttreten des Gesetzes umgesetzt werden kann, sondern erst spätestens 18 Monate nach der Verkündung zu erfüllen ist, wäre für gespeicherte Standortdaten in der Zwischenzeit kein Abruf möglich, denn der geänderte § 100g Absatz 1 sieht einen solchen nicht mehr vor; § 100g Absatz 2 hingegen kann erst Wirkung entfalten, wenn die Daten tatsächlich gespeichert werden.

Außerdem muss eine Übergangsregelung für die in § 101b vorgesehenen Statistikpflichten vorgesehen werden. Angeknüpft wird dabei an den in § 150 Absatz 13 TKG-E vorgesehenen Zeitpunkt, ab dem die Speicherungsverpflichtung nach § 113b TKG-E spätestens zu erfüllen ist. Für das diesem Zeitpunkt nachfolgende Berichtsjahr sind die Neuregelungen anzuwenden, für die vorangehenden Berichtsjahre die bisherige Regelung in § 100g Absatz 4 StPO.

Zu Artikel 4 (Änderung des Justizvergütungs- und –entschädigungsgesetzes - JVEG)

Zu Nummer 1 (Inhaltsübersicht)

Die Anlage 3 zum JVEG wird bisher in der Inhaltsübersicht nicht genannt. Die entsprechende Angabe soll nunmehr eingefügt werden.

Zu Nummer 2 (§ 6 Absatz 1 JVEG-E)

Der Verweis in § 6 Absatz 1 JVEG auf § 4 Absatz 5 Satz 1 Nummer 5 Satz 2 des Einkommensteuergesetzes muss wegen der Änderung des Einkommensteuergesetzes durch Artikel 1 Nummer 2 Buchstabe a des Gesetzes zur Änderung und Vereinfachung der Unternehmensbesteuerung und des steuerlichen Reisekostenrechts vom 20. Februar 2013 (BGBl. I S. 285) angepasst werden. Die Verweisung soll entsprechend der Regelung in § 6 Absatz 1 Satz 2 des Bundesreisekostengesetzes erfolgen, der durch Artikel 3 des genannten Steuergesetzes neugefasst worden ist.

Zu Nummer 3 (§ 23 Absatz 2 Satz 1 JVEG-E)

Die Vorschrift gilt auch im Bußgeldverfahren vor der Verwaltungsbehörde. Daher soll diese als „Verfolgungsbehörde“ ausdrücklich genannt werden wie dies bereits in § 13 Absatz 2 Satz 1 und Absatz 6 Satz 2 JVEG der Fall ist.

Zu Nummer 4 (Vorbemerkung Anlage 2)

Es handelt sich um eine redaktionelle Korrektur.

Zu Nummer 5 (Anlage 3)

Die Entschädigungsregelungen für Auskünfte über Verkehrsdaten oder über Bestandsdaten, zu deren Erteilung auf Verkehrsdaten zurückgegriffen werden muss, sollen für diejenigen Fälle modifiziert werden, in denen ein Rückgriff auf Daten erforderlich wird, die aufgrund der Speicherpflicht nach § 113b Absatz 2 bis 4 TKG gespeichert werden. Das insoweit in § 113d Satz 2 Nummer 5 TKG-E vorgegebene Vier-Augen-Prinzip führt zu einem erhöhten Personaleinsatz. Daher müssen die Entschädigungspauschalen für diese Fälle angehoben werden.

Der Vorschlag sieht neben der Einfügung der neuen Nummern 202 und 401 aus Gründen der Übersichtlichkeit eine Neufassung des Abschnitts 3 der Anlage 3 zum JVEG vor. In den neuen Nummern 202, 301, 304, 307, 309, 311, 315 bis 317, 319 und 401 werden bei der Einbeziehung von Daten, die nach § 113b Absatz 2, 3 oder 6 TKG gespeichert werden, um 20 Prozent erhöhte Pauschalen vorgeschlagen, wobei die Beträge jeweils auf volle 5 Euro gerundet sind. Dem Vorschlag liegt die Annahme zugrunde, dass für das Vier-Augen-Prinzip Gesamtaufwand gegenüber der Durchführung durch eine Einzelperson (nur) leicht erhöht, da die zweite Person die Daten nicht erneut eingeben muss, sondern die Eingabe lediglich prüft und freigibt.

Die Entschädigung soll sich auch dann insgesamt nach den erhöhten Pauschalen richten, wenn nur für einen Teil der Daten, auf die zugegriffen wird, das Vier-Augen-Prinzip vorgeschrieben ist.

