Bundesrat **Drucksache** **275/1/07**

29.05.07

Empfehlungen
der Ausschüsse

R - Fz - In - Wi

zu **Punkt ...** der 834. Sitzung des Bundesrates am 8. Juni 2007

Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG

Der **federführende Rechtsausschuss** (R),
der **Finanzausschuss** (Fz),
der **Ausschuss für Innere Angelegenheiten** (In) und
der **Wirtschaftsausschuss** (Wi)
empfehlen dem Bundesrat,

zu dem Gesetzentwurf gemäß Artikel 76 Abs. 2 des Grundgesetzes wie folgt Stellung zu nehmen:

R 1. Zu Artikel 1 Nr. 1 (§ 53b Abs. 1 Satz 3 und 4 StPO)

Nr. 7 (§ 100a Abs. 4 Satz 3 und 4 StPO)

Artikel 1 ist wie folgt zu ändern:

a) In Nummer 1 § 53b Abs. 1 Satz 3 und Nummer 7 § 100a Abs. 4 Satz 3 ist jeweils das Wort "löschen" durch das Wort "sperren" zu ersetzen.

b) In Nummer 1 § 53b Abs. 1 Satz 4 und Nummer 7 § 100a Abs. 4 Satz 4 ist jeweils das Wort "Löschung" durch das Wort "Sperrung" zu ersetzen.

Begründung:

Das Anliegen des Gesetzentwurfs, nach § 53b Abs. 1 StPO-E bzw. nach § 100a

...

Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Amsterdamer Str. 192, 50735 Köln
Telefon: (02 21) 97 66 83 40, Telefax: (02 21) 97 66 83 44
ISSN 0720-2946

Abs. 4 StPO-E einem Beweiserhebungsverbot oder einem Beweisverwertungsverbot unterfallende Daten besonders zu schützen, wird unterstützt. Allerdings werden bei einer Datenlöschung Informationen unwiederbringlich vernichtet. Es ist aber nicht ausgeschlossen, dass diese in einem späteren Verfahrensstadium - auch zu Gunsten des Verdächtigen - noch Bedeutung erlangen können und einer Verwertung als Beweismittel auch zugeführt werden dürfen. Dies gilt etwa für den Fall, dass die Verstrickung einer durch § 53b StPO-E geschützten Person erst zu einem späteren Zeitpunkt erkennbar wird, aber auch für den Fall, dass die geschützte Person in die Verwertung der Daten einwilligt (vgl. Meyer-Goßner, StPO, 49. Auflage, § 53 Rnr. 6 m.w.N.).

Bei einer technischen Datensperrung werden die Informationen gleichfalls zuverlässig gegen eine unbefugte Kenntnisnahme geschützt. Davon geht auch der Gesetzentwurf aus (vgl. Artikel 1 Nr. 11 § 101 Abs. 10 Satz 3 StPO). Anders als bei der Datenlöschung gehen die Daten jedoch nicht unwiederbringlich verloren, sondern können, soweit dies rechtlich zulässig und zur Erforschung der materiellen Wahrheit erforderlich ist, wieder zugänglich gemacht werden. Damit bleibt ein gerechter Ausgleich zwischen dem Strafverfolgungsanspruch des Staates sowie dem Grundsatz der Ermittlung der materiellen Wahrheit einerseits und dem Schutz der Individualrechte der von Strafverfolgungsmaßnahmen Betroffenen andererseits möglich, der in der Entwurfsbegründung zu Recht betont wird.

Eine Löschung der Daten soll erst zu dem in § 101 Abs. 10 StPO-E bezeichneten Zeitpunkt erfolgen.

R bei Annahme entfällt Ziffer 3

2. Zu Artikel 1 Nr. 1 (§ 53b Abs. 4 Satz 1 StPO)

Nr. 3 Buchstabe a Doppelbuchstabe bb (§ 97 Abs. 2 Satz 3 StPO)

Artikel 1 ist wie folgt zu ändern:

a) Nummer 1 § 53b Abs. 4 Satz 1 ist wie folgt zu fassen:

"Die Absätze 1 bis 3 sind nicht anzuwenden, soweit die zur Verweigerung des Zeugnisses Berechtigten der Teilnahme an der Tat, der Begünstigung, der Strafvereitelung, der Hehlerei oder der Geldwäsche verdächtig sind."

b) Nummer 3 Buchstabe a Doppelbuchstabe bb § 97 Abs. 2 Satz 3 ist wie folgt zu fassen:

"Die Beschränkungen der Beschlagnahme gelten nicht, wenn die zur Verweigerung des Zeugnisses Berechtigten der Teilnahme an der Tat, der Begünstigung, der Strafvereitelung, der Hehlerei oder der Geldwäsche verdächtig sind oder wenn es sich um Gegenstände handelt, die durch eine Straftat hervorgebracht oder zur Begehung einer Straftat gebraucht oder bestimmt sind oder die aus einer Straftat herrühren."

Begründung:

Die Geldwäsche stellt mit ihrer Bezugnahme auf Vermögenswerte, die aus bestimmten Vortaten herrühren, eine der Begünstigung, Strafvereitelung oder Hehlerei vergleichbare Form der Verstrickung in die aufzuklärende Straftat dar. Es ist deswegen gerechtfertigt, sie dementsprechend in die Verstrickungsregelungen des § 53b Abs. 4 und des § 97 Abs. 2 StPO-E einzubeziehen.

Nicht ersichtlich ist, weswegen in dem Gesetzentwurf nunmehr abweichend vom bisherigen Recht zur Voraussetzung der Verstrickungsregelung gemacht werden soll, dass ein Ermittlungsverfahren eingeleitet ist. Das Argument in der Begründung des Entwurfs, nach dem durch die Formulierung die Ermittlungsbehörden für die geschützten Belange der betroffenen Berufsgeheimnisträger "zu sensibilisieren und eine Umgehung der Schutzregelungen allein auf Grund bloßer Vermutungen auszuschließen" sei, überzeugt nicht. Auch nach geltendem Recht, das Bezug auf den Verdacht einer Verstrickung nimmt, muss ein auf bestimmten Tatsachen beruhender Verdacht vorliegen, um die Beschlagnahmebeschränkungen entfallen zu lassen (vgl. KK-Nack, 5. Auflage, § 97 Rnr. 35). Bloße Vermutungen reichen nicht aus (vgl. Meyer-Goßner, StPO, 49. Auflage, § 97 Rnr. 20 m.w.N.). Für eine Umgehung der Beschlagnahmebeschränkungen durch Ermittlungsbehörden gibt es keinen Anhaltspunkt. Es ist daher insoweit kein Bedarf für eine Änderung des Strafverfahrensrechts ersichtlich. Darüber hinaus wird in die Strafprozessordnung nunmehr der Begriff einer Einleitung des Strafverfahrens eingeführt, obgleich - worauf die Begründung des Entwurfs zutreffend hinweist - die förmliche Einleitung eines Ermittlungsverfahrens nach der Strafprozessordnung gar nicht vorgesehen ist. Es sollte deswegen insoweit bei der bisher geltenden Formulierung bleiben.

In entfällt bei Annahme von Ziffer 2

3. Zu Artikel 1 Nr. 1 (§ 53b Abs. 4 StPO)

Artikel 1 Nr. 1 § 53b Abs. 4 ist wie folgt zu fassen:

"(4) Die Absätze 1 bis 3 sind nicht anzuwenden, soweit die zeugnisverweigerungsberechtigte Person selbst der Beteiligung an der Tat oder der Begünstigung, Strafvereitelung oder Hehlerei verdächtig ist."

Begründung:

Es ist rechtlich nicht zwingend erforderlich, die Anwendung der Verstrickungsregelung an die Voraussetzung zu knüpfen, dass bereits ein Ermittlungsverfahren auf Grund des Tatverdachts gegen den betroffenen Berufsgeheimnisträger eingeleitet bzw. dass in Ansehung von Presseangehörigen bei Straftaten, die nur auf Antrag oder Ermächtigung verfolgbar sind, der Strafantrag gestellt bzw. die Ermächtigung erteilt worden ist.

Der Gewährleistung einer funktionstüchtigen Strafrechtspflege ist daher der Vorzug einzuräumen und auf die genannten Voraussetzungen für die Anwend-

barkeit der Verstrickungsregelung und das Vorliegen der entsprechenden Anträge oder Ermächtigungen zu verzichten.

R
In

4. Zu Artikel 1 Nr. 7 (§ 100a Abs. 2 Nr. 1 Buchstabe f StPO)

In Artikel 1 Nr. 7 § 100a Abs. 2 Nr. 1 Buchstabe f ist die Angabe "176a, 176b, 177 Abs. 2 Nr. 2 und des § 179 Abs. 5 Nr. 2" durch die Angabe "176 bis 179 sowie 181a Abs. 1" zu ersetzen.

Begründung:

Der vorgesehene Straftatenkatalog des § 100a Abs. 2 Nr. 1 Buchstabe f StPO-E ist hinsichtlich der Straftaten gegen die sexuelle Selbstbestimmung nicht ausreichend. Auch bei weiteren schwerwiegenden Sexualdelikten besteht ein Bedürfnis, Straftaten beziehungsweise kriminelle Strukturen durch Maßnahmen der Telekommunikationsüberwachung aufzudecken und so zum wirksamen Opferschutz beizutragen. Es ist nicht nachzuvollziehen, warum zahlreiche Straftatbestände in diesem Bereich trotz ihres hohen Unrechtsgehalts keine Berücksichtigung im Straftatenkatalog gefunden haben.

Bezüglich des sexuellen Missbrauchs von Kindern gemäß § 176 StGB ergibt sich dies bereits daraus, dass der bislang im Gesetzentwurf enthaltene § 176a Abs. 1 StGB an das einschlägige Vortatverhalten des Täters anknüpft. Ob dieses vorliegt bzw. ein Verdacht hierfür, kann vielfach gerade zu Beginn der Ermittlungen, in denen eine Maßnahme der Telekommunikationsüberwachung erforderlich wäre, nicht sofort beurteilt werden. Erforderlich ist daher bereits die Aufnahme des Grundtatbestandes.

Ferner ist weder nachvollziehbar noch sachgerecht, warum bei den §§ 177 und 179 StGB jeweils nur einzelne und zudem seltene Tatvarianten erfasst sind. Nicht nur bei der gemeinschaftlichen Begehung kann die Telekommunikationsüberwachung wichtige Ermittlungsergebnisse liefern. Zu beachten ist hierbei insbesondere, dass Maßnahmen der Telekommunikationsüberwachung nicht nur zur Erforschung des Sachverhalts eingesetzt werden, sondern insbesondere auch ein unverzichtbares Fahndungsinstrument sein können. Hinsichtlich des Unrechtsgehalts sind alle Tatvarianten mit den bereits aufgenommenen Varianten vergleichbar.

Erforderlich ist ferner die Aufnahme des Tatbestands der Zuhälterei gemäß § 181a Abs. 1 StGB. Es handelt sich hierbei um ein Delikt, das vielfach dem Bereich der organisierten Kriminalität zuzurechnen ist. Der Strafrahmen setzt höher an als beispielsweise § 233a Abs. 1 StGB und zeigt, dass der Unrechtsgehalt des Delikts hoch ist. Die Erfahrung zeigt zudem, dass die Zuhälterszene organisiert und vernetzt ist, wobei vielfach konspirativ vorgegangen wird. Bereits aus diesem Grund erscheint ein Aufbrechen dieser konspirativen Strukturen durch die Überwachung der Telekommunikation angezeigt.

R
In

5. Zu Artikel 1 Nr. 7 (§ 100a Abs. 2 Nr. 1 Buchstabe i StPO)

In Artikel 1 Nr. 7 § 100a Abs. 2 Nr. 1 Buchstabe i ist nach der Angabe "234a," die Angabe "238 Abs. 2 und 3, §§" einzufügen.

Begründung:

Bei der Nachstellung gemäß § 238 StGB handelt es sich, wie sich insbesondere auch aus § 238 Abs. 1 Nr. 2 StGB ergibt, um ein Delikt, das häufig mit Mitteln der Telekommunikation begangen wird. Von Bedeutung ist hierbei nicht nur die Tatsache, ob beziehungsweise wann entsprechende Anrufe beim Opfer erfolgen, sondern zu Beweiszwecken auch der Inhalt der Äußerungen. Auch für die Fahndung nach entsprechenden Beschuldigten spielt die Lokalisierung eine bedeutende Rolle.

Aus Gründen der Verhältnismäßigkeit erfolgt eine Beschränkung auf die Qualifikationstatbestände des § 238 Abs. 2 und 3 StGB, wie sie auch im geänderten § 112a StPO vorgenommen wurde.

R
bei Annahme entfällt Ziffer 7

6. Zu Artikel 1 Nr. 7 (§ 100a Abs. 2 Nr. 1 Buchstabe j und o1 -neu- StPO)

Artikel 1 Nr. 7 § 100a Abs. 2 Nr. 1 ist wie folgt zu ändern:

a) In Buchstabe j sind vor dem Wort "Bandendiebstahl" die Wörter "Diebstahl unter den in § 243 Abs. 1 Satz 2 Nr. 3 genannten Voraussetzungen," einzufügen.

b) Nach Buchstabe o ist folgender Buchstabe o1 einzufügen:

"o1) Untreue unter den in § 266 Abs. 2 in Verbindung mit § 263 Abs. 3 Satz 2 genannten Voraussetzungen,"

Begründung:

Der Diebstahl im besonders schweren Fall ist in der Form des gewerbsmäßigen Diebstahls in den Straftatenkatalog aufzunehmen. In diesem Deliktsfeld handelnde Tätergruppen gehen häufig konspirativ und verdeckt vor, die Telekommunikation untereinander ist dabei ein wichtiges Mittel der Tatbegehung. Aber auch bei Einzeltätern können wesentliche Erkenntnisse über die Tatbegehung und die Verwertung der erlangten Gegenstände zu erwarten sein. Daraus resultiert ein besonderer Bedarf für die Zulassung der Überwachung der Telekommunikation zur Aufklärung dieser Straftaten.

Die Strafandrohung ist beim Diebstahl im besonders schweren Fall mit einer Freiheitsstrafe von drei Monaten bis zu zehn Jahren hinreichend schwer.

Der Gesetzentwurf weist zu Recht auf das Bedürfnis einer effektiven Verfol-

gung von Straftaten aus dem Bereich der Wirtschaftkriminalität hin. Ebenso wie bei den in den Gesetzentwurf aufgenommenen Qualifikationstatbeständen des Betrugs, des Computerbetrugs, des Subventionsbetrugs oder des Bankrotts wird der besonders schwere Fall der Untreue typischerweise von in organisierten Strukturen und unter Nutzung entsprechender Organisations- und Kommunikationsstrukturen handelnden Tätern begangen. Der in dem Gesetzentwurf dazu festgestellte Bedarf einer Einsatzmöglichkeit des Instruments der Telekommunikationsüberwachung besteht daher auch hier.

Die Strafandrohung (Freiheitsstrafe von sechs Monaten bis zehn Jahren) wiegt bei der Untreue im besonders schweren Fall ebenso wie bei den vorbezeichneten Tatbeständen hinreichend schwer.

In entfällt bei Annahme von Ziffer 6

7. Zu Artikel 1 Nr. 7 (§ 100a Abs. 2 Nr. 1 Buchstabe o1 -neu- StPO)

In Artikel 1 Nr. 7 § 100a Abs. 2 Nr. 1 ist nach Buchstabe o folgender Buchstabe o1 einzufügen:

"o1) Untreue unter den in § 266 Abs. 2 genannten Voraussetzungen in Verbindung mit § 263 Abs. 3,"

Begründung:

Als Anlassstraftaten wurden unter anderem der Computerbetrug, der Subventionsbetrug, der Bankrott sowie die Urkundenfälschung und der Betrug im besonders schweren Fall in den Katalog des § 100a Abs. 2 StPO-E aufgenommen. Die Untreue findet bisher jedoch keine Berücksichtigung, obwohl sie als besonders schwerer Fall die gleichen Qualifizierungsmerkmale und die gleiche Strafandrohung wie der Betrug aufweist und einigen Tathandlungen des Bankrotts (§ 283 Abs. 1 Nr. 1 bis 4, 8 StGB) ähnlich ist, wodurch sich eine Abgrenzung schwierig gestaltet. Die Aufnahme der Untreue gemäß § 266 Abs. 2 in Verbindung mit § 263 Abs. 3 StGB wird daher als notwendig erachtet.

R In

8. Zu Artikel 1 Nr. 7 (§ 100a Abs. 2 Nr. 1 Buchstabe t StPO)

In Artikel 1 Nr. 7 § 100a Abs. 2 Nr. 1 Buchstabe t sind vor dem Wort "Bestechlichkeit" die Wörter "Vorteilsannahme und Vorteilsgewährung nach den §§ 331 und 333 sowie" einzufügen.

Begründung:

Neben der Bestechlichkeit und der Bestechung nach den §§ 332 beziehungsweise 334 StGB sind auch die Vorteilsannahme und die Vorteilsgewährung

nach den §§ 331 beziehungsweise 333 StGB in den Straftatenkatalog aufzunehmen. Die Entwurfsbegründung, soweit sie hier ein Bedürfnis für eine Telekommunikationsüberwachung in Frage stellt, ist nicht nachvollziehbar. Ein Bedürfnis wird vielmehr seitens der staatsanwaltschaftlichen Praxis nachhaltig bejaht. Die Delikte sind in ihrer Struktur jeweils vergleichbar. Gerade zu Beginn der Ermittlungen ist vielfach nicht absehbar, welche der Deliktsformen vorliegt und ob die zusätzlichen Voraussetzungen der Bestechung oder der Bestechlichkeit beziehungsweise ein Verdacht hierfür tatsächlich vorliegen.

Zu Recht führt die Begründung des Gesetzentwurfs an anderer Stelle aus, dass in Einzelfällen auf Grund der besonderen Bedeutung des geschützten Rechtsgutes auch eine geringere Freiheitsstrafe als eine Mindesthöchststrafe von fünf Jahren Freiheitsstrafe ausreicht. Die von den §§ 331 beziehungsweise 333 StGB geschützten Rechtsgüter der Lauterkeit des öffentlichen Dienstes sowie des Vertrauens der Allgemeinheit in diese Lauterkeit sind von so hoher Bedeutung, dass auch die Tatsache, dass diese Vorschriften nur Freiheitsstrafen bis zu drei Jahren vorsehen, einer Aufnahme in den Katalog nicht entgegensteht.

R
In

9. Zu Artikel 1 Nr. 7 (§ 100a Abs. 2 Nr. 2 Buchstabe a StPO)

In Artikel 1 Nr. 7 § 100a Abs. 2 Nr. 2 Buchstabe a ist die Angabe "Nr. 5" zu streichen.

Begründung:

Die Beschränkung der Telekommunikationsüberwachung auf die in § 370 Abs. 3 Satz 2 Nr. 5 AO-E genannten Tatbestände der Steuerhinterziehung ist nicht nachvollziehbar. Wie die Entwurfsbegründung an anderer Stelle zu Recht ausführt, ist die Telekommunikationsüberwachung insbesondere bei Straftaten der Wirtschaftskriminalität ein besonders effektives Instrument. Eine Beschränkung auf die bandenmäßige Begehung wird dem nicht gerecht. So zeigt beispielsweise § 370 Abs. 3 Nr. 3 AO, dass das Delikt vielfach unter Zusammenwirkung Mehrerer begangen wird, was deren Abstimmung voraussetzt. Gerade in diesem Bereich kann die Überwachung der Telekommunikation ein besonders wertvolles Ermittlungsinstrument darstellen. Auch bei den weiteren in § 370 Abs. 3 AO genannten Fallgruppen kann davon ausgegangen werden, dass zur Verfolgung der Täter eine Telekommunikationsüberwachung erforderlich sein kann. Im Unrechtsgehalt sind sämtliche Tatvarianten vergleichbar.

In

10. Zu Artikel 1 Nr. 7 (§ 100a Abs. 2 Nr. 3 StPO)

Der Bundesrat bittet, im weiteren Verlauf des Gesetzgebungsverfahrens sicherzustellen, dass zur Bekämpfung des Dopings im Sport in hinreichendem Maße der Einsatz der Telekommunikationsüberwachung ermöglicht wird.

Begründung:

Zu Recht geht die Entwurfsbegründung davon aus, dass ein effektives Vorgehen gegen strafbares Doping im Sport beziehungsweise die hierfür mit verantwortlichen Hintermänner eine Aufnahme der entsprechenden Delikte in den Straftatenkatalog des § 100a StPO-E erfordert. Der Bundesrat bittet, das weitere Gesetzgebungsverfahren zum Entwurf eines Gesetzes zur Verbesserung der Bekämpfung des Dopings im Sport (BR-Drs. 223/07) sorgfältig zu beobachten und die dort gefundenen Ergebnisse zu berücksichtigen.

Nach Auffassung des Bundesrates sollten alle Strafvorschriften, die einen ausreichenden Unrechtsgehalt aufweisen, in den Katalog aufgenommen werden. Der von der Bundesregierung bisher vorgeschlagene Teilbereich der besonders schweren Fälle erscheint zu eng geraten.

R In

11. Zu Artikel 1 Nr. 7 (§ 100a Abs. 2 Nr. 7a -neu- StPO)

In Artikel 1 Nr. 7 § 100a Abs. 2 ist nach Nummer 7 folgende Nummer 7a einzufügen:

"7a. aus dem Grundstoffüberwachungsgesetz:

Straftaten nach § 29 Abs. 1 unter den in § 29 Abs. 3 Satz 2 genannten Voraussetzungen,"

Begründung:

Im Bereich der Bekämpfung der Betäubungsmittelkriminalität spielt die Strafbarkeit nach § 29 GÜG in der Praxis mittlerweile eine bedeutende Rolle. Wie bei sonstiger Betäubungsmittelkriminalität handelt es sich vielfach um Taten im Bereich der organisierten Kriminalität. Die Täter sind hierbei hoch organisiert und wirken arbeitsteilig zusammen. Gerade hier sind eine Aufdeckung der kriminellen Strukturen sowie der Tatnachweis häufig nur durch die Überwachung der Telekommunikation möglich. Wie bei den Delikten aus dem Betäubungsmittelgesetz erfolgt eine Beschränkung auf besonders schwere Fälle.

R In

12. Zu Artikel 1 Nr. 7 (§ 100a Abs. 2 Nr. 8a -neu- StPO)

In Artikel 1 Nr. 7 § 100a Abs. 2 ist nach Nummer 8 folgende Nummer 8a einzufügen:

"8a. aus dem Vereinsgesetz:

Straftaten nach § 20 Abs. 1 Nr. 1 bis 4,"

R bei Annahme entfällt Ziffer 14

13. Begründung:

Ziel des Gesetzentwurfs ist eine Beschränkung der Katalogtaten für die Anordnung von Telekommunikationsüberwachungsmaßnahmen auf die Kategorie schwerer Straftaten. Dazu zählt der Entwurf die Straftaten, die eine Mindesthöchststrafe von fünf Jahren aufweisen, aber auch solche mit einer geringeren Mindesthöchststrafe, wenn im Einzelfall dem geschützten Rechtsgut besondere Bedeutung zukommt oder ein besonderes öffentliches Interesse an einer Strafverfolgung besteht. Ausgeschlossen werden soll die Telekommunikationsüberwachung aber für die Fälle, in denen die Bedeutung des zu schützenden Rechtsguts und das öffentliche Interesse an der Strafverfolgung nicht so gewichtig erscheinen, dass der von der Maßnahme zu erwartende Nutzen die mit ihr verbundenen Beeinträchtigungen überwiegen würde.

Nach der Entwurfsbegründung liegen diese Voraussetzungen bei § 20 Abs. 1 Nr. 1 bis 4 VereinsG nicht vor.

Gerade extremistische Gruppierungen verstoßen regelmäßig gegen Verbote im Sinne dieser Vorschrift. Bis in die jüngste Vergangenheit konnten auf Grundlage dieser Vorschrift insbesondere Straftaten rechtsextremer Gruppierungen aufgeklärt und der Tatnachweis geführt werden. Aus derartigen Ermittlungsmaßnahmen ergaben sich auch regelmäßig Ansatzpunkte für Ermittlungen wegen weiterer Straftaten der Mitglieder dieser Gruppierungen. Die effektive Bekämpfung demokratiefeindlicher Bestrebungen dient der öffentlichen Sicherheit und staatlichen Ordnung und betrifft daher bereits besonders bedeutsame Rechtsgüter.

Trotz der angedrohten Höchststrafe von nur einem Jahr sind damit die Voraussetzungen für eine schwere Straftat im Sinne der Entwurfsbegründung erfüllt.

In entfällt bei Annahme von Ziffer 13

14. Begründung:

Der vorgesehene § 100a Abs. 2 StPO-E beschreibt, was schwere Straftaten sind, die unter bestimmten Voraussetzungen die Überwachung und Aufzeichnung der Telekommunikation ohne Wissen der Betroffenen erlauben. Durch die vorgeschlagene Ergänzung sollen Straftaten nach § 20 Abs. 1 Nr. 1 bis 4 VereinsG in den Straftatenkatalog aufgenommen werden. Der hohe Konspirationsgrad ehemaliger Mitglieder verbotener Vereine des rechten als auch des ausländerextremistischen Spektrums erschwert den Nachweis der Fortführung oder Unterstützung einer verbotenen Vereinigung oder macht ihn unmöglich. Da herkömmliche Ermittlungsinstrumente kaum erfolgversprechend einsetzbar sind, bleiben Telekommunikationsüberwachungsmaßnahmen oftmals die einzige Möglichkeit, Beweismaterial zu erlangen. Abhilfe kann auch nicht der im Straftatenkatalog von § 100a StPO-E enthaltene § 85 StGB (Verstoß gegen ein Vereinigungsverbot) schaffen, da dieser Tatbestand erst dann erfüllt ist, wenn das Vereinsverbot rechtskräftig ist. Bis zur Rechtskraft eines Vereinsverbotes kann es bei Ausschöpfung aller Rechtsmittel geraume Zeit dauern.

In 15. Zu Artikel 1 Nr. 7 (§ 100a Abs. 3 Satz 2 -neu- StPO)

Dem Artikel 1 Nr. 7 § 100a Abs. 3 ist folgender Satz anzufügen:

"Die Maßnahme darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden."

Begründung:

Kennzeichnend für die Telekommunikationsüberwachung ist, dass die Erhebung nicht allein auf Daten der Zielperson, also die Person, gegen die die Maßnahme nach § 100a Abs. 3 StPO-E gerichtet werden darf (Beschuldigter, Nachrichtenmittler, Anschlussinhaber), beschränkt werden kann, denn Erkenntnisse aus der Überwachungsmaßnahme sollen ja gerade aus der Kommunikation der Zielperson mit anderen Personen gewonnen werden.

Die im Zeitpunkt der Überwachungsanordnung in aller Regel unbekannten Kommunikationspartner der Zielpersonen sind in der datenschutzrechtlichen Terminologie als unvermeidbar betroffene Dritte einzustufen.

Auch die Kommunikationspartner der Zielpersonen unterfallen dem Schutzbereich des Artikels 10 GG. Die Telekommunikationsüberwachung stellt daher auch ihnen gegenüber einen Eingriff in das Fernmeldegeheimnis dar. Dass der Eingriff ihnen gegenüber nicht gezielt erfolgt, verringert lediglich die Intensität des Eingriffs.

Vor diesem Hintergrund bedarf auch der Eingriff gegenüber den Kommunikationspartner der Zielpersonen einer ausdrücklichen gesetzlichen Grundlage. Eine vergleichbare Regelung sieht § 100c Abs. 3 Satz 3 StPO vor.

Darüber hinaus empfiehlt es sich, die Kommunikationspartner einer eindeutigen datenschutzrechtlichen Kategorie zuzuordnen, um hierauf bei den verfahrensrechtlichen Vorkehrungen, wie z.B. der Unterrichtungspflicht nach § 101 StPO-E, Bezug nehmen zu können.

In 16. Zu Artikel 1 Nr. 7 (§ 100a Abs. 4 StPO)

Die Regelungen zur Telekommunikationsüberwachung sehen vor, dass Aufzeichnungen aus dem Kernbereich der privaten Lebensgestaltung unverzüglich zu löschen sind.

Die bundesweit eingesetzte TKÜ-Technik lässt derzeit keine Löschung einzelner Aufzeichnungspassagen zu. Die Umsetzung der Vorschrift würde eine Neukonzeption der kompletten Archivierungsmechanismen - sowohl Software als auch Hardware - in sämtlichen TKÜ-Anlagen erforderlich machen. Diese Neukonzeption der Archivierung bedeutet für die Lieferanten der TKÜ-Technik, aber auch für die polizeilichen Bedarfsträger einen hohen finanziellen sowie

zeitlichen Aufwand, um die Anforderungen in die Systeme zu implementieren. Das Problem bedarf der Klärung im weiteren Verlauf des Gesetzgebungsverfahrens. Es muss in jedem Fall sichergestellt werden, dass das Inkrafttreten der Gesetzesnovelle nicht zu einer faktischen Nichtanwendbarkeit der TKÜ-Befugnisse führt.

Hinsichtlich der Löschung von kernbereichsrelevanten Daten im Zusammenhang mit der "Internetüberwachung" wird ferner darauf hingewiesen, dass innerhalb einer Internetsitzung, die eine Dauer von bis zu 24 Stunden aufweisen kann, mehrere Dienste (VoIP, E-Mail, Chat und "normales Surfen") aufgerufen werden können. Wird hier z.B. der Dienst VoIP (Internettelefonie) verwendet, kann ein einzelnes Gespräch aus dem kompletten Datenstrom nicht explizit gelöscht werden. Um Gespräche mit kernbereichsrelevanten Informationen zu löschen, müsste die komplette Internetsitzung mit allen darin enthaltenen Daten (VoIP, E-Mail, Chat und "normales Surfen") gelöscht werden, wodurch gegebenenfalls auch ermittlungsrelevante Informationen verloren gingen. Die Bundesregierung wird gebeten, zu dieser Problematik Stellung zu nehmen.

R 17. Zu Artikel 1 Nr. 7 (§ 100b Abs. 1 Satz 4 und 5 StPO)

In Artikel 1 Nr. 7 § 100b Abs. 1 Satz 4 und 5 ist jeweils das Wort "zwei" durch das Wort "drei" zu ersetzen.

Begründung:

Die Begründung des Gesetzentwurfs zur Notwendigkeit der Verkürzung der Dauer der Anordnung von Maßnahmen nach § 100a StPO-E und deren Verlängerung von drei auf zwei Monate entgegen der bewährten Praxis vermag nicht zu überzeugen.

So wird einerseits ausgeführt, dass rechtstatsächliche Untersuchungen ergeben hätten, dass etwa drei Viertel der Telekommunikationsüberwachungsmaßnahmen über einen Zeitraum von bis zu zwei Monaten geführt und nur etwa 9 Prozent der Anschlüsse tatsächlich über die Dauer von drei Monaten überwacht werden. Daraus ergebe sich, dass für den Großteil der Maßnahmen eine Anordnungsdauer von maximal zwei Monaten ausreichend erscheine. Andererseits solle durch die Verkürzung der Verlängerungsfrist eine jeweils zeitnahe gerichtliche Kontrolle der Telekommunikationsüberwachungsmaßnahme im Sinne eines möglichst effektiven Grundrechtsschutzes der von der Maßnahme betroffenen Personen gewährleistet werden.

Eine inhaltliche Verbesserung des Grundrechtsschutzes ist aber allein durch die Verkürzung der Kontrollfrist nicht zu erwarten. Auch beträfe diese Verkürzung

der Kontrollfrist nur einen geringen Teil der Maßnahmen, da nach den angeführten rechtstatsächlichen Erkenntnissen ein Großteil der Maßnahmen bereits nach zwei Monaten beendet ist.

Es ist nicht davon auszugehen, dass es durch die Verkürzung der Fristen zu einer Verkürzung der Dauer der durchzuführenden Telekommunikationsüberwachungsmaßnahmen kommen wird. Vielmehr führt die Neuregelung - wie in der Begründung zu dem Gesetzentwurf zu Recht festgestellt wird - zu einem Anstieg der Anzahl der Verlängerungsanordnungen und damit auch der Gesamtzahl der jährlichen Überwachungsanordnungen.

Diese unnötige Belastung der Gerichte und Staatsanwaltschaften mit erheblichem bürokratischen Mehraufwand und die dadurch verursachten Mehrkosten stehen daher insgesamt in keinem Verhältnis zu dem Gewinn an Kontrolldichte, so dass an der bisher geltenden Dauer von drei Monaten bezüglich der Anordnung und der Verlängerung von Maßnahmen nach § 100a StPO-E festzuhalten ist.

Im Übrigen entspricht dies auch der Gegenäußerung der Bundesregierung zu der Stellungnahme des Bundesrates zum Entwurf eines Gesetzes zur Änderung des Zollfahndungsdienstgesetzes und anderer Gesetze vom 18. April 2007 (BT-Drs. 16/4663 und 16/5053). In dieser stimmte die Bundesregierung bei der Erhebung von Verkehrsdaten einer Verlängerung der Fristen in § 23g Abs. 4 Satz 4 und 5 ZFdG bei der Anordnung und Verlängerung von Telekommunikationsüberwachungsmaßnahmen auf jeweils drei Monate (anstelle der vorgesehenen zwei Monate bzw. eines Monats) zu (vgl. BT-Drs. 16/5053, S. 3). Die Zustimmung erfolgte vor dem Hintergrund einer einheitlichen Regelung im Verhältnis der einzelnen Telekommunikationsmaßnahmen innerhalb des Zollfahndungsdienstgesetzes zueinander (gleichlautende Fristen).

Auf Grund eines harmonischen Gesamtkonzeptes sollte es daher auch keine Abweichung zwischen den Regelungen des Zollfahndungsdienstgesetzes und der Strafprozessordnung geben, so dass es bei der bisher geltenden Dauer von drei Monaten bezüglich der Anordnung und der Verlängerung von Maßnahmen nach § 100a StPO-E verbleiben sollte.

R In 18. Zu Artikel 1 Nr. 7 (§ 100b Abs. 1 Satz 6 StPO)

Artikel 1 Nr. 7 § 100b Abs. 1 Satz 6 ist zu streichen.