Zu Artikel 5 (Änderung des Strafgesetzbuches)

Zu Nummer 1 (Inhaltsübersicht)

Es handelt sich um eine redaktionelle Folgeänderung zur Einfügung des § 202d StGB (Artikel 3 Nummer 2).

Zu Nummer 2 (§ 202d StGB-E)

Der neue Straftatbestand der Datenhehlerei soll wegen seines Zusammenhangs mit den §§ 202a bis 202c StGB im Fünfzehnten Abschnitt des Besonderen Teils des Strafgesetzbuches (Verletzung des persönlichen Lebens- und Geheimbereichs) verortet werden. Die §§ 202a bis 202c StGB schützen das formelle Datengeheimnis desjenigen, der aufgrund seines Rechts an dem gedanklichen Inhalt über eine Weitergabe und Übermittlung der Daten entscheidet (Münchener Kommentar/Graf, 2. Auflage, § 202a Rz. 2) und damit das Interesse an der Aufrechterhaltung des Herrschaftsverhältnisses über eine Information (Leipziger Kommentar/Hilgendorf, 12. Auflage, § 202a Rz. 6), ohne dass sie eine Verletzung des persönlichen Lebens- oder Geheimbereichs voraussetzen (vgl. Bundestagsdrucksache 10/5058, S. 28). Hieran knüpft der neue Tatbestand an, der das formelle Datengeheimnis vor einer Fortsetzung und Vertiefung seiner durch die Vortat erfolgten Verletzung schützt.

Zu Absatz 1

Nach der Vorschrift macht sich strafbar, wer Daten, die ein anderer durch eine rechtswidrige Tat erlangt hat, sich oder einem anderen verschafft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, um sich oder einen Dritten zu bereichern oder einen anderen zu schädigen.

Der Straftatbestand erfasst nur nicht öffentlich zugängliche Daten. Die Regelung nimmt dabei auf die Legaldefinition von Daten in § 202a Absatz 2 StGB (Ausspähen von Daten) Bezug. Daten im Sinne von § 202d StGB sind demnach nur solche, die elektronisch,

magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

Der Ausschluss von Daten, die allgemein zugänglich sind, folgt daraus, dass es in diesen Fällen an einer Beeinträchtigung des von der Vorschrift geschützten formellen Datengeheimnisses fehlt. Dass der Täter nicht auf die allgemein zugängliche Quelle zurückgreift, sondern sich die Vortat zunutze macht, vermag daher eine Strafwürdigkeit nicht zu begründen. Öffentlich zugängliche Daten sind in § 10 Absatz 5 Satz 2 BDSG im Hinblick auf automatisierte Abrufverfahren definiert, als Daten, die jedermann, sei es ohne oder nach vorheriger Anmeldung, Zulassung oder Entrichtung eines Entgelts nutzen kann. Daher sind insbesondere veröffentlichte, urheberrechtlich geschützte Werke auch dann allgemein zugänglich, wenn für ihre Nutzung bezahlt werden muss. Entsprechende Werke, die vom Vortäter durch eine Urheberrechtsverletzung erlangt wurden, unterfallen daher nicht dem Tatbestand.

Die Daten müssen von einem anderen durch eine rechtswidrige Tat (§ 11 Absatz 1 Nummer 5 StGB) erlangt worden sein. Damit kommen als Vortat der Datenhehlerei alle Taten in Betracht, die ein Strafgesetz verwirklichen, unabhängig von der Schuld des Täters oder vom Vorliegen eines Strafantrages, so wie dies auch bei der Sachhehlerei der Fall ist (vgl. Fischer, StGB, 62. Auflage, § 259 Rz. 6). Vortaten können daher nicht nur das Abfangen und Ausspähen von Daten (§§ 202a, 202b StGB) sein, sondern beispielsweise auch Diebstahl (§ 242 StGB), Betrug (§ 263 StGB), Computerbetrug (§ 263a StGB), Nötigung (§ 240 StGB) und die Fälschung technischer Aufzeichnungen (§ 269 StGB), soweit sie sich im Einzelfall auch gegen die formelle Verfügungsbefugnis des Berechtigten richten und der Täter dadurch Daten erlangt hat. Ebenfalls in Betracht kommt das Erlangen von Daten im Wege der Vorbereitung der Fälschung von Zahlungskarten mit Garantiefunktion (§ 152b Absatz 5 in Verbindung mit § 149 Absatz 1 Nummer 1 StGB; zum sog. Skimming vgl. BGH, Beschluss vom 29. Januar 2014 – 1 StR 654/13). Die Datenhehlerei kommt schließlich ebenso als Vortat in Betracht wie grundsätzlich auch Straftaten nach dem Bundesdatenschutzgesetz.