Begründung:

Die Bestimmung einer Zuständigkeit des im Rechtszug übergeordneten Gerichts für die Verlängerung von Anordnungen zur Telekommunikationsüberwachung (und von Maßnahmen hinsichtlich derer auf § 100b Abs. 1 Satz 6 StPO-E verwiesen wird) über sechs Monate hinaus ist abzulehnen. Die Kompetenzverlagerung würde zu einer sachlich nicht gerechtfertigten Mehrbelastung der Gerichte führen. Bislang nicht mit dem Verfahrensstoff befasst gewesene Richter müssten sich mit hohem Aufwand und Zeitverlust in einen nach

sechsmonatigen Ermittlungen zwangläufig äußerst komplexen Sachverhalt und umfangreiche Akten einarbeiten. Es ist nicht ersichtlich, dass dies durch eine unzureichende Kontrolle durch das zunächst für die Anordnung und Verlängerung der Überwachungsmaßnahme zuständige Gericht gerechtfertigt wäre. Soweit aus dem Regelungsvorschlag des Gesetzentwurfs ein Misstrauen gegenüber den regelmäßig zur Entscheidung berufenen Ermittlungsrichtern spricht, ist ein solches unangebracht. Deren Spezialisierung im Bereich der Anordnung verdeckter Ermittlungsmaßnahmen soll durch die in § 162 Abs. 1 StPO-E vorgesehene Kompetenzbündelung gerade für die Anordnung von solchen Maßnahmen mit technischem Hintergrund zur Verbesserung des Rechtsschutzes Betroffener gefördert werden.

R 19. Zu Artikel 1 Nr. 7 (§100b Abs. 2 Satz 2 Nr. 2 StPO)

In Artikel 1 Nr. 7 § 100b Abs. 2 Satz 2 Nr. 2 sind die Wörter "wenn diese allein dem zu überwachenden Endgerät zuzuordnen ist" durch die Wörter "sofern sich nicht aus bestimmten Tatsachen ergibt, dass diese zugleich auch einem anderen Endgerät zugeordnet ist" zu ersetzen.

Begründung:

Die Möglichkeit der Angabe einer Kennung des zu überwachenden Endgerätes steht unter der Einschränkung, dass die anzugebende Endgerätekennung auch allein dem zu überwachenden Endgerät zugeordnet ist.

Die Formulierung des Gesetzentwurfs, der die Überwachung auf Grund der Kennung des Endgerätes, sofern diese allein dem zu überwachenden Endgerät zuzuordnen ist, vorsieht, führt allerdings in Fällen, in denen die (hypothetische) Möglichkeit der mehrfachen Zuordnung der Gerätekennung nicht ausgeschlossen werden kann, ohne dass hierfür konkrete Anhaltspunkte bestehen, zu Rechtsunsicherheit. Der in der Entwurfsbegründung vorgeschlagene Weg, die Voraussetzung der eindeutigen Zuordnung werde in der Praxis dadurch sicherzustellen sein, dass die zur Mitwirkung und Auskunftserteilung verpflichteten Telekommunikationsdienstleister vor der Schaltung der Überwachungsmaßnahme überprüfen, ob die betreffende Gerätekennung mehrfach in das Netz eingebucht ist, ist nicht geeignet, Zweifel an der Eindeutigkeit der Kennung zum Zeitpunkt der richterlichen Entscheidung auszuräumen. Dies hätte zur Folge, dass eine entsprechende Anordnung nicht erlassen werden könnte.

Die vorgeschlagene Fassung trägt diesen Bedenken Rechnung. Dass die zu überwachende Endgerätekennung nicht zugleich auch einem anderen Endgerät zugeordnet ist, wird in der Praxis durch eine Anfrage der Ermittlungsbehörden nach den §§ 161 StPO und 113 TKG bei den nach § 100b Abs. 3 StPO-E zur Mitwirkung und Auskunftserteilung verpflichteten Telekommunikationsdienstleistern vor Beantragung eines richterlichen Überwachungsbeschlusses zu klären sein. Sollten die angesprochenen Telekommunikationsdienstleister lediglich nicht ausschließen können, dass die Kennung mehrfach vergeben ist,

steht diese hypothetische Möglichkeit einer "IMEI-gestützten" Überwachung nicht entgegen. Hingegen ist eine solche nicht zulässig, wenn gesicherte Erkenntnisse - wie etwa die mehrfache Einbuchung der Gerätekennung in das Mobilfunknetz - bestehen, dass die betreffende Endgerätekennung nicht allein dem zu überwachenden Endgerät zugeordnet ist.

In 20. Zu Artikel 1 Nr. 7 (§ 100b Abs. 3 Satz 1 StPO)

In Artikel 1 Nr. 7 § 100b Abs. 3 Satz 1 ist nach dem Wort "Auskünfte" das Wort "unverzüglich" einzufügen.

Begründung:

Die Erfahrungen in der Praxis zeigen, dass es bei der Beantwortung von Auskunftsersuchen auf Grund unzureichender Mitwirkung der Verpflichteten immer wieder zu nicht unerheblichen Zeitverzögerungen kommt.

Die Regelung stellt daher klar, dass den zuständigen Behörden unverzüglich durch die Verpflichteten Auskunft zu erteilen ist.

R 21. Zu Artikel 1 Nr. 7 (§ 100b Abs. 4 Satz 2 StPO)

Artikel 1 Nr. 7 § 100b Abs. 4 Satz 2 ist zu streichen.

Begründung:

Die vorgesehene Verpflichtung der Staatsanwaltschaft, nach Beendigung einer Telekommunikationsüberwachung das anordnende Gericht über Verlauf und Ergebnisse zu unterrichten, ist zu streichen, weil sie verfassungsrechtlich nicht geboten und mit einem erheblichen Mehraufwand verbunden ist.

Der Ermittlungsrichter hat gemäß § 162 Abs. 3 StPO (§ 162 Abs. 2 StPO-E) auf Antrag der Staatsanwaltschaft zur Anordnung bestimmter Ermittlungshandlungen lediglich zu prüfen, ob die Handlung nach den Umständen des Falles gesetzlich zulässig ist, also die Voraussetzungen der entsprechenden Ermittlungsmaßnahme vorliegen; die begründete Erfolgsaussicht sieht das Gesetz als Zulässigkeitsvoraussetzung nicht vor. Allenfalls kann in Fällen ersichtlich aussichtsloser Maßnahmen der Verhältnismäßigkeitsgrundsatz der Zulässigkeit der Maßnahme entgegenstehen; ansonsten steht es dem Ermittlungsrichter grundsätzlich gerade nicht zu, die Zweckmäßigkeit und die Notwendigkeit der beantragten Ermittlungsmaßnahme bei der Entscheidung zu berücksichtigen. Da die Regelung in § 100b Abs. 4 Satz 2 StPO-E zudem erst greifen soll, wenn die Maßnahme beendet ist, dient sie im Unterschied zu § 100d Abs. 4 Satz 1 StPO auch nicht dem Zweck, das Gericht über den Verlauf der Maßnahme zu informieren, damit dieses den Abbruch der Maßnahme anordnen kann, wenn die

Voraussetzungen der Anordnung nicht mehr vorliegen. Ausweislich der Begründung zum Gesetzentwurf ist allein eine Erfolgskontrolle für das Gericht erstrebt, um die daraus resultierenden Erfahrungen bei künftigen Entscheidungen berücksichtigen zu können (BR-Drs. 275/07, S. 106). Eine solche Kontrolle bereits abgeschlossener Maßnahmen für zukünftige Zwecke ist aber von der Rechtsprechung des Bundesverfassungsgerichts nicht verlangt und in Anbetracht des mit dem Gesetzentwurf insgesamt für die justizielle Praxis verbundenen Mehraufwands nicht zwingend erforderlich.

R
bei Annahme entfallen die Ziffern 23 und 24

22. Zu Artikel 1 Nr. 7 (§ 100b Abs. 5 und 6 StPO)

Artikel 1 Nr. 10 (§ 100e Abs. 1 StPO)

Artikel 9 (§ 12 Abs. 1 EGStPO)

a) In Artikel 1 Nr. 7 § 100b sind die Absätze 5 und 6 zu streichen.

b) Artikel 1 Nr. 10 § 100e Abs. 1 ist wie folgt zu fassen:

"(1) Die Länder und der Generalbundesanwalt berichten dem Bundesamt für Justiz kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres über in ihrem Zuständigkeitsbereich angeordnete Maßnahmen nach § 100c. Das Bundesamt für Justiz erstellt eine Übersicht zu den im Berichtsjahr bundesweit angeordneten Maßnahmen und veröffentlicht diese im Internet. Vor der Veröffentlichung im Internet berichtet die Bundesregierung dem Deutschen Bundestag über die im jeweils vorangegangenen Kalenderjahr nach § 100c angeordneten Maßnahmen."

c) Artikel 9 § 12 Abs. 1 ist wie folgt zu fassen:

"(1) § 100g Abs. 4 der Strafprozessordnung ist erstmalig für das Berichtsjahr 2008 anzuwenden. § 100e Abs. 1 der Strafprozessordnung ist bereits für das Berichtsjahr 2007 anzuwenden."

Begründung:

Der Gesetzentwurf sieht in § 100b Abs. 5 und 6 StPO-E eine umfassende gesetzliche Neuregelung von bislang durch Verwaltungsvorschriften festgelegten Berichtspflichten über nach § 100a StPO-E angeordnete Maßnahmen vor.

Der Begründung zum Gesetzentwurf lässt sich nicht entnehmen, weshalb von der bisherigen Praxis abgewichen werden soll. Weder ist ausreichend dargelegt worden, aus welchem Grund bei den Berichten zwischen Anordnungs- und Verlängerungsbeschlüssen zu unterscheiden ist, noch, wieso die Angabe der Anzahl der überwachten Telekommunikationsvorgänge aufgeschlüsselt nach Festnetz-, Mobilfunk- und Internettelekommunikation erforderlich ist.

Diese ausgeweitete Berichtspflicht führt entgegen den Ausführungen in der Begründung zu einer deutlich erhöhten Belastung der Praxis durch Verwaltungsaufgaben, die in keinem Verhältnis zum Nutzen der Information steht.

Es ist kein überzeugender Grund dafür ersichtlich, die Telekommunikationsüberwachung durch eine gesetzliche Regelung auf die gleiche Stufe wie die eingriffsintensivere Wohnraumüberwachung zu stellen. Vielmehr erscheint die Streichung der Berichtspflichten aus der Strafprozessordnung und das Festhalten an der bisherigen Regelung in Verwaltungsvorschriften geboten.

Die sich hieraus ergebenden Änderungen in § 100e StPO und § 12 Abs. 1 EGStPO sind redaktioneller Natur.

In entfällt bei Annahme von Ziffer 22

23. Zu Artikel 1 Nr. 7 (§ 100b Abs. 6 Nr. 2 StPO)

Artikel 1 Nr. 7 § 100b Abs. 6 Nr. 2 ist wie folgt zu fassen:

"2. die Anzahl der Überwachungsanordnungen nach § 100a Abs. 1, unterschieden nach Erst- und Verlängerungsanordnungen;"

Begründung:

Die im Gesetzentwurf geforderte Abgrenzung zwischen Festnetz-, Mobilfunk- und Internettelekommunikation führt zu Problemen, § 100b Abs. 6 Nr. 2 Buchstabe b StPO-E ist daher zu streichen. Die überwachten Anschlüsse werden nicht ausschließlich für eine Kommunikationsform verwendet. So eignen sich ISDN-Anschlüsse zur Festnetztelefonie und als Internetzugang. Gleiches gilt für Mobilfunkgeräte, welche im Mobilfunknetz, als GPRS/UMTS-Gerät und im W-LAN genutzt werden können. Eine klare Differenzierung, wie in § 100b Abs. 6 Nr. 2 Buchstabe b StPO-E vorgesehen, ist daher nicht möglich.

§ 100b Abs. 6 Nr. 4 StPO-E ist entsprechend anzupassen.

In entfällt bei Annahme von Ziffer 22

24. Zu Artikel 1 Nr. 7 (§ 100b Abs. 6 Nr. 3 StPO)

Artikel 1 Nr. 7 § 100b Abs. 6 Nr. 3 ist wie folgt zu fassen:

"3. der jeweils zugrunde liegende Überwachungsanlass;"

Begründung:

Die im Gesetzentwurf geforderte Unterteilung nach Straftaten im Sinne des § 100a Abs. 2 StPO-E ist nicht oder nur unzureichend möglich. So ist den Beschlüssen oftmals kein konkreter Tatbestand zu entnehmen. Auch §100b Abs. 2 StPO-E sieht keine Pflicht zur Angabe der Anlassstraftat nach §100a Abs. 2

StPO-E vor.

In 25. Zu Artikel 1 Nr. 11 (§ 100f Abs. 1a -neu-, 2 und 4, § 101 Abs. 4 Satz 1 Nr. 5 StPO)

Artikel 1 Nr. 11 ist wie folgt zu ändern:

a) § 100f ist wie folgt zu ändern:

aa) Nach Absatz 1 ist folgender Absatz 1a einzufügen:

"(1a) Ohne Wissen der Betroffenen dürfen über Telekommunikationsanlagen (§ 3 Nr. 23 des Telekommunikationsgesetzes) mit technischen Mitteln Speichermedien durchsucht und darin enthaltene Daten beschlagnahmt werden, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand eine in § 100a Abs. 2 bezeichnete Straftat begangen hat, und die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Beschuldigten auf andere Weise - insbesondere durch eine Durchsuchung nach den §§ 102 und 103 - aussichtslos oder wesentlich erschwert wäre."

bb) In Absatz 2 sind jeweils das Wort "Maßnahme" durch das Wort "Maßnahmen", jeweils das Wort "darf" durch das Wort "dürfen" und nach dem Wort "führen" das Wort "wird" durch das Wort "werden" zu ersetzen.

cc) Absatz 4 ist wie folgt zu fassen:

"(4) Für Maßnahmen nach Absatz 1 gelten § 100b Abs. 1, 4 Satz 1 und § 100d Abs. 2, für Maßnahmen nach Absatz 1a § 100a Abs. 4, § 100b Abs. 1 Satz 1 bis 3, Abs. 2 Satz 1 und § 110 Abs. 1 entsprechend."

b) In § 101 Abs. 4 Satz 1 Nr. 5 sind nach der Angabe "§ 100f" die Angabe "Abs. 1" und nach dem Wort "Personen" die Wörter "und des § 100f Abs. 1a der Inhaber der Speichermedien sowie die erheblich mitbetroffenen Personen" einzufügen.

Begründung:

Bedürfnis für eine Regelung:

Die Online-Durchsuchung ist ein unverzichtbares Instrument der Kriminalitätsbekämpfung. Sie dient nicht nur zur Aufklärung von Sachverhalten, son-

dern auch zur Lokalisierung und Identifizierung von Tätern. Diese Auffassung wird auch durch die staatsanwaltschaftliche und polizeiliche Praxis bestätigt, die ein erhebliches Bedürfnis für die Durchführung sogenannter Online-Durchsuchungen sieht.

Gegenstand der bisher in der Öffentlichkeit bekannt gewordenen Fälle von (gerichtlich genehmigten) Online-Durchsuchungen waren unter anderem Verfahren wegen Gründung einer terroristischen Vereinigung und im Zusammenhang mit "Phishing" (Online-Banking-Betrug). Ziel der Online-Durchsuchung kann es dabei unter anderem sein, den Standort eines Computers oder die Identität des Nutzers zu ermitteln. Gerade bei ersterem ist eine konventionelle Wohnraumdurchsuchung nicht möglich.

Generell können bei einer Online-Durchsuchung Hintermänner und Täternetzwerke umfassender ermittelt werden, weil die Offenlegung der Ermittlungen, die mit einer konventionellen Wohnraumdurchsuchung verbunden ist, noch zurückgestellt werden kann. Späteren Verdunkelungsmaßnahmen (Löschung von Daten, Einwirkung auf bislang nicht bekannte Zeugen oder Mittäter etc.) kann entgegengewirkt werden.

Als mögliche Anwendungsbereiche für eine Online-Durchsuchung sind weiter zu nennen:

- die Fälschung von Zahlungskarten (hier stehen sämtliche Tatphasen - von der Datenerlangung über die Herstellung von Falsifikaten bis hin zu deren Gebrauch - in direktem Zusammenhang mit der elektronischen Datenverarbeitung. Die Tatbegehung findet international organisiert unter Nutzung modernster Technologien auf dem Gebiet der EDV statt)
- der gesamte Bereich der organisierten Kriminalität, z.B. Geldwäsche, Terrorfinanzierung, gewerbsmäßige Steuerhinterziehung bzw. Drogenhandel
- der Bereich des islamistischen Extremismus und Terrorismus (Das Betätigungsfeld der Islamisten im Internet reicht dabei von der Radikalisierung, Rekrutierung, Missionierung und Spendengeldsammlung bis hin zur Bildung von Netzwerken und der Bereitstellung bzw. dem Herunterladen von Bombenbauanleitungen, Bekennervideos und Videobotschaften.)
- der Bereich der Internetkriminalität bzw. der Bekämpfung von Kinderpornografie
- der Bereich der Produkterpressung (Androhung der Vergiftung von Lebensmitteln) bzw. der Erpressung von Großbetrieben und Konzernen (z.B. Bahn, Luftfahrtunternehmen).

Ausgestaltung der Regelung:

a) Inhalt der Befugnis

Den Strafverfolgungsbehörden soll die Befugnis gegeben werden, "ohne Wissen der Betroffenen über Telekommunikationsanlagen mit technischen Mitteln Speichermedien zu durchsuchen und darin enthaltene Daten zu beschlagnahmen".

Dies umfasst nicht die Möglichkeit, am PC des Betroffenen installierte Mikrofone oder gar Kameras über die eingeschleuste Software zu aktivieren und damit Gespräche und Aktivitäten im Raum mitzuverfolgen. Ein

solcher Eingriff wäre eine (akustische bzw. optische) Überwachung. Für vergleichbare Maßnahmen bestehen bereits gesetzliche Regelungen (§§ 100c und 100f StPO).

b) Materielle Voraussetzungen der Online-Durchsuchung

Im Hinblick auf die Heimlichkeit der Maßnahme handelt es sich um einen nicht unerheblichen Eingriff in die Grundrechte des Betroffenen. Dementsprechend hat auch der Bundesgerichtshof betont, dass für derartige Maßnahmen hohe materielle Anforderungen an die Anordnung und die Durchführung bestehen. Auch im Hinblick auf verfassungsrechtliche Anforderungen erscheint es daher geboten, den Kreis der Straftaten, bei deren Verdacht eine Online-Durchsuchung möglich ist, zu begrenzen.

Hierzu soll auf den Straftatenkatalog des § 100a Abs. 2 StPO-E (Telekommunikationsüberwachung) abgestellt werden. Ein Rückgriff auf den Katalog des § 100c Abs. 2 StPO (Wohnraumüberwachung) wäre zu restriktiv. Auch der Bundesgerichtshof hat eine Vergleichbarkeit der Intensität der Online-Durchsuchung mit einer Wohnraumüberwachung bezweifelt, so dass die besonders hohen Hürden des dortigen Straftatenkataloges nicht errichtet werden sollten. Auch § 100f Abs. 2 StPO (§ 100f Abs. 1 StPO-E), der die Abhörung und Aufzeichnung des nichtöffentlich gesprochenen Wortes außerhalb von Wohnungen regelt, stellt auf § 100a StPO (§ 100a StPO-E) ab.

Auch die dort zusätzlich genannten Voraussetzungen, wonach die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert sein muss, können auf die Online-Durchsuchung übertragen werden, um die Subsidiarität der Maßnahme zu betonen. Insoweit wird ergänzend die Subsidiarität zur offenen Durchsuchung klargestellt.

c) Kein Regelungsbedarf für die Installation des "Trojaners" oder anderer Software

Insoweit besteht kein zwingendes Bedürfnis für eine ausdrückliche gesetzliche Regelung. Nach jedenfalls herrschender Auffassung sind notwendige Beeinträchtigungen des Betroffenen durch typischerweise mit der Maßnahme verbundene Vorbereitungs- und Begleitmaßnahmen durch die Befugnisnorm gedeckt (vgl. Meyer/Goßner, StPO, 49. Auflage, § 100f Rnr. 7). So hat auch der Bundesgerichtshof den Einbau eines GPS-Empfängers im Rahmen einer Maßnahme nach § 100f Abs. 1 Nr. 2 StPO in das Fahrzeug des Beschuldigten für zulässig erklärt, falls im konkreten Fall kein milderes Mittel in Betracht kommt (vgl. BGH, Urteil vom 24. Januar 2001 - 3 StR 324/00 -, BGHSt 46, 266).

Diese Überlegungen sind auf die Installation eines Trojaners oder anderer Software auf den Rechner des Betroffenen übertragbar.

d) Formelle Voraussetzungen

Angesichts der Grundrechtsintensität ist die Schaffung eines Richtervorbehalts erforderlich, ferner eine Eilzuständigkeit der Staatsanwaltschaft bei Gefahr in Verzug vergleichbar der Zuständigkeitsregelung bei der Telekommunikationsüberwachung in § 100b Abs. 1 Satz 1 StPO-E, auf den

verwiesen werden kann. Ebenso wie bei akustischer Überwachung außerhalb von Wohnräumen (§ 100f Abs. 1 und 4 StPO-E) muss bei einer Eilanordnung der Staatsanwaltschaft eine richterliche Bestätigung eingeholt werden (vgl. den Verweis auf § 100b Abs. 1 Satz 3 in § 100f Abs. 4 StPO-E).

Hinsichtlich der Durchsicht der Daten, auf die zugegriffen wurde, wird auf § 110 StPO verwiesen, der nach herrschender Meinung bereits bisher auch auf die Durchsicht von Daten anwendbar war, die im Rahmen einer konventionellen Durchsuchung beschlagnahmt wurden. Demnach steht die Durchsicht der Staatsanwaltschaft und auf deren Anordnung ihren Ermittlungspersonen zu. Dies entspricht dem Verfahren bei der Beschlagnahme von Festplatten im Rahmen einer konventionellen Durchsuchung.

e) Kernbereichsschutz

Auf Grund der Rechtsprechung des Bundesverfassungsgerichts zur Wohnraumüberwachung müssen Regelungen aufgenommen werden, die den Kernbereich privater Lebensgestaltung von Online-Durchsuchungen freihalten. Dies erfolgt durch Verweis auf § 100a Abs. 4 StPO-E.

R In 26. Zu Artikel 1 Nr. 11 (§ 100g Abs. 1 StPO)

Artikel 1 Nr. 11 § 100g Abs. 1 ist wie folgt zu fassen:

"(1) Begründen bestimmte Tatsachen den Verdacht, dass jemand als Täter oder Teilnehmer eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Abs. 2 bezeichnete Straftat, oder eine Straftat mittels Telekommunikation begangen, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht oder durch eine Straftat vorbereitet hat, so dürfen auch ohne Wissen des Betroffenen Verkehrsdaten (§ 96 Abs. 1, § 113a des Telekommunikationsgesetzes) erhoben werden, soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsorts des Beschuldigten erforderlich ist."

Begründung:

Der Gesetzentwurf unterscheidet hinsichtlich der Voraussetzungen für eine Erhebung von Verkehrsdaten zwischen Straftaten von auch im Einzelfall erheblicher Bedeutung und mittels Telekommunikation begangenen Straftaten. Diese Unterscheidung ist abzulehnen. Der Verhältnismäßigkeitsgrundsatz ist generell bei Eingriffsmaßnahmen zu wahren, so dass eine strikte Normierung, wie sie der Entwurf versucht, weder erforderlich ist noch die gebotene Flexibilität bei der Abwägung ermöglicht. Da die Erhebung von Verkehrsdaten ein wesentlich geringerer Grundrechtseingriff ist als die Erhebung von Inhaltsdaten, reicht die Berücksichtigung des allgemeinen Verhältnismäßigkeitsgrundsatzes aus.

Abzulehnen ist insbesondere, dass bei dem Versuch einer Straftat mittels Telekommunikation, die im Einzelfall nicht von erheblicher Bedeutung ist, eine Verkehrsdatenerhebung generell nicht mehr zulässig sein soll (§ 100g Abs. 1 Satz 1 Nr. 2 StPO-E). Die Schuldschwere eines versuchten Delikts wiegt grundsätzlich nicht derart weniger schwer, dass eine solche Einschränkung geboten ist. Auch hier sollte die Ermittlungsmaßnahme generell möglich sein.

Abzulehnen ist weiterhin die besondere Subsidiaritätsklausel für Maßnahmen nach § 100g Abs. 1 Satz 1 Nr. 2 StPO-E. Diese ist sogar noch strenger als im Falle der - gravierenderen - Erhebung von Inhaltsdaten (vgl. § 100a Abs. 1 Satz 3 a. E. StPO bzw. § 100a Abs. 1 Nr. 3 StPO-E). Dort ist eine Maßnahme auch dann zulässig, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsorts des Beschuldigten sonst wesentlich erschwert wäre, und nicht nur dann, wenn sie sonst aussichtslos wäre.

Die strenge Subsidiaritätsklausel könnte bewirken, dass zum Beleg der sonstigen Aussichtslosigkeit umfangreiche Ermittlungen geführt werden, die zu insgesamt größeren Grundrechtseingriffen führen können als eine schon im Vorfeld erfolgreiche Verkehrsdatenerhebung.

Die vom Gesetzentwurf vorgenommene Unterscheidung zwischen erheblichen und mittels Telekommunikation begangenen Straftaten hat auch keine Entsprechung in 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. Zu Recht weist die Begründung darauf hin, dass auch in der vom Rat für Justiz und Inneres der Europäischen Union am 21. Februar 2006 angenommenen Erklärung zu Artikel 1 Abs. 1 der Richtlinie 2006/24/EG nicht zwischen schweren Straftaten und Straftaten unter Einsatz von Telekommunikationseinrichtungen unterschieden wird. Der Begriff "serious crime", der sich in der englischen Textfassung von Artikel 1 der Richtlinie findet, sei in der deutschen Fassung zwar - wenig glücklich - mit "schwere Straftat" übersetzt worden, habe im europäischen Kontext aber nicht dieselbe Bedeutung wie der nunmehr in § 100a StPO-E verwandte Begriff der "schweren Straftat". Dieser Begriff diene in europäischen Rechtsinstrumenten regelmäßig dazu, Tatbestände auszugrenzen, die lediglich die Schwere von Ordnungswidrigkeiten oder Bagatellkriminalität erreichen. Dies sei vor dem Hintergrund zu sehen, dass nicht alle Mitgliedstaaten die im deutschen Recht vorgenommene Herabstufung von ehedem strafbarem Verhalten zu Ordnungswidrigkeiten vollzogen hätten. Der Begriff "serious crime" sei daher im europäischen Kontext eher im Sinne einer "ernsthaften Straftat" zu übersetzen als mit schwerer Kriminalität zu assoziieren. Die Begründung gibt auch mit Recht zu bedenken, dass die Richtlinie 2006/24/EG keine Schwelle für den Zugriff auf die zu speichernden Daten vorgibt, sondern die Regelung des Zugangs dem Recht der Mitgliedstaaten überlässt und lediglich sichergestellt wissen will, dass dabei die einschlägigen Bestimmungen der Europäischen Union und des Völkerrechts sowie die Anforderungen der Notwendigkeit und der Verhältnismäßigkeit einzuhalten sind.

Auch auf einen generellen Ausschluss der Erhebung von Standortdaten in Echtzeit bei mittels Telekommunikation begangenen Straftaten von im Einzel-

fall nicht erheblicher Bedeutung sollte zu Gunsten der Ermöglichung einer flexiblen Verhältnismäßigkeitsprüfung verzichtet werden.

R
In

27. Zu Artikel 1 Nr. 11 (§ 100g Abs. 2 Satz 2 StPO)

In Artikel 1 Nr. 11 § 100g Abs. 2 Satz 2 sind nach dem Wort " Sachverhalts" die Wörter "oder die Ermittlung des Aufenthaltsortes des Beschuldigten" einzufügen.

Begründung:

Die Funkzellenabfrage stellt ein wichtiges Instrument der Strafverfolgung dar. Nach dem Wortlaut des Gesetzentwurfs ist diese Maßnahme allerdings nur zulässig, wenn die Erforschung des Sachverhalts andernfalls aussichtslos oder wesentlich erschwert wäre. Fälle, in denen der Sachverhalt bereits erforscht ist, jedoch der Aufenthaltsort des Beschuldigten ohne diese Maßnahme nicht oder nur unter wesentlichen Erschwernissen ermittelt werden kann, sind dagegen nicht erfasst.

Die unterschiedliche Behandlung ist nicht zweckmäßig, da Fallgestaltungen bekannt sind, in denen eine Funkzellenabfrage notwendig ist, um den Aufenthaltsort des Beschuldigten zu ermitteln, und andere Mittel nicht geeignet sind. Das Ziel, den Aufenthaltsort festzustellen, kann den Eingriff ebenfalls rechtfertigen. Die Voraussetzungen sind bei beiden Maßnahmezielen im Übrigen identisch. Eine Ergänzung des § 100g Abs. 2 Satz 2 StPO-E ist daher geboten.

In

28. Zu Artikel 1 Nr. 11 (§ 100g Abs. 2 Satz 3 -neu- und 4 -neu- StPO)

Dem Artikel 1 Nr. 11 § 100g Abs. 2 sind folgende Sätze anzufügen:

"Zur Ermittlung von Zeugen dürfen Verkehrsdaten erhoben werden, die in einem räumlich und zeitlich hinreichend bestimmten Bereich angefallen sind, wenn

1. die Erforschung einer Straftat nach § 100a Abs. 2 auf andere Weise aussichtslos oder unverhältnismäßig erschwert wäre und

2. bestimmte Tatsachen, die Annahme rechtfertigen, dass in dem Bereich, für den die Anordnung der Erhebung der Verkehrsdaten beantragt wird, Zeugen ermittelt werden können, durch deren Aussagen Hinweise auf Täter oder Teilnehmer zu erwarten sind. Solche Tatsachen können sich insbesondere aus Art oder Ausführung der Tat oder der Art der Örtlichkeit oder deren Frequentierung durch Passanten ergeben."

Begründung:

Nach § 100g Abs. 2 Satz 2 StPO-E darf sich die Anordnung einer Funkzellenauswertung nur gegen den Beschuldigten oder dessen Nachrichtenmittler richten.

Gerade bei schweren Straftaten, wie Mord oder bei Brandstiftungen, bei denen Menschenleben gefährdet werden, ist die gezielte Ansprache von potenziellen Zeugen, die im tatkritischen Zeitraum in Tatortnähe mit einem Mobilfunkgerät kommuniziert haben, ein wichtiger Ermittlungsansatz, insbesondere zur Gewinnung von Hinweisen auf Täter und Teilnehmer der Straftat.

Zur Ermittlung von Zeugen müssen die Verkehrsdaten unbeteiligter Dritter erhoben werden. Damit die Maßnahme nicht als Standardmaßnahme eingesetzt wird, sieht die vorgeschlagene Regelung folgende Sicherungsmechanismen vor:

Die Zeugenermittlung durch eine Verkehrsdatenerhebung soll nur bei schweren Straftaten entsprechend dem Straftatenkatalog des § 100a Abs. 2 StPO-E zugelassen werden.

Die Maßnahme wird nur dann zugelassen, wenn die Aufklärung durch andere Maßnahmen aussichtslos ist, z.B. weil ein Zeugenaufruf der Polizei an die Bevölkerung ergebnislos geblieben ist oder andere Ermittlungsansätze nicht weitergeführt haben (strenge Subsidiarität).

Bestimmte Tatsachen müssen die Annahme rechtfertigen, dass in dem Bereich, für den die Anordnung der Erhebung der Verkehrsdaten beantragt wird, Zeugen ermittelt werden können, durch deren Aussagen Hinweise auf Täter oder Teilnehmer zu erwarten sind. Dadurch wird klargestellt, dass Abfragen ins Blaue hinein unzulässig sind. Vielmehr muss auf der Grundlage konkreter Umstände nachvollziehbar dargelegt werden, dass auf Grund einer Funkzellenauswertung mit Zeugen gerechnet werden kann, die Hinweise zu Tat, Tätern oder Teilnehmern geben können. Solche Tatsachen können sich insbesondere aus Art oder Ausführung der Tat, der Art der Örtlichkeit oder deren Frequentierung durch Passanten ergeben.

Schließlich muss die Funkzellenabfrage auf einen räumlich und zeitlich hinreichend bestimmten Bereich begrenzt werden. Die in die Abfrage einzubeziehenden Funkzellen sind anhand der konkret aufzuklärenden Straftat zu bestimmen. Eine großflächige Abfrage, zum Beispiel aller Funkzellen einer Großstadt, wäre danach unzulässig.

R
In

29. Zu Artikel 1 Nr. 11 (§ 100g Abs. 4 und 5 -neu- StPO)

Artikel 1 Nr. 11 § 100g ist wie folgt zu ändern:

a) Absatz 4 ist wie folgt zu fassen:

"(4) Die Länder und der Generalbundesanwalt berichten dem Bundesamt für Justiz kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr

folgenden Jahres über in ihrem Zuständigkeitsbereich nach dieser Vorschrift angeordnete Maßnahmen. Das Bundesamt für Justiz erstellt eine Übersicht zu den im Berichtsjahr bundesweit angeordneten Maßnahmen."

b) Folgender Absatz 5 ist anzufügen:

"(5) In den Berichten und der Übersicht nach Absatz 4 sind anzugeben:

1. die Anzahl von Verfahren, in denen Maßnahmen nach Absatz 1 durchgeführt worden sind;
2. die Anzahl der Anordnungen von Maßnahmen nach Absatz 1;
3. die Anzahl der zurückliegenden Monate, für die Verkehrsdaten nach Absatz 1 abgefragt wurden, bemessen ab dem Zeitpunkt der Anordnung;
4. die Anzahl der Maßnahmen, die ergebnislos geblieben sind, weil die abgefragten Daten ganz oder teilweise nicht verfügbar waren."

Begründung:

Neue Berichtspflichten für den Bereich der Verkehrsdatenerhebung belasten die Praxis erheblich. Sie sollten daher nicht, wie nach dem Gesetzentwurf vorgesehen, über die Vorgaben 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, hinausgehen. Nach Artikel 10 der Richtlinie muss aus der Statistik weder bei der Anzahl der Anordnungen eine Unterscheidung nach Erst- und Verlängerungsanordnungen noch zwingend die Angabe der Anlassstraftaten hervorgehen. Der hier in Betracht kommende Spiegelstrich lautet: "in welchen Fällen im Einklang mit dem innerstaatlichen Recht Daten an die zuständigen Behörden weitergegeben worden sind,". Zur Erfüllung der Anforderungen dieses Spiegelstrichs ist die Angabe der Anzahl der Anordnungen von Verkehrsdatenerhebungen ausreichend.