Die Vortat muss sich (auch) gegen die formelle Verfügungsbefugnis des Berechtigten richten. Berechtigter ist derjenige, der über die Daten verfügen darf (vgl. Leipziger Kommentar/Hilgendorf, 12. Auflage, § 202a Rz. 26), also grundsätzlich derjenige, der die Daten gesammelt und abgespeichert hat oder auf dessen Veranlassung die Speicherung erfolgt ist (vgl. BayOLG, Urteil vom 14. Juni 1993, JR 1994, 476, 477; Münchener Kommentar/Graf, 2. Auflage, § 202a Rz. 19). Das Eigentum und der Besitz am Datenträger sind dafür nicht entscheidend. Die Berechtigung ist von der datenschutzrechtlichen Betroffenheit zu unterscheiden. Betroffener ist die bestimmte oder bestimmbare natürlichen Person, zu der die Daten Einzelangaben über persönliche oder sachliche Verhältnisse enthalten (§ 3 Absatz 1 BDSG). Die formelle Berechtigung und die datenschutzrechtliche Betroffenheit können in einer Person zusammenfallen.

Entsprechend der Rechtslage bei der Sachhehlerei (vgl. Maurach/Schroeder/Maiwald, Strafrecht Besonderer Teil, 10. Auflage, § 39 Rz. 20) ist ausreichend, dass die Vortat unabhängig von ihrer systematischen Einordnung in ihren praktischen Auswirkungen die formelle Verfügungsbefugnis des Berechtigten verletzt. An einer gegen die formelle Verfügungsbefugnis gerichteten Vortat fehlt es insbesondere, wenn das Delikt nur gegen öffentliche Interessen verstößt wie beispielsweise § 184d StGB (Verbreitung pornographischer Darbietung durch Rundfunk, Medien- oder Teledienste). Dies gilt auch, wenn der Vortäter Daten selbst erstellt und sich dabei nach dem Bundesdatenschutzgesetz strafbar macht (vgl. § 44 BDSG), da eine Beeinträchtigung der formellen Verfügungsbefugnis voraussetzt, dass die Daten zuvor der Verfügungsmacht des Berechtigten unterlagen.

Nicht durch eine rechtswidrige Tat erlangt sind Daten, die dem Vortäter bereits zur Verfügung stehen und die er unter Verletzung des Urheberrechts vervielfältigt. Ebenso wenig erlangt der Vortäter Daten durch eine rechtswidrige Tat, wenn er lediglich eine Vertrags-

verletzung, ein Disziplinarvergehen oder eine Ordnungswidrigkeit begeht. Als Vortat ist es daher nicht ausreichend, wenn in einem berechtigt genutzten System Daten lediglich unter Verletzung von vertraglichen Zugriffsbeschränkungen erlangt werden.

Wie sich aus der Formulierung „erlangt hat“ ergibt, muss die Vortat entsprechend der Regelung bei der Sachhehlerei (§ 259 StGB) bereits vollendet sein, wenn der Täter die Daten sich oder einem anderen verschafft, einem anderen überlässt, verbreitet oder sonst zugänglich macht. Nicht tatbestandsmäßig ist es daher beispielsweise, wenn die Vortat erst durch die Übermittlung der Daten an den Hehler begangen wird (vgl. zur Rechtslage bei der Sachhehlerei, BGH Beschluss vom 24. Oktober 2012 – 5 StR 392/12).