Ein Zurückbleiben des Inhalts der Berichterstattung zur Verkehrsdatenerhebung hinter dem schon unabhängig von einer gesetzlichen Regelung bei der Inhaltsdatenerhebung gelieferten ist folgerichtig. Die Erhebung von Verkehrsdaten ist zum einen ein wesentlich geringerer Grundrechtseingriff als die Erhebung von Inhaltsdaten und zum anderen ein wesentlich häufiger angewandtes Ermittlungsinstrument. Die zusätzliche Belastung für die ohnehin am Rande ihrer Belastbarkeit arbeitenden Staatsanwaltschaften durch eine detaillierte statistische Erhebung wäre entsprechend größer. Eine weitere Belastung wird auch nicht dadurch gerechtfertigt, dass Grundlagen für rechtstatsächliche Untersuchungen geschaffen werden. Dies widerspräche auch der allseits bekundeten Absicht, die Justiz zu entlasten und auf ihre Kernaufgaben zu beschränken.

Eine gesetzliche Regelung einer Veröffentlichung im Internet ist nicht erforderlich.

R 30. Zu Artikel 1 Nr. 11 (§ 101 Abs. 3 Satz 1 StPO)

In Artikel 1 Nr. 11 § 101 Abs. 3 Satz 1 sind nach dem Wort "sind" die Wörter "mit Ausnahme von Maßnahmen nach § 100c StPO nur" einzufügen, der abschließende Punkt durch ein Komma zu ersetzen und folgende Wörter anzufügen: "soweit sie zu Beweiszwecken verwendet werden können."

Begründung:

Die vorgesehene umfassende Kennzeichnungspflicht personenbezogener Daten wird die Praxis vor erhebliche Umsetzungsprobleme und einen enormen Mehraufwand stellen. Es bleibt auf Grundlage der Entwurfsbegründung unklar, wie zu verfahren ist, wenn Einzelinformationen vermischt bzw. zusammengeführt werden. Dies ist etwa möglich bei polizeilichen Schlussberichten oder auch in der Anklageschrift. Die Strafverfolgungspraxis würde gerade in größeren Verfahrenskomplexen vor nahezu unlösbare Aufgaben gestellt.

Sinn und Zweck der Kennzeichnung ist aber nur die Einhaltung der Verwendungsbeschränkung nach § 100d Abs. 5, § 161 Abs. 2 und § 477 Abs. 2 StPO-E. Dabei wird, abgesehen von § 100d Abs. 5 StPO-E, die Verwendung nur für Beweiszwecke beschränkt. Entsprechend muss die Kennzeichnung auch nicht weiter gehen, als hierfür erforderlich.

Damit beschränkt sich die Kennzeichnungspflicht, abgesehen von den Fällen der Wohnraumüberwachung, auf die Originalunterlagen aus der verdeckten Maßnahme und direkte Abschriften und erfasst nicht Zusammenfassungen und Ähnliches, die zu Beweiszwecken praktisch nicht verwendet werden können. Dies sollte im Wortlaut der Norm zum Ausdruck gebracht werden, um nicht die Strafverfolgungspraxis unnötig zu belasten.

In bei Annahme entfällt Ziffer 32

31. Zu Artikel 1 Nr. 11 (§ 101 Abs. 4 Nr. 3 und 6 StPO)

Artikel 1 Nr. 11 § 101 Abs. 4 ist wie folgt zu ändern:

a) Nummer 3 ist wie folgt zu fassen:

"3. des § 100a die Betroffenen, gegen die sich die Maßnahme richtete sowie andere unvermeidbar betroffene Personen, soweit gegen sie nach Auswertung der Daten weitere Ermittlungen geführt wurden,"

b) Nummer 6 ist wie folgt zu fassen:

"6. des § 100g die Betroffenen, gegen die sich die Maßnahme richtete sowie andere unvermeidbar betroffene Personen, soweit gegen sie nach Auswertung der Daten weitere Ermittlungen geführt wurden,"

Begründung:

Kennzeichnend sowohl für die Telekommunikationsüberwachung als auch die Verkehrsdatenerhebung ist, dass die Erhebung nicht allein auf Daten der Zielperson, also die Person, gegen die die Maßnahme nach § 100a Abs. 3 bzw. § 100g Abs. 2 Satz 1 i.V.m. § 100a Abs. 3 StPO-E gerichtet werden darf (Beschuldigter, Nachrichtenmittler, Anschlussinhaber), beschränkt werden kann, denn Erkenntnisse aus der Überwachungsmaßnahme sollen ja gerade aus der Kommunikation der Zielperson mit anderen Personen gewonnen werden.

Sowohl bei der Telekommunikationsüberwachung als auch bei der Erhebung von Verkehrsdaten ist daher eine Vielzahl von Personen betroffen. Der Eingriff gegenüber den unvermeidbar betroffenen Kommunikationspartnern der Zielpersonen ist allerdings von erheblich geringerer Intensität, da der Eingriff ihnen gegenüber nicht zielgerichtet erfolgt.

Die Anknüpfung der Benachrichtigungspflicht an den Begriff des Beteiligten der überwachten bzw. der betroffenen Telekommunikation führt zu einem praktisch nicht mehr handhabbaren Adressatenkreis. So müsste z.B. im Rahmen des § 100g StPO-E jeder im Verkehrsdatennachweis aufgeführte Gesprächspartner des Beschuldigten von der Ermittlungsmaßnahme benachrichtigt werden. In größeren Ermittlungsverfahren müssten teilweise mehrere Millionen Datensätze ausgewertet werden. Auf Grund der großen Zahl der Beteiligten, die im Rahmen der genannten Maßnahmen regelmäßig betroffen sind, steht der zu erwartende Benachrichtigungsaufwand in keinem Verhältnis zu der eigentlichen Überwachungsmaßnahme und dem damit einhergehenden geringfügigen Grundrechtseingriff.

Es ist daher erforderlich, dass bereits auf Gesetzesebene eine angemessene Begrenzung der potenziell zu benachrichtigenden Personen vorgenommen wird und die Reduzierung des Adressatenkreises nicht der Praxis anhand der wenig konturierten Ausnahmetatbestände des § 101 Abs. 4 Satz 3 f. StPO-E zugemutet wird.

Bei der Postbeschlagnahme wird die Benachrichtigungspflicht richtigerweise bereits auf den Absender und Empfänger der Sendung begrenzt. Gemessen an der Ausgestaltung der Benachrichtigungspflicht bei der Telekommunikationsüberwachung und der Verkehrsdatenerhebung müsste bei der Postbeschlagnahme auch jede aus dem Inhalt der Postsendung bestimmbare Person in den Kreis der zu benachrichtigenden Personen aufgenommen werden.

Soweit dieser Argumentation in der Entwurfsbegründung (vgl. BR-Drs. 275/07, S. 70 f.) entgegengehalten wird, die Bewertung beruhe offenbar nur auf dem auch in der Untersuchung von Albrecht/Dorsch/Krüpe festgestellten Befund, wonach die Praxis den bestehenden Benachrichtigungspflichten nicht immer in der vom geltenden Recht geforderten Weise Rechnung trägt,

wird verkannt, dass sich dieser Befund in aller erster Linie auf die Handhabung der Benachrichtigungspflicht gegenüber den Zielpersonen der Maßnahme bezogen hat. Der Verweis auf die genannte Untersuchung ist daher nicht geeignet, das Erfordernis eines über diese Zielpersonen hinausgehenden Adressatenkreises zu rechtfertigen.

Zu Recht wird in der Entwurfsbegründung (vgl. a.a.O., S. 45 f.) auf die bislang in der Praxis bestehenden Meinungsverschiedenheiten bei der Frage hingewiesen, welche Personen Beteiligte im Sinne des § 101 Abs. 1 Satz 1 StPO-E und damit zu benachrichtigen sind. Der Gesetzentwurf weicht aber der Lösung dieser Frage aus, indem er im Grundsatz alle irgendwie von der Maßnahme betroffenen Personen in den Kreis der zu benachrichtigenden Personen aufnimmt und gleichzeitig der Praxis nur schwer handhabbare und wenig konturierte Ausnahmetatbestände an die Hand gibt, um diesen Adressatenkreis wieder zu reduzieren. Das Problem wird damit nur von der Auslegung des Begriffs der "Beteiligten" auf die Auslegung der Ausnahmetatbestände verlagert. Das gesetzgeberische Ziel kann auf diese Weise nicht erreicht werden. Vorzuziehen wäre daher, dass der Gesetzgeber selbst klar Position bezieht.

R
entfällt bei Annahme von Ziffer 31

32. Zu Artikel 1 Nr. 11 (§ 101 Abs. 4 Satz 1 Nr. 6 StPO)

Dem Artikel 1 Nr. 11 § 101 Abs. 4 Satz 1 Nr. 6 sind die Wörter "hinsichtlich derer weitere Ermittlungen geführt wurden, die über ein Auskunftsersuchen nach § 113 des Telekommunikationsgesetzes hinausgehen," anzufügen.

Begründung:

Durch die im Entwurf vorgesehenen Benachrichtigungspflichten besteht die konkrete Gefahr, die Ermittlungsbehörden bei der Abwicklung verdeckter Maßnahmen erheblich zu überlasten, ohne dass dies verfassungsrechtlich geboten wäre.

Der Kreis der zu Benachrichtigenden wird durch den Entwurf erheblich ausgedehnt. Dies gilt vor allem bei Auskünften über Verbindungsdaten nach § 100g StPO-E, wo ganz regelmäßig eine Vielzahl von Personen einbezogen wird, die zum allergrößten Teil aber sofort wieder als nicht verfahrensrelevante Kontakte ausgeschieden werden. Ihre Grundrechte sind daher nur minimal beeinträchtigt.

Es entsteht erheblicher Arbeitsaufwand bei den Strafverfolgungsbehörden bei der Prüfung des zu benachrichtigenden Personenkreises. Auch wenn § 101 Abs. 4 StPO-E hier Einschränkungen vorsieht, so bleibt den Staatsanwaltschaften die zeitaufwändige Prüfung der Identifizierbarkeit und die Abwägung mit anderweitigen Interessen für jede einzelne in Betracht zu ziehende Person.

Benachrichtigungen mitbetroffener Dritter bei Maßnahmen mit geringen Grundrechtsbeeinträchtigungen sind verfassungsrechtlich zudem nicht zwingend geboten. In seinem Urteil vom 3. März 2004 (- 1 BvR 2378/98 und 1 BvR 1084/99 -, BVerfGE 109, 279) zur akustischen Wohnraumüberwachung hat

das Bundesverfassungsgericht ausgeführt, dass der Begriff des Beteiligten "unter Berücksichtigung des Zwecks der Benachrichtigungspflicht" zu bestimmen sei (vgl. BVerfG a.a.O. Rnr. 303). Weiter hat es ausgeführt, dass das Bestehen einer Benachrichtigungspflicht von einer Abwägung abhänge, in deren Rahmen unter anderem die Intensität des Eingriffs eine Rolle spiele, insbesondere in welchem Umfang und zu welchem Inhalt Kommunikation des unbekannten Betroffenen abgehört und aufgezeichnet worden sei (vgl. BVerfG, a.a.O. Rnr. 307). Auch in seinem Beschluss vom 22. August 2006 (- 2 BvR 1345/03 -, NJW 2006, 805) zu § 100i StPO hat das Bundesverfassungsgericht ausgeführt, dass es angesichts der geringen Eingriffsintensität nicht unverhältnismäßig sei, auf die Benachrichtigung mitbetroffener Dritter zu verzichten (vgl. BVerfG, a.a.O. Rnr. 77).

Bei geringer Eingriffsintensität erscheint es daher zulässig, die Abwägung, ob eine Benachrichtigung erforderlich ist, nicht erst im Einzelfall, sondern allgemein durch den Gesetzgeber zu treffen. Es ist daher geboten, für die Verkehrsdatenerhebung in § 101 Abs. 4 Satz 1 Nr. 6 StPO-E den Personenkreis auf diejenigen Personen einzuschränken, gegen die weitere Ermittlungen geführt wurden, die über eine Nummernidentifizierung hinausgehen (vgl. § 101 Abs. 4 Satz 1 Nr. 1 StPO-E).

R 33. Zu Artikel 1 Nr. 15 (§ 162 Abs. 1 Satz 1a -neu- StPO)

In Artikel 1 Nr. 15 § 162 Abs. 1 ist nach Satz 1 folgender Satz einzufügen:

"Hält sie daneben den Erlass eines Haftbefehls für erforderlich, so kann sie, unbeschadet des § 125, auch diesen Antrag bei dem in Satz 1 bezeichneten Gericht stellen."

Begründung:

Mit der Konzentrationsregelung in § 162 Abs. 1 Satz 1 StPO-E wird die bisherige Regelung des Satzes 2, wonach die Staatsanwaltschaft, wenn sie richterliche Anordnungen für die Vornahme von Untersuchungshandlungen in mehr als einem Bezirk für erforderlich hält, ihre Anträge bei dem Amtsgericht stellt, in dessen Bezirk sie ihren Sitz hat, zwar in einer Vielzahl von Verfahrenskonstellationen entbehrlich. Allerdings besteht nach wie vor in der Praxis, insbesondere in umfangreichen Ermittlungsverfahren, das Bedürfnis, Anträge auf Erlass eines Haftbefehls bei dem mit dem Verfahren auf Grund anderweitiger Anträge bereits befassten Gericht zu stellen, da dadurch das Verfahren beschleunigt und abweichende Entscheidungen vermieden werden. Dies sieht der Gesetzentwurf nicht vor. Vielmehr wird in der Begründung festgestellt, dass Sonderregelungen zur Zuständigkeit wie z.B. § 125 StPO als speziellere Regelung vorgehen.

Die vorgeschlagene Einfügung des Satzes 1a trägt dem Bedürfnis Rechnung, bei Kumulation mehrerer ermittlungsrichterlicher Entscheidungen auch den

Antrag auf Erlass eines Haftbefehls bei diesem Gericht stellen zu können.

R 34. Zu Artikel 1 Nr. 18 (§ 163f Abs. 4 Satz 2 StPO)

Artikel 1 Nr. 18 ist wie folgt zu fassen:

'18. In § 163f Abs. 4 Satz 2 werden die Wörter "den Richter" durch die Wörter "das Gericht" ersetzt.'

Begründung:

Die im Gesetzentwurf vorgeschlagene Regelung ist abzulehnen.

§ 163f Abs. 3 und 4 StPO sieht bisher eine differenzierte Kompetenz für die Anordnung längerfristiger Observationen vor. Danach ist bei Anordnungen bis zu einer Dauer von höchstens einem Monat grundsätzlich die Staatsanwaltschaft zuständig. Erst bei einer Verlängerung der Maßnahme wird die Anordnung des Gerichts erforderlich.

Soweit in der Begründung des Entwurfs nunmehr ausgeführt wird, dass ein Richtervorbehalt notwendig sei, da "die längerfristige Observation im Einzelfall mit erheblichen Eingriffen in das Recht auf informationelle Selbstbestimmung des Betroffenen verbunden sein und (...) eine Eingriffsintensität erreichen kann, die eine staatsanwaltliche Anordnung nicht mehr als ausreichend erscheinen lässt", wird dem ausdrücklich entgegengetreten:

Das Bundesverfassungsgericht hat in seinem Urteil vom 12. April 2005 (- 2 BvR 581/01 -, BVerfGE 112, 304) festgestellt, dass die geltende Rechtslage verfassungsrechtlich unbedenklich ist. Es hat dabei ausgeführt, dass auch bei Verwendung von Instrumenten technischer Observation Ausmaß und Intensität des Eingriffs in das allgemeine Persönlichkeitsrecht typischerweise nicht den unantastbaren Kernbereich privater Lebensgestaltung erreichen (vgl. BVerfG, a.a.O. Rnr. 54). Es hat schließlich festgestellt: "Die in § 163f Abs. 4 Satz 2 StPO getroffene Regelung ist Ausdruck der verfassungsrechtlich geforderten Vergewisserung des Gesetzgebers im Bereich der modernen technischen Ermittlungseingriffe des Strafprozessrechts (...); sie ist Ergebnis einer gesetzgeberischen Entscheidung, die Grundrechte des Beschuldigten bei langfristiger Observation prozedural besonders zu sichern" (vgl. BVerfG, a.a.O. Rnr. 56).

Danach steht fest, dass die vorgeschlagene Ausweitung des Richtervorbehalts verfassungsrechtlich nicht erforderlich ist. Sie ist auch zur Harmonisierung des Rechts verdeckter Ermittlungsmaßnahmen nicht erforderlich. Denn die Observation ist auch dann, wenn sie längerfristig erfolgt, mit der Eingriffstiefe anderer, zu Recht dem Richtervorbehalt unterstellter Ermittlungsmaßnahmen nicht vergleichbar.

Ein Bedarf für den vorgeschlagenen Richtervorbehalt besteht auch in tatsächlicher Hinsicht nicht. Es ist insbesondere nicht ersichtlich, warum die Staatsanwaltschaft nicht in der Lage sein sollte, die Rechts- und Zweckmäßigkeit von

Ermittlungsmaßnahmen auch im Hinblick auf ihre Grundrechtsrelevanz abschließend dort zu prüfen, wo die Entscheidung nicht aus verfassungsrechtlichen Gründen dem Gericht vorzubehalten ist. Dies entspricht der gesetzlichen Aufgabenverteilung zwischen Gericht und Staatsanwaltschaft, nach der die Staatsanwaltschaft zur Verfahrensherrschaft im Ermittlungsverfahren berufen ist. Es entspricht auch ihrer Funktion als einem dem Gericht gleichgestellten Organ der Strafrechtspflege (vgl. BGHSt 24, 170 <171>), das in gleicher Weise wie das Gericht an Gesetz und Recht gebunden und zur Sicherung des rechtsstaatlichen Gebots eines fairen Verfahrens verpflichtet ist.

Schließlich spricht gegen die vorgeschlagene Änderung der Gesichtspunkt der Verfahrensökonomie. Die Staatsanwaltschaft ist auf Grund der Leitung des Ermittlungsverfahrens mit dem Sachverhalt nach dem jeweils aktuellen Ermittlungsstand vertraut und kann deswegen unmittelbar sachkundig entscheiden. Es bedarf daher weder einer zusätzlichen Aktenversendung noch einer zusätzlichen Einarbeitung in den Akteninhalt durch das Gericht.

Gegen eine redaktionelle Anpassung der Vorschrift an die Terminologie des Entwurfs im Übrigen bestehen keine Bedenken.

R
In

35. Zu Artikel 1 Nr. 20 Buchstabe a (§ 477 Abs. 2 Satz 3 Nr. 1 StPO)

In Artikel 1 Nr. 20 Buchstabe a § 477 Abs. 2 Satz 3 Nr. 1 sind nach dem Wort "Sicherheit" die Wörter "und Ordnung" einzufügen.

Begründung:

Die Streichung der erheblichen Gefahren für die öffentliche Ordnung ist abzulehnen. Aus fachlicher Sicht ist die Verwendung von Daten aus dem Bereich der Strafverfolgung auch zur Abwehr von Gefahren für die öffentliche Ordnung notwendig. Bei einer Streichung drohen sicherheitsrechtliche Lücken. Die Bedeutung der Abwehr von erheblichen Gefahren für die öffentliche Ordnung ist in den vergangenen Jahren wiederholt bestätigt worden. Exemplarisch zu nennen sind Maßnahmen gegen die öffentliche Verletzung oder Herabwürdigung von Minderheiten, des religiösen Gefühls von Personen, wenn dies den inneren Frieden im Staat zu stören droht, oder die Identifizierung unbekannter Toter nach Naturkatastrophen. In diesen Bereichen kann eine Datenübermittlung erforderlich werden. Nachdem es sich um erhebliche Gefahren handeln muss, ist - wie auch nach bisheriger Rechtslage - gewährleistet, dass der Grundsatz der Verhältnismäßigkeit gewahrt ist. Die öffentliche Ordnung ist Bestandteil der verfassungsrechtlichen Werteordnung (vgl. Artikel 13 Abs. 7 GG) und damit ein schützenswertes Gut, das im Bereich der Gefahrenabwehr nicht ohne durchgreifende Begründung außen vor bleiben kann.

In

36. Zu Artikel 1 Nr. 20 Buchstabe a (§ 477 Abs. 2 Satz 4 StPO)

In Artikel 1 Nr. 20 Buchstabe a § 477 Abs. 2 Satz 4 ist das Wort "bleibt" durch

die Wörter "und § 481 bleiben" zu ersetzen.

Begründung:

Die im Vergleich zum Referentenentwurf geänderte Fassung stellt eine erhebliche Verschlechterung der präventiven Nutzungsmöglichkeit von Daten aus strafrechtlichen Ermittlungsverfahren dar. Sie ist aus rechtlichen Gründen nicht geboten und geht an den praktischen Bedürfnissen vorbei.

Im Ergebnis wird der Versuch unternommen, die Rechtsfigur des hypothetischen Ersatzeingriffs auf wesentliche Teile der in der Gesetzgebungskompetenz der Länder liegenden präventiven Datenverarbeitung zu erstrecken.

Nach § 477 Abs. 1 i.V.m. § 481 StPO richtet sich die weitere Verarbeitung von Daten aus strafrechtlichen Ermittlungsverfahren nach den Polizeigesetzen der Länder. Soweit in den Polizeigesetzen der Länder keine weitergehende Beschränkung vorgesehen ist, wie dies in der weit überwiegenden Zahl der Landespolizeigesetze der Fall ist, können daher sämtliche Daten aus strafrechtlichen Ermittlungsverfahren für präventive Zwecke weiter verarbeitet werden und zwar unabhängig davon, ob das Datum mittels einer Maßnahme erlangt wurde, die nach der Strafprozessordnung nur bei Verdacht bestimmter Straftaten zulässig ist.

Verfehlt ist die Regelung nicht nur deshalb, weil eine präventive Nutzung von Daten, die durch eine Maßnahme nach § 477 Abs. 2 Satz 2 StPO-E erlangt wurden, nicht nur fast sämtliche heimlichen Ermittlungsmaßnahmen betreffen würde (Rasterfahndung, Telekommunikationsüberwachung, Wohnraumüberwachung, akustische Überwachung außerhalb von Wohnungen, Verkehrsdatenerhebung, IMSI-Catcher, Einsatz Verdeckter Ermittler, Schleppnetzfahndung, Ausschreibung zur polizeilichen Beobachtung, längerfristige Observation), womit viele wesentlichen Informationsquellen von der weiteren präventiven Verarbeitung weitgehend ausgeschlossen wären, sondern auch deshalb, weil die weitere Verarbeitung nur noch zum Zwecke der Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit zulässig wäre und damit das Hauptanwendungsfeld der Umwidmung repressiver Daten für präventive Zwecke ausnahmslos ausgeschlossen bliebe. Hiervon wäre vor allem die Führung von Kriminalakten und die Vorhaltung von Daten zur vorbeugenden Bekämpfung von Straftaten in polizeilichen Datenbanken betroffen.

Mit der weiteren Verarbeitung von Daten ist ein erneuter Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen verbunden. Der vorangegangene Eingriff kann insbesondere durch die Ausweitung des Empfängerkreises oder die Verarbeitung in einem neuen Verwendungszusammenhang (Zweckänderung) vertieft werden.

Die Rechtsprechung des Bundesverfassungsgerichts, die im Zusammenhang mit der Wohnraum- und der Telekommunikationsüberwachung (vgl. BVerfGE 100, 313 <369>; 109, 279 <375 f.>) formuliert wurde und auf die der neu gefasste § 477 Abs. 2 StPO-E erkennbar Bezug nimmt, kann aber nicht undifferenziert auf die gesamte repressive und präventive Datenverarbeitung ausgeweitet werden.

Die konkrete Bedeutung und Reichweite dieser Rechtsprechung, nach der eine Unvereinbarkeit vorliegen kann, wenn die Eingriffsschwelle für die weitere Verarbeitung unverhältnismäßig weit unter diejenige abgesenkt wird, die für den entsprechenden Eingriff bei der Datenerhebung (Primäreingriff) gilt, ist weitgehend ungeklärt. Schon die Formulierung des Bundesverfassungsgerichts macht deutlich, dass keineswegs eine schematische Übertragung der Eingriffsschwelle des Primäreingriffs auf den Sekundäreingriff durch die weitere Verarbeitung gefordert wird.

Nicht ohne Grund stellt auch das Bundesverfassungsgericht entscheidend darauf ab, für welche Zwecke die weitere Verarbeitung erfolgen soll. Es ist deshalb zu differenzieren, ob die weitere Verarbeitung im Strafverfahren für Beweiszwecke oder als weiterer Ermittlungsansatz oder zur Abwehr von Gefahren, einschließlich der vorbeugenden Bekämpfung von Straftaten, erfolgen soll.

Nach § 161 Abs. 2 StPO-E ist die Verwendung von Daten aus einem strafrechtlichen Ermittlungsverfahren, die durch eine Maßnahme nach § 477 Abs. 2 Satz 2 StPO-E erlangt wurden, als Ermittlungsansatz uneingeschränkt möglich. Einschränkungen werden lediglich bei der Verwendung in einem anderen Strafverfahren zu Beweiszwecken gemacht. Dies entspricht auch der vom Bundesverfassungsgericht gebilligten fachgerichtlichen und gefestigten Rechtsprechung, wonach auch Erkenntnisse, die nicht Katalogtaten betreffen, zwar im Strafverfahren nicht zu Beweiszwecken verwertet werden dürfen, aber Anlass zu weiteren Ermittlungen und zur Gewinnung neuer Beweismittel sein können (BVerfG vom 29. Juni 2005 - 2 BvR 866/05 -, NJW 2005, 2766 ff., m.w.N.).

Erst Recht muss dies für den präventiven Bereich gelten. Für die Angemessenheit der weiteren Datenverarbeitung von repressiven Daten zu präventiven Zwecken sprechen vor allem zwei Gesichtspunkte: Zum einen nimmt der Polizeivollzugsdienst sowohl Aufgaben der Strafverfolgung als auch der Gefahrenabwehr wahr. Zwischen beiden Aufgabenbereichen besteht ein enger Zusammenhang. Der Übergang ist teilweise fließend.

Zum anderen haben die in die Abwägung einzustellenden, den Grundrechtseingriff rechtfertigenden Belange regelmäßig höheres Gewicht. Während im repressiven Bereich erfolgende Eingriffe allein gegen den Gemeinwohlbelang der Strafrechtspflege abzuwägen sind, muss im präventiven Bereich zusätzlich in die Abwägung eingestellt werden, dass der Eingriff auch zum Schutz der Grundrechtsträger erfolgt, deren Rechtsgüter durch die Gefahr bedroht sind.

Ein so weitgehendes Datenverarbeitungsverbot, wie es in § 477 Abs. 2 StPO-E jetzt vorgesehen ist, könnte daher selbst zur Verletzung bedeutender Rechtsgüter führen und sich damit als unverhältnismäßiger Eingriff gegenüber der Person darstellen, zu deren Schutz die weitere Verarbeitung erforderlich ist. Die weitgehende Verarbeitungsbeschränkung in § 477 Abs. 2 StPO-E wirft somit selbst die Frage nach ihre Verfassungsmäßigkeit auf.

Die Umsetzung der vorgeschlagenen Regelung würde zu einer Implosion des polizeilichen Datenbestandes führen, der die polizeiliche Aufgabenerfüllung ernstlich in Frage stellen würde.

Wi 37. Zu Artikel 2 (Änderung des Telekommunikationsgesetzes)

Der Bundesrat bittet, im weiteren Verlauf des Gesetzgebungsverfahrens sicherzustellen, dass eine Ex-Post-Regulierung durch die Bundesnetzagentur im Sinne einer nachträglichen Missbrauchsaufsicht (§ 42 TKG) und Entgeltregulierung (§ 38 TKG) auch ohne den Abschluss eines förmlichen Marktanalyseverfahrens erfolgen kann.

Begründung:

Nach der Rechtsprechung des Verwaltungsgerichts Köln, die die frühere Praxis der Bundesnetzagentur im Bereich der Ex-Post-Regulierung untersagt hat, sofern die Verfahren der Marktdefinition und Marktanalyse nicht förmlich abgeschlossen sind, ist eine Regelungslücke auf allen Märkten entstanden, für die diese Voraussetzungen nicht erfüllt sind. Es ist den derzeitigen Marktverhältnissen in wichtigen Marktbereichen nicht angemessen, dass die Bundesnetzagentur hier keine ausreichende Eingriffsbefugnis hat und damit lediglich die allgemeine kartellrechtliche Missbrauchsaufsicht durch das Bundeskartellamt möglich ist. Es sollte daher eingehend geprüft werden, wie diese rechtssystematische und ursprünglich vom Gesetzgeber nicht gewollte Regelungslücke geschlossen werden kann.

Der Bundesrat hatte bereits in seiner Stellungnahme zum Entwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Vorschriften am 7. Juli 2006 ausgeführt, dass eine effiziente Ausgestaltung der nachträglichen Entgeltregulierung und der besonderen Missbrauchsaufsicht (§§ 38 und 42 TKG) dringend notwendig ist - vgl. BR-Drs. 359/06 (Beschluss) -; diese Auffassung hat er im so genannten Zweiten Durchgang zu diesem Gesetz in Form einer Entschließung bekräftigt (vgl. BR-Drs. 886/06 (Beschluss) vom 15. Dezember 2006). Die Existenz dieser Problematik ist zwischenzeitlich von keiner Seite angezweifelt worden, sodass der Gesetzentwurf die Gelegenheit bieten sollte, die oben genannte Regelungslücke zu schließen.

In 38. Zu Artikel 2 Nr. 01 -neu- (§ 95 Abs. 4 Satz 1 TKG)

Dem Artikel 2 Nr. 1 ist folgende Nummer 01 voranzustellen:

'01. § 95 Abs. 4 Satz 1 wird wie folgt gefasst:

"Der Diensteanbieter hat im Zusammenhang mit dem Begründen und dem Ändern des Vertragsverhältnisses sowie dem Erbringen von Telekommunikationsdiensten die Angaben des Teilnehmers anhand eines amtlichen Ausweises zu prüfen." '

Begründung:

Seit dem 25. Juni 2004 verpflichtet § 111 TKG Diensteanbieter, Kundendaten zu erheben. Die Diensteanbieter sind aber nach § 95 Abs. 4 TKG nicht zu einer wirksamen Identitätsprüfung, z.B. durch Vorlegen eines amtlichen Ausweises mit Lichtbild, verpflichtet. Die Regelung ist lediglich als "kann"-Vorschrift ausgestaltet.

Tatverdächtige und Beschuldigte verwenden zur Verschleierung von Kontakten häufig Prepaid-Karten, da der Gebrauch von herkömmlichen Kartenverträgen die Angabe einer Bankverbindung und den damit verbundenen Angaben von belegbaren Personalien bedingt. Es erfolgt ein häufiger Wechsel der Prepaid-Karten auf Grund des einfachen Vertriebssystems über Provider. Ein problemloses und anonymes "Nachladen" der Karten nach Kauf ist z.B. bei Tankstellen möglich. Die Prepaid-Karten werden auch zum Führen von Telefonaten über sogenannte Callback-Nummern benutzt. Hierbei wird über die Vorwahl 0800 zu einem Rechner eines Providers eine Verbindung hergestellt und nach Eingabe eines bestimmten Codes, welcher ohne Festhalten von Personalien gekauft werden kann, erst die eigentliche Rufnummer angewählt und das Guthaben abtelefoniert. Diese Verbindungen zum jeweiligen Provider werden meist international hergestellt, so dass die Erhebung von Verbindungsdaten in der Regel nicht oder nur sehr schwer möglich ist.

Telekommunikationsbetreiber und die Provider geben sich teilweise immer noch mit unüberprüften Selbstauskünften der Käufer hinsichtlich deren Identität zufrieden (Fiktive Personalien bzw. nicht existente Anschriften sind möglich.) bzw. verzichten innerhalb einer Frist von bis zu drei Monaten auf eine Identitätsangabe und sperren danach die Prepaid-Karte. In einer Vielzahl anderer Fälle wird nur die Adresse des Zwischenverkäufers als Anschlussinhaber registriert, obwohl die Prepaid-Karte weiterveräußert wurde. Die Erfahrung zeigt auch, dass viele der in Ermittlungsverfahren bekannt gewordenen Prepaid-Karten weiterverkauft, verschenkt oder ausgeliehen wurden. In einschlägigen Newsgroups im Internet wurde bereits dazu aufgerufen, bei Computerangriffen und Sabotagehandlungen im Internet, den Internetzugang über eine Funkmodemverbindung herzustellen und hierzu Prepaid-Karten zu nutzen, die anschließend weggeworfen werden. Damit soll eine Rückverfolgung des Täters vereitelt werden. Insbesondere im Zusammenhang mit der Bekämpfung der Schwerstkriminalität sollen die Ermittlungen häufig dadurch wesentlich erschwert werden, dass Beschuldigte bewusst und gezielt in kurzen Zeitabständen von zwei bis vier Wochen neue Prepaid-Verhältnisse eingehen und die Karten wechseln, mehrere Prepaid-Karten parallel nutzen und diese teilweise von Telefonat zu Telefonat wechseln, oder unter Angabe falscher Personalien bzw. unter dem Namen der Anbieterfirma und deren Angestellten Prepaid-Verhältnisse eingehen.

In einer Vielzahl von Fällen konnten in Verfahren wegen Verstoßes gegen das Betäubungsmittelgesetz Mittäter nicht identifiziert werden, da sie Prepaid-Karten verwendeten, die keine Rückschlüsse auf ihre Person zuließen.

Die Identifizierung von Karteninhabern ist ein ganz wesentlicher Ermittlungsansatz. Die Verpflichtung nach § 111 TKG zur Erhebung bestimmter Kundendaten kann ihren Zweck nicht erfüllen, wenn mangels wirksamer Kontrolle

durch die Diensteanbieter unrichtige Daten erhoben und gespeichert werden. So kann es nach wie vor vorkommen, dass im Rahmen von Auskunftsverfahren "Micky Maus" und "Donald Duck" als Karteninhaber ausgewiesen werden.