Der Täter muss die vom Vortäter erlangten Daten sich oder einem anderen verschaffen, einem anderen überlassen, verbreiten oder sonst zugänglich machen. Diese Tathandlungen sind § 202c Absatz 1 StGB (Vorbereiten des Ausspähens und Abfangens von Daten) entnommen, sodass die dazu in Rechtsprechung und Literatur erfolgte Auslegung herangezogen werden kann. Verzichtet wird auf die Übernahme der in § 259 Absatz 1 StGB enthaltenen Tatbestandsvariante des „Ankaufens“ und der in § 202c StGB enthaltenen Tatbestandsvariante des „Verkaufens“, für die umstritten ist, ob es schon durch den schuldrechtlichen Abschluss eines (möglicherweise zivilrechtlich nichtigen) Kaufvertrages erfüllt werden kann (vgl. Fischer, StGB, 61. Auflage, § 202c Rz. 7), oder ob dafür auch die Übertragung der Verfügungsmacht über die Daten erforderlich ist, so dass es sich beim Ankauf um einen Unterfall des „Verschaffens“ handelt (vgl. Leipziger Kommentar/Hilgendorf, StGB, 12. Auflage, § 202c Rz. 22, 24). Ungeachtet der von der Rechtsprechung noch nicht entschiedenen Auslegungsfrage bei § 202c StGB soll jedenfalls eine Strafbarkeit wegen Datenhehlerei voraussetzen, dass der Täter die Daten sich oder einem Dritten verschafft, also durch die Tathandlung die tatsächliche Verfügungsmacht über sie erlangt wird. Der bloß vertraglich vereinbarte Ankauf der Daten vom Vortäter bzw. ihr vertraglich vereinbarter Verkauf an einen Dritten führen noch nicht zu einer Fortsetzung oder Vertiefung der Verletzung des formellen Datengeheimnisses und überschreiten damit nicht die Schwelle der Strafwürdigkeit.

Wie bei der Sachhehlerei ist ein einverständliches Zusammenwirken zwischen Täter und Vortäter erforderlich. Der Täter muss die vom Vortäter durch seine rechtswidrige Tat geschaffene Möglichkeit, Zugriff auf die Daten nehmen zu können, im Einvernehme mit dem Vortäter nutzen. Eine Strafbarkeit wegen Datenhehlerei scheidet aus, wenn der Täter zwar Kenntnis von der Vortat hat, er aber nicht den Vortäter als Quelle der Daten nutzt, sondern auf andere Weise darauf zugreift. Ein unmittelbarer Kontakt zwischen Täter und Vortäter ist nicht erforderlich, sodass die Strafbarkeit nicht wegen des Einsatzes von Mittelmännern ausscheidet.

Eine Strafbarkeit scheidet aus, wenn der durch die Vortat verletzte Berechtigte die ihm gestohlenen Daten zurückkauft (vgl. Münchener Kommentar/Maier, 2. Auflage, § 259 Rz. 60). Eine Täterschaft des lediglich datenschutzrechtlich Betroffenen kommt dagegen (ebenso wie bei § 202a StGB, vgl. Münchener Kommentar/Graf, 2. Auflage, § 202a Rz. 19) in Betracht.

Der Täter muss vorsätzlich handeln. Von seinem Vorsatz muss insbesondere der Umstand erfasst sein, dass die Daten von einem anderen durch eine rechtswidrige Tat erlangt worden sind. Wie bei der Sachhehlerei ist dafür erforderlich, dass der Täter die als möglich und nicht ganz fernliegend erkannte Tatbestandsverwirklichung billigend in Kauf nimmt oder sich um des erstrebten Zieles willen wenigstens mit ihr abfindet (BGH, Beschluss vom 23. November 1999 – 4 StR 491/99, wistra 2000, S. 177 f.). Allein das Bewusstsein, dass die Sache aus irgendeiner rechtswidrigen Tat stammt, reicht zur Vorsatzbegründung nicht aus (BGH, Beschluss vom 13. November 2012 – 3 StR 364/12, NStZ-RR 2013, S. 79). Die genauen Einzelheiten der Vortat, das heißt ihre Art, die Umstände ihrer Begehung oder die Person des Vortäters, müssen nicht bekannt sein (BeckOK StGB/Ruhmannseder StGB § 259, Rz. 40). Auch den Umstand, dass es sich um nicht

öffentlich zugängliche Daten handelt, hat der Täter in seinen Vorsatz aufzunehmen. Der Vorsatz muss zum Zeitpunkt der Tathandlung gegeben sein (vgl. Schönke/Schröder/Stree/Hecker, StGB § 259, Rz. 39). Erfährt der Täter nachträglich von der illegalen Herkunft der Daten, so erfüllt er den Tatbestand nur, wenn er im Anschluss daran tatbestandliche Handlungen wie das Verbreiten der inkriminierten Daten vornimmt (Schönke/Schröder/Stree/Hecker, StGB, 29. Auflage, § 259, Rz. 41).