Es ist daher erforderlich in § 95 Abs. 4 TKG eine Verpflichtung für Diensteanbieter zu normieren, die eine verbindliche und zuverlässige Identitätsüberprüfung und Speicherung der Kundendaten von Prepaid-Karten gewährleistet.

In 39. Zu Artikel 2 Nr. 3 Buchstabe b (§ 110 Abs. 2 Nr. 1 Buchstabe a TKG)

Der Bundesrat fordert die Bundesregierung auf, die TKÜV dahin gehend zu überarbeiten, dass für die Anlieferung der Verkehrsdaten durch die Diensteanbieter ein einheitliches Dateiformat und eine einheitliche Schnittstelle sowie die Erreichbarkeit der Verpflichteten auch außerhalb der Büroarbeitszeiten geregelt wird.

Durch Artikel 2 Nr. 3 Buchstabe b wird die Verordnungsermächtigung in § 110 Abs. 2 TKG dahin gehend erweitert, dass auch Regelungen zur Erteilung von Auskünften, insbesondere im Zusammenhang mit der Erhebung von Verkehrsdaten, geschaffen werden können.

Aus der Ermittlungspraxis berichtete Probleme zeigen die Notwendigkeit auf, auch für den Bereich der Auskunftserteilung grundlegende technische und organisatorische Anforderungen festzulegen. Mangels konkreter verordnungsrechtlicher Vorgaben können die Diensteanbieter derzeit die ersuchten Verkehrsdaten in unterschiedlicher Form und unterschiedlichen Formaten, z.B. als Listenausdrucke, Excel-Tabellen auf Disketten, Tabellen im txt-Format, zur Verfügung stellen. Der Aufwand für die Aufbereitung und Auswertung der in der Regel erheblichen Datenmengen in ungeordneter Form und in nicht kompatiblen Datenformaten stellt die Sachbearbeiter vor nahezu unlösbare Aufgaben. So waren z.B. in einem Ermittlungsverfahren zur Aufklärung von Tötungsdelikten mehrere Millionen Daten zu verarbeiten und auszuwerten. Eine Überarbeitung der TKÜV ist daher erforderlich.

Wi 40. Zu Artikel 2 Nr. 3 (§ 110 Abs. 9 TKG)

Der Bundesrat fordert die Bundesregierung auf, bis zum Abschluss dieses Gesetzgebungsverfahrens eine Verordnung zur angemessenen Entschädigung von Telekommunikationsnetzbetreibern für die erbrachten Leistungen laufender Te-

lekommunikationsüberwachungen nach § 110 Abs. 9 TKG vorzulegen. Der Bundesrat verweist insoweit auf seinen Beschluss vom 14. Oktober 2005 - vgl. BR-Drs. 631/05 (Beschluss) -.

In Anbetracht der bereits heute im Zuge laufender Telekommunikationsüberwachungen extrem gestiegenen technischen und organisatorischen Anforderungen an die Telekommunikationsunternehmen, sieht es der Bundesrat als unabdingbar an, zeitgleich mit dem vorliegenden Gesetzentwurf angemessene Entschädigungsregelungen in Kraft treten zu lassen.

Begründung:

Durch die Neuregelung der Telekommunikationsüberwachung werden die ohnehin bereits hohen technischen und organisatorischen Anforderungen an die Telekommunikationsunternehmen noch weiter steigen. Dementsprechend sollte auch eine angemessene Vergütung gewährt werden, die von den üblichen Sätzen des Justizvergütungs- und -entschädigungsgesetzes (JVEG) abweicht und die die laufenden Aufwendungen der Unternehmen berücksichtigt. Die im JVEG bislang vorgesehenen Entschädigungsbeträge sind in keiner Weise ausreichend und sind darüber hinaus kaum dazu geeignet den reinen Verwaltungsaufwand der Telekommunikationsunternehmen ansatzweise zu decken.

Die Ermächtigungsgrundlage für eine Telekommunikationsentschädigungsverordnung (TK-EntschVO) ist in § 110 Abs. 9 TKG gegeben. Dementsprechend ist es nahe liegend, die Frage der Entschädigung sektorspezifisch zu regeln.

Sofern aus rechtssystematischen Gründen einer gesetzlichen Regelung der Vorzug gegeben werden soll, wäre auch dort der besonderen Situation der Telekommunikationsunternehmen angemessen Rechnung zu tragen.

Wi 41. Zu Artikel 2 Nr. 4 Buchstabe a (§ 111 Abs. 1 Satz 1 Nr. 5 und 6, Satz 4 TKG)

a) Artikel 2 Nr. 4 Buchstabe a § 111 Abs. 1 Satz 1 Nr. 5 und 6 ist wie folgt zu fassen:

"5. in Fällen, in denen im Zusammenhang mit dem Abschluss oder der Verlängerung eines Vertrages über einen Mobilfunkanschluss ein Mobilfunkendgerät überlassen wird, die Gerätenummer dieses Gerätes sowie

6. das Datum des Vertragsbeginns oder einer Vertragsverlängerung"

b) Die Pflicht nach § 111 Abs. 1 Satz 4 TKG-E ist auf die Nummern 1 bis 4 des § 111 Abs. 1 Satz 1 TKG-E zu beschränken.

Begründung:

§ 111 Abs. 1 Satz 1 Nr. 5 TKG-E soll die Pflicht zur Erhebung und Speicherung von Bestandsdaten auf die Gerätenummer ausdehnen, um hierüber Auskunft nach den §§ 112 f. TKG erteilen zu können. Diensteanbieter überlassen ihren Kunden Mobilfunkgeräte typischerweise nur im Zusammenhang mit dem Abschluss oder der Verlängerung eines Vertrages über einen Mobilfunkanschluss. Aus Gründen der Rechtsklarheit ist die Speicherpflicht deshalb ausdrücklich hierauf zu beziehen. Gleichzeitig ist sicherzustellen, dass aus § 111 Abs. 1 TKG-E keine Pflicht zur Aktualisierung der Bestandsdaten anhand erhobener Verkehrsdaten herleitbar ist. Die unterschiedlichen Speicherpflichten dürfen nicht verknüpft werden.

R
In

42. Zu Artikel 2 Nr. 4 Buchstabe c1 -neu- (§ 111 Abs. 3a -neu- TKG)
Nr. 5a -neu- (§ 113 Abs. 1 Satz 1 TKG)
Nr. 8 Buchstabe a Doppelbuchstabe aa1 -neu- (§ 149 Abs. 1 Nr. 29a -neu- TKG)

Artikel 2 ist wie folgt zu ändern:

a) In Nummer 4 ist nach Buchstabe c folgender Buchstabe c1 einzufügen:

'c1) Folgender Absatz 3a wird angefügt:

"(3a) Werden Telekommunikationsdienste im Voraus bezahlt, hat der nach Absatz 1 Satz 1 Verpflichtete, in den Fällen des Absatzes 2 Satz 1 der Vertriebspartner, die Identität des Inhabers einer Rufnummer oder einer anderen Anschlusskennung anhand amtlicher Ausweise oder sonstiger amtlicher Urkunden zweifelsfrei festzustellen und durch Kopien der Nachweise zu dokumentieren. Der Vertriebspartner hat die Kopien unverzüglich an den Diensteanbieter zu übermitteln." '

b) Nach Nummer 5 ist folgende Nummer 5a einzufügen:

'5a. In § 113 Abs. 1 Satz 1 werden nach dem Wort "erteilen" die Wörter "und Kopien nach § 111 Abs. 3a herauszugeben oder zu übermitteln" eingefügt.'

c) In Nummer 8 Buchstabe a ist nach Doppelbuchstabe aa folgender Doppelbuchstabe aa1 einzufügen:

'aa1) Nach Nummer 29 wird folgende Nummer 29a eingefügt:

"29a. entgegen § 111 Abs. 3a die Identität nicht feststellt und do-

kumentiert," '

Begründung:

Der bestehende § 95 Abs. 4 TKG gestattet es dem Diensteanbieter, von Kunden zu Vertragszwecken die Vorlage ihres Ausweises zu verlangen und von dem Ausweis eine Kopie zu fertigen, die unverzüglich nach Überprüfung der Angaben zu vernichten ist. Für eine effektive Strafverfolgung ist dies bei so genannten Prepaid-Angeboten im Mobilfunk-Bereich unzureichend. Zwar besteht nach § 111 Abs. 1 TKG-E die Pflicht zur Erhebung und Speicherung von Daten über den Rufnummerninhaber, eine Verifikationspflicht ist allerdings nicht normiert. Die Notwendigkeit einer Überprüfung anhand amtlicher Ausweise ist durch die Erfahrungen der polizeilichen Praxis allerdings belegt. Bei der Nutzung von Prepaid-Produkten durch Straftäter stehen den Strafverfolgungsbehörden auf Grund der vorhandenen Kundendaten aus der Ersterfassung häufig wertvolle Ermittlungsansätze zur Verfügung, selbst wenn die Produkte durch einen "Strohmann" erworben wurden oder wenn diese vom Ersterwerber weiter veräußert worden sind. Die Verwendung anonym erworbener Prepaid-Produkte kann die Ermittlungstätigkeit der Sicherheitsbehörden dagegen erheblich erschweren oder unmöglich machen. Angesichts der hohen Zahl von derartigen Prepaid-Angeboten kommt der Verifikation der Daten eine immer größere Bedeutung zu.

Es bedarf daher einer Ergänzung des § 111 TKG. Zur Absicherung der Qualität der Datenbasis hat derjenige, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, eine Kopie amtlicher Ausweise (Personalausweis oder Reisepass) oder sonstiger geeigneter Nachweise (bei juristischen Personen z.B. Handelsregisterauszug) zur Feststellung der Identität anzufertigen und aufzubewahren. Soweit sich der Diensteanbieter eines Vertriebspartners bedient, gilt die Verpflichtung für diesen entsprechend. Es genügt dabei nicht, dass der Kunde eine selbst angefertigte Ausweiskopie übergibt oder übersendet. Die neue Regelung wird als neuer Absatz 3a eingefügt, dessen Beachtung durch eine Bußgeldbewehrung in § 149 Abs. 1 Nr. 29a TKG-E sichergestellt wird. Die Herausgabe bzw. elektronische Übermittlung der Kopie wird in § 113 Abs. 1 Satz 1 TKG-E (Manuelles Auskunftsverfahren) geregelt. Sofern die Kopie nicht elektronisch gespeichert und damit ohne Qualitätsverlust reproduzierbar ist, ist sie nach der Auswertung an den Diensteanbieter zurückzugeben.

In 43. Zu Artikel 2 Nr. 5a -neu- (§ 113 Abs. 1 Satz 1a -neu- und 1b -neu- TKG)

In Artikel 2 ist nach Nummer 5 folgende Nummer 5a einzufügen:

'5a. In § 113 Abs. 1 werden nach Satz 1 folgende Sätze eingefügt:

"Satz 1 gilt auch für Auskünfte über Name und Anschrift eines Nutzers, wenn

sich das Auskunftsersuchen auf einen mittels dynamischer IP-Adresse und Uhrzeit eindeutig individualisierten Nutzer bezieht. Das Auskunftsersuchen kann auch unter Verwendung unvollständiger Anfragedaten erfolgen. Die um Auskunft ersuchende Stelle hat unverzüglich zu prüfen, inwieweit sie die auf Grund unvollständiger Anfragedaten übermittelten Daten benötigt; nicht benötigte Daten sind unverzüglich zu löschen." '

Begründung:

In der Entwurfsbegründung (vgl. BR-Drs. 275/07, S. 53 f.) wird zutreffend auf Unsicherheiten in der Praxis bei der Frage, ob die Auskunft über den Inhaber einer dynamischen IP-Adresse auf ein Auskunftsersuchen nach den §§ 161,163 StPO i.V.m. § 113 TKG gestützt werden kann oder nur nach Maßgabe der §§ 100g und 100h StPO-E zu erlangen ist.

Zwar entspricht es der inzwischen herrschenden Meinung, dass sich die Auskunft darüber, wer hinter einer dynamischen IP-Adresse steht, nach den §§ 161 und 163 StPO i.V.m. § 113 TKG und nicht nach den §§ 100g und 100h StPO beurteilt. Gerichtliche Entscheidung liegen bislang aber nur auf Ebene der Landgerichte vor. In der Entwurfsbegründung wird ferner ausdrücklich auf die abweichende Auffassung des Landgerichts Bonn (vgl. DuD 2005, 832 ff.) und gegenteilige Literaturauffassungen hingewiesen.

In der Praxis bereitet die Durchsetzung entsprechender Auskunftsersuchen nach wie vor Schwierigkeiten, da nicht wenige Diensteanbieter eine Auskunftserteilung nach den §§ 161 und 163 StPO i.V.m. § 113 TKG ablehnen, solange das für ihren Landgerichtsbezirk zuständige Landgericht keine positive Entscheidung getroffen hat. Durch den hinhaltenden Widerstand einiger Diensteanbieter werden die Ermittlungen zum Teil erheblich behindert.

Vor diesem Hintergrund ist eine klarstellende Regelung durch den Gesetzgeber angezeigt.

Ferner wird mit den neuen Sätzen 1a und 1b klarstellend geregelt, dass ein Auskunftsersuchen auch mit unvollständigen Anfragedaten erfolgen kann. In diesem Fall hat die ersuchende Stelle die auf Grund der unvollständigen Abfragedaten übermittelten Daten unverzüglich auf ihre Erforderlichkeit zu prüfen. Nicht benötigte Daten sind unverzüglich zu löschen.

R
In

44. Zu Artikel 2 Nr. 6 (§ 113a Abs. 1 Satz 1 TKG)

In Artikel 2 Nr. 6 § 113a Abs. 1 Satz 1 sind die Wörter "sechs Monate" durch die Wörter "ein Jahr" zu ersetzen.

Begründung:

Die vorgesehene Speicherungsdauer von sechs Monaten reicht nicht über die in Artikel 6 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, vorgesehene Mindestspeicherungsdauer von sechs Monaten hinaus und entspricht daher der Forderung des Deutschen Bundestages in seinem Beschluss vom 16. Februar 2006 (vgl. BT-Drs. 16/545, S. 4). Eine längere Speicherungsdauer ist jedoch nach Einschätzung sowohl der polizeilichen als auch der staatsanwaltschaftlichen Praxis unabdingbar, um dem Anliegen einer effektiven Strafverfolgung hinreichend Rechnung zu tragen. Von den genannten Behörden ist zu Recht darauf hingewiesen worden, dass in der Vergangenheit immer wieder Fallkonstellationen aus dem Bereich der schweren Kriminalität aufgetreten sind, in denen auch nach Ablauf von sechs Monaten ein Bedarf zur Erhebung von Verkehrsdaten bestand. Eine Speicherungsdauer von weniger als einem Jahr würde mithin mit einem nicht unerheblichen Verlust an Aufklärungsmöglichkeiten auch hinsichtlich schwerer Straftaten einhergehen, deren Aufklärung und Verfolgung zu den wesentlichen Aufgaben des Rechtsstaates gehört. Hieran gemessen stellt die Gewährleistung einer gegenüber der Mindestspeicherungsdauer moderat erhöhten Speicherungsdauer von einem Jahr an die betroffenen Telekommunikationsunternehmen keine unverhältnismäßigen Anforderungen.

Wi 45. Zu Artikel 2 Nr. 6 (§ 113a Abs. 10 Satz 2 TKG)

In Artikel 2 Nr. 6 § 113a Abs. 10 Satz 2 sind die Wörter "Er hat" durch die Wörter "Im Rahmen dessen hat er" zu ersetzen, nach dem Wort "hierzu" die Wörter "von ihm" einzufügen, der abschließende Punkt durch ein Semikolon zu ersetzen und folgende Wörter anzufügen: "diese sind gemäß § 5 Satz 2 BDSG zu verpflichten."

Begründung:

Die vorzuhaltenden Verkehrsdaten werden bereits durch § 5 BDSG und § 88 TKG geschützt. Gemäß § 9 Satz 1 BDSG sind die Diensteanbieter verpflichtet, technische und organisatorische Maßnahmen zu treffen, die den Schutz der personenbezogenen Daten sicherstellen. Ein darüber hinaus gehendes Schutzbedürfnis besteht nicht. Dies wird auch durch § 113a Abs. 10 Satz 1 TKG-E anerkannt. Die in Umsetzung der Richtlinie 2006/24/EG aufzunehmende Pflicht sicherzustellen, dass der Zugang zu diesen Daten ausschließlich hierzu besonders ermächtigten Personen möglich ist, ist daher in die bestehenden datenschutzrechtlichen Obliegenheiten einzubeziehen.

Im Hinblick auf die Rechtsfolgen eines Verstoßes gegen § 113a Abs. 10 TKG-E (vgl. § 149 Abs. 1 Nr. 38 TKG-E) muss darüber hinaus eindeutig geregelt werden, wer zur Ermächtigung berechtigt ist und welche Anforderungen an die zu ermächtigenden Personen zu stellen sind.