Der Täter muss mit der Absicht handeln, sich oder einen Dritten zu bereichern oder einen anderen zu schädigen. Dies entspricht der Regelung des § 44 Absatz 1 BDSG, so dass die hierzu von Rechtsprechung und Literatur entwickelte Auslegung herangezogen werden kann. Eine (Fremd-)Bereicherungsabsicht liegt danach vor, wenn nach der Vorstellung des Täters die Tat auf die Erlangung eines Vermögensvorteils für sich selbst oder einen Dritten gerichtet ist, wobei hinsichtlich der Bereicherung dolus directus 1. Grades erforderlich ist (BeckOK DatenSR/Holländer BDSG § 44, Rz. 9). Im Gegensatz zu § 263 StGB kann dieser Vermögensvorteil rechtswidriger Natur sein, muss es aber nicht (vgl. Simitis, BDSG, § 3 Rz. 6). Schädigungsabsicht liegt bei jedem vom Täter beabsichtigten, auch immateriellen Nachteil für eine andere Person vor (beispielsweise den Datenhandel zum Zwecke der öffentlichen Bloßstellung im Internet), wobei es ihm darauf ankommen muss, einen anderen durch die Tatbestandsverwirklichung zu schädigen (BeckOK DatenSR/Holländer BDSG, § 44 Rz. 11).

Die Tat ist mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bedroht. Dieser Strafrahmen entspricht der Strafandrohung des § 202a Absatz 1 StGB, der ebenso wie die Datenhehlerei das formelle Datengeheimnis schützt.

Zu Absatz 2

Die Strafe darf nicht schwerer sein als die für die Vortat angedrohte Strafe. Die Regelung entspricht der Vorschrift des § 258 Absatz 3 StGB (Strafvereitelung) und trägt dem Umstand Rechnung, dass als Vortaten auch Delikte mit geringerer Strafandrohung in Betracht kommen, wie beispielsweise das Abfangen von Daten nach § 202b StGB. Die durch die Datenhehlerei erfolgende Aufrechterhaltung und Vertiefung der Verletzung des formellen Datengeheimnisses soll nicht schwerer bestraft werden als die Verletzung dieses Rechtsguts durch die Vortat.

Zu Absatz 3

§ 202d Absatz 3 StGB sieht einen Tatbestandsausschluss für Handlungen vor, die ausschließlich zu dem Zwecke der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen. Dazu gehören insbesondere Handlungen von Amtsträgern, mit denen Daten ausschließlich der Verwertung in einem Besteuerungsverfahren, einem Strafverfahren oder einem Ordnungswidrigkeitenverfahren zugeführt werden sollen.

Die Regelung entspricht dem in § 184b Absatz 5 StGB (Besitz kinderpornografischer Schriften) vorgesehenen Tatbestandsausschluss. Durch die Regelung wird sichergestellt, dass Daten zu Ermittlungszwecken verwendet werden dürfen. Der Tatbestandsausschluss gilt für Amtsträger (§ 11 Absatz 2 Nummer 2 StGB) und auch für aufgrund eines privatrechtlichen Auftrages im konkreten Einzelfall von einem Amtsträger beauftragte behördenexterne Personen, die den Strafverfolgungsbehörden Besitz an Daten verschaffen, die diesen zur Erfüllung ihrer dienstlichen oder beruflichen Pflichten dienen.

Von beruflichen Pflichten sind insbesondere auch journalistische Tätigkeiten in Vorbereitung einer konkreten Veröffentlichung umfasst (vgl. Münchener Kommentar/Hörnle, 12. Auflage, § 184b Rz. 41). Durch das Ausschließlichkeitskriterium soll entsprechend der Regelung des § 184b Absatz 5 StGB sichergestellt werden, dass die konkrete Aufgabenerfüllung einziger Grund für die Verwendung der Daten ist (vgl. Bundestagsdrucksache 12/4883, S. 8 f.).

§ 202d Absatz 3 Satz 2 StGB stellt einen Unterfall des §202d Absatz 3 Satz 1 StGB dar. Er entzieht insbesondere den Ankauf von steuerrechtlich relevanten Daten dem Anwendungsbereich der Datenhehlerei.

Zu Nummer 3

Das in § 205 Absatz 1 Satz 2 StGB-E (Strafantrag) vorgesehene relative Strafantragserfordernis soll auch für den Straftatbestand der Datenhehlerei gelten. Die Tat soll nur auf Antrag verfolgt werden, es sei denn, dass die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält

Zu Artikel 6 (Grundrechtseinschränkungen)

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

Zu Artikel 7 (Inkrafttreten)

Die Vorschrift regelt das Inkrafttreten des Gesetzes.