R
In

46. Zu Artikel 2 Nr. 6 (§ 113b Satz 1 TKG)

Der Bundesrat bittet, im weiteren Verlauf des Gesetzgebungsverfahrens

a) sicherzustellen, dass ein Diensteanbieter Auskunft über den Inhaber einer dynamischen IP-Adresse auch zur zivilrechtlichen Durchsetzung der Rechte am geistigen Eigentum erteilen und dabei die gemäß § 113a Abs. 4 TKG-E gespeicherten Daten zur Erfüllung des Auskunftsersuchens intern verarbeiten darf;

b) zu prüfen, ob zur Klarstellung der vom Gesetzentwurf gewollten Möglichkeit, auch künftig Auskunft über Bestandsdaten nach den §§ 161, 163 StPO in Verbindung mit § 113 TKG zu erteilen, in § 113b Satz 1 Halbsatz 2 TKG-E das Wort "verwenden" durch das Wort "übermitteln" ersetzt werden sollte.

Begründung:

Bei unveränderter Umsetzung des Gesetzentwurfs würde der zivilrechtliche Drittauskunftsanspruch gegenüber Internetprovidern, wie er im Entwurf eines Gesetzes zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums (BR-Drs. 64/07) in dem neuen § 140b Abs. 9 PatentG und den entsprechenden Regelungen in den anderen Gesetzen zum Schutz des geistigen Eigentums vorgesehen ist, leerlaufen, da die gemäß § 113a Abs. 4 TKG-E gespeicherten Daten nicht für eine zivilrechtliche Auskunft verwendet werden dürfen, andere aber faktisch nicht zur Verfügung stehen, auch die Qualifikation der Anfrage über den Inhaber einer dynamischen IP-Adresse als Auskunft über Bestandsdaten darüber nicht hinweghilft und § 14 Abs. 2 und § 15 Abs. 5 Satz 4 TMG nicht anwendbar sind.

Der Gesetzentwurf konterkariert damit ein wesentliches Anliegen des Gesetzentwurfs zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums. Um dies zu verhindern ist in dem Gesetzentwurf - z. B. in § 113b TKG-E - eine Regelung aufzunehmen, wonach die Weitergabe von Bestandsdaten unter interner Verwendung von nach § 113a Abs. 4 TKG-E gespeicherten Verkehrsdaten auch zulässig ist, soweit es zur zivilrechtlichen Durchsetzung der Rechte am geistigen Eigentum erforderlich ist und auf Grund eines Gesetzes erlaubt wird. Dem steht die Richtlinie über die Vorratsspeicherung von Verkehrsdaten 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, nicht entgegen.

- Nach § 113b Satz 1 TKG-E dürfen die allein auf Grund der Speicherungsverpflichtung nach § 113a TKG-E gespeicherten Daten nicht für eine zivilrechtliche Auskunft, sondern nur für die genannten Zwecke (Verfolgung von Straftaten, Abwehr von erheblichen Gefahren für die öffentliche Sicherheit oder Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden) verwendet werden.

  Grundlage für eine zivilrechtliche Auskunft, wie sie der Gesetzentwurf zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums vorsieht - unabhängig ob mit oder ohne Richtervorbehalt - können danach nur Daten sein, die die Internetprovider unabhängig von § 113a TKG-E speichern. Diese Daten sind aber gemäß § 96 Abs. 2 TKG, § 97 Abs. 3 Satz 3 TKG-E unverzüglich zu löschen, soweit sie für die Abrechnung nicht mehr erforderlich sind.

  In allen Fällen, in denen der Internetprovider auf der Basis einer Flatrate abrechnet - und dies sind gerade die in der Praxis relevanten Fälle - dürfte damit eine Speicherung der für eine Auskunft über den hinter der IP-Adresse stehenden Nutzer notwendigen Verkehrsdaten allenfalls für einen sehr kurzen Zeitraum erfolgen. Der zivilrechtliche Auskunftsanspruch wird deshalb regelmäßig nicht erfüllt werden können.

- Der Gesetzentwurf geht davon aus, dass es sich bei der Auskunft über den Inhaber einer dynamischen IP-Adresse um eine Auskunft über Bestandsdaten nach den §§ 161, 163 StPO in Verbindung mit § 113 TKG handelt und kein Beschluss gemäß den §§ 100g, 100h StPO erforderlich ist. Maßgebend sei, dass ein entsprechendes Auskunftsersuchen allein auf die Mitteilung der den Regelungen der §§ 111 ff. TKG unterfallenden Bestandsdaten gerichtet ist und nicht auf die Erhebung von - bei Stellung des Auskunftsersuchens notwendigerweise bereits bekannten - Verkehrsdaten. Der Umstand, dass der Dienstleister zur Erfüllung des Auskunftsanspruchs bei dynamischen IP-Adressen regelmäßig anhand interner Verkehrsdatenaufzeichnungen eine Zuordnung zu einer Kundenkennung vornehmen müsse, ändere daran nichts (vgl. BR-Drs. 275/07, S. 53 f.).

  Diese Auffassung deckt sich vollständig mit der Ansicht des Bundesrates in seiner Stellungnahme zum Entwurf eines Gesetzes zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums (vgl. BR-Drs. 64/07 (Beschluss) S. 8 f.); die Entwurfsbegründung weist zu Recht darauf hin.

  Der Gesetzentwurf zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums geht demgegenüber in seiner Begründung (vgl. BR-Drs. 64/07, S. 93) davon aus, dass die Auskunft bei dynamischen IP-Adressen in der Regel nur mit Hilfe von Verkehrsdaten und nicht unmittelbar über Bestandsdaten erteilt werden kann. Der Gesetzentwurf ordnet einen Richtervorbehalt gerade deswegen an, weil bei der Auskunft über den Inhaber einer dynamischen IP-Adresse Verkehrsdaten verwendet werden.

Aus den oben im ersten Spiegelstrich genannten Gründen stehen aber faktisch nur die gemäß § 113a Abs. 4 TKG-E gespeicherten Verkehrsdaten zur Verfügung, da die zur Ermittlung der Bestandsdaten notwendigen Verlaufsaufzeichnungen im Übrigen gelöscht werden müssen, sobald sie zur Entgeltermittlung und -abrechnung nicht mehr benötigt werden. § 113b Satz 1 Halbsatz 2 TKG-E verbietet aber eine Verwendung der nach § 113a TKG-E gespeicherten Daten für andere als die in Satz 1 Halbsatz 1 genannten Zwecke und damit auch die Verarbeitung dieser Daten zur Erteilung einer zivilrechtlichen Auskunft.

- In ihrer Gegenäußerung zur Stellungnahme des Bundesrates zum Entwurf eines Gesetzes zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums (BT-Drs. 16/5048) führt die Bundesregierung zu Nummer 1 aus, dass § 14 Abs. 2 TMG eine Auskunftserteilung durch den Diensteanbieter im Einzelfall zulasse, soweit es sich um Bestandsdaten im Sinne dieser Vorschrift handle und eine zur Auskunftserteilung verpflichtende Anordnung der zuständigen öffentlichen Stellen vorliege. Gemäß § 15 Abs. 5 Satz 4 TMG würde dies auch für Nutzungsdaten gelten. Die Vorschriften sind hier aber nicht anwendbar:

  Internet Service Provider, deren Leistungen überwiegend in der Übertragung von Signalen bestehen, sind zwar vom Anwendungsbereich des Telemediengesetzes umfasst und unterliegen sowohl dem TKG wie dem TMG (Begründung des Entwurfs eines Gesetzes zur Vereinheitlichung von Vorschriften über bestimmte elektronische Informations- und Kommunikationsdienste (Elektronischer-Geschäftsverkehr-Vereinheitlichungsgesetz - ElGVG) - BR-Drs. 556/06, S. 17).

  Allerdings bestimmt § 11 Abs. 3 TMG hinsichtlich des Datenschutzes, dass für Telemediendienste, die überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen und damit insbesondere für Internet-Access-Provider einschlägig sind, die Datenschutzvorschriften des Telekommunikationsgesetzes gelten und daneben nur noch bestimmte Datenschutzvorschriften des Telekommunikationsgesetzes anwendbar sind (vgl. BR-Drs. 556/06, S. 22). § 14 Abs. 2 und § 15 Abs. 5 Satz 4 TMG sind danach für Internetprovider nicht anwendbar. Vielmehr gelten für Internetprovider insoweit die Vorschriften des Telekommunikationsgesetzes.

- Den Mitgliedstaaten steht es frei, in ihrem nationalen Recht Regelungen über die Verwendung der gespeicherten Verkehrsdaten für andere als Strafverfolgungszwecke zu treffen (vgl. BR-Drs. 275/07, S. 170). Dabei sind insbesondere auch die Vorgaben der Richtlinie 2004/48/EG des Europäischen Parlaments und des Rates vom 29. April 2004 zur Durchsetzung der Rechte des geistigen Eigentums zu beachten.

  Nach der Begründung des Entwurfs zum Elektronischer-Geschäftsverkehr-Vereinheitlichungsgesetz (vgl. BR-Drs. 556/06, S. 15) dienen § 14 Abs. 2 und § 15 Abs. 5 Satz 4 TMG der notwendigen Umsetzung der Richtlinie 2004/48/EG. Da die Problematik sich gerade bei Internet Service Providern stellt, ist eine entsprechende Umsetzung erst Recht im Telekommunikationsgesetz erforderlich.

Zur Klarstellung der vom Gesetzentwurf gewollten Möglichkeit, auch künftig

Auskunft über Bestandsdaten nach den §§ 161 und 163 StPO in Verbindung mit § 113 TKG zu erteilen, wird angeregt, in § 113b Satz 1 Halbsatz 2 TKG-E das Wort "verwenden" durch das Wort "übermitteln" zu ersetzen.

Eine Verwendung der gemäß § 113a TKG-E gespeicherten Daten für eine Auskunft gemäß den §§ 161 und 163 StPO in Verbindung mit § 113 TKG scheitert nicht am Verwendungszweck. Allerdings ist im Hinblick auf die Formulierung von § 113b Satz 1 Halbsatz 2 TKG-E fraglich, ob nicht auch diese Verwendung nur unter den Bedingungen des § 113b Satz 1 Halbsatz 1 TKG-E möglich ist und damit insbesondere nur in Verbindung mit § 100g StPO.

R
In

47. Zu Artikel 2 Nr. 6 (§ 113b Satz 1 Halbsatz 1 TKG)

In Artikel 2 Nr. 6 § 113b Satz 1 Halbsatz 1 sind die Wörter "unter Bezugnahme auf § 113a" zu streichen.

Begründung:

Die Gesetzgebungskompetenz des Bundes für die Telekommunikationsüberwachung aus Artikel 73 Nr. 7 GG betrifft nach der Rechtsprechung des Bundesverfassungsgerichts lediglich die technische Seite der Errichtung einer Telekommmunikationsinfrastruktur und der Informationsübermittlung, nicht dagegen Regelungen, die auf die übermittelten Inhalte oder die Art der Nutzung der Telekommunikation ausgerichtet sind. Das Gericht hat dazu auch festgestellt (vgl. BVerfG, Urteil vom 27. Juli 2005 - 1 BvR 668/04 -, BVerfGE 113, 348, Rnr. 94), dass es bei Befugnissen zur Telekommunikationsüberwachung zu Zwecken der Gefahrenabwehr "nicht vorrangig um technische Fragen der Datenübermittlung, sondern um den Zugriff auf Informationen" geht. Weiter hat es ausgeführt: "Überwachungsmaßnahmen umfassen zwar Tätigkeiten, mit denen die Übertragungstechnik in Anspruch genommen wird; auch sind sie darauf angewiesen, dass die Ausstattung der Telekommunikationsnetze eine Überwachung technisch zulässt. Vorschriften, die die Telekommunikationsüberwachung zum Zwecke der Erlangung von Informationen für Aufgaben des Straf- oder Polizeirechts ermöglichen, werden jedoch maßgebend durch den jeweiligen Zweck der Überwachungsmaßnahmen und die daran ausgerichteten Eingriffsvoraussetzungen geprägt. Sie sind auch kompetenzmäßig dem Bereich zuzurechnen, für dessen Zwecke die Überwachung erfolgen soll, hier dem der Straftatenverhütung oder -verfolgung."

Nach diesen Grundsätzen hat der Bund keine Zuständigkeit zur Regelung der (rechtlichen und nicht nur technischen) Voraussetzungen von Befugnissen, die die Erhebung von Verkehrsdaten zu Zwecken der Gefahrenabwehr oder zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden der Länder zum Gegenstand haben. Die Gesetzgebungskompetenz liegt insoweit vielmehr bei den Ländern. Daher kann der Bund auch keine Regelung treffen, wonach eine ausdrückliche Bezugnahme bzw. eine Zitierung des § 113a TKG-E im Landesrecht rechtliche Voraussetzung für eine entsprechende Datenerhebung ist.

Die Regelung, wonach in den landesrechtlichen Befugnissen eine Bezugnahme auf § 113a TKG zu erfolgen hat, ist auch nicht zweckmäßig und kann zu erheblichen Sicherheitslücken sowie zu Wertungswidersprüchen führen. In Ländern, in denen bereits Befugnisse zur Erhebung von Verkehrsdaten zu Zwecken der Gefahrenabwehr bestehen, könnten künftig - bis zum Erlass entsprechender landesgesetzlicher Änderungen - nur die Daten erhoben werden, die zu Abrechnungszwecken gespeichert werden, nicht dagegen solche, die dem § 113a TKG-E unterfallen. Es käme daher entscheidend darauf an, ob zwischen dem Dienstleister und den Kundinnen bzw. Kunden eine pauschalierte Abrechung vertraglich vereinbart wurde. Bei der Abwehr von erheblichen Gefahren kann dies allerdings kein Kriterium dafür sein, ob Daten, die zur Abwehr von erheblichen Gefahren erforderlich sind, erhoben werden dürfen. Dies gilt nicht zuletzt deshalb, da die Datenerhebung gerade auch dem Schutz der Kundinnen und Kunden dienen kann. Entsprechendes gilt für den Bereich des Verfassungsschutzes.

[ ] nur In

[Darüber hinaus ist dem Entwurf nicht zu entnehmen - und dies birgt die Gefahr die Norm interpretierender gerichtlicher Entscheidungen -, ob es sich bei der Bezugnahme auf § 113a TKG-E in den jeweiligen Fachgesetzen lediglich um eine Herausgabebefugnis für oder gar um eine Verwendungsbeschränkung durch die Telekommunikationsdiensteanbieter handeln könnte. Bei Annahme einer Herausgabebeschränkung hätte dies zur Folge, dass bei inkorrekter Bezugnahme in den jeweils fachgesetzlichen Normen die Herausgabe der nach § 113a TKG-E zu speichernden Daten seitens der Telekommunikationsdiensteanbieter verweigert werden könnte.]

Wi 48. Zu Artikel 2 Nr. 7 (§ 115 Abs. 2 TKG)

Der Bundesrat bittet, im weiteren Verlauf des Gesetzgebungsverfahrens durch geeignete Maßnahmen sicherzustellen, dass Zwangsgelder nach § 115 Abs. 2 Satz 1 Nr. 1 TKG in Verbindung mit § 113a Abs. 1 bis 6 TKG-E nicht vor dem 1. Januar 2009 erhoben werden können.

Begründung:

Die Anwendung der Ordnungswidrigkeitentatbestände nach § 149 Abs. 1 Nr. 36 und Nr. 37 TKG-E soll nach § 150 Abs. 12b TKG-E erst nach einer angemessenen Übergangsfrist ab dem 1. Januar 2009 möglich sein. Damit wird der Tatsache Rechnung getragen, dass die Umsetzung der Speicherverpflichtungen von den Diensteanbietern größtenteils kurzfristig nicht zu bewerkstelligen ist. Dieser Zwecksetzung liefe es entgegen, bereits mit Inkrafttreten des Gesetzes die Verhängung von Zwangsgeldern zur Durchsetzung der Pflichten nach § 113a TKG-E zu ermöglichen.

In bei Annahme entfällt Ziffer 50

49. Zu Artikel 2 Nr. 9 (§ 150 Abs. 12b TKG)

In Artikel 2 Nr. 9 § 150 Abs. 12b sind die Wörter "ab dem 1. Januar 2009" durch die Wörter "drei Monate nach dem Inkrafttreten dieses Gesetzes" zu ersetzen.

Begründung:

Durch § 150 Abs. 12b TKG-E soll die Anwendung der Ordnungswidrigkeitentatbestände nach § 149 Abs. 1 Nr. 36 TKG-E (Pflicht zur Speicherung nach § 113a Abs. 1 Satz 1 oder Abs. 6 TKG-E) und § 149 Abs. 1 Nr. 37 TKG-E (Pflicht zur Sicherstellung der Speicherung nach § 113a Abs. 1 Satz 2 TKG-E) bis zum 1. Januar 2009 aufgeschoben werden. Damit soll dem Umstand Rechnung getragen werden, dass die Vorgaben aus § 113a TKG-E für die verpflichteten Unternehmen nicht ohne weiteres kurzfristig umsetzbar sind. Der Bundesgerichtshof hat allerdings deutlich herausgestellt, dass die verpflichteten Unternehmen gegenwärtig nur die Daten bis zu maximal drei Monaten speichern dürfen, die für die Rechnungsstellung unabdingbar notwendig sind. Alle Kundendaten, z. B. über Flatrate-Verträge, müssen sofort gelöscht werden. Aus diesem Grund sind Ermittlungen wegen schwerwiegender Delikte, z. B. wegen Kinderpornografie im Internet, gegenwärtig häufig aussichtslos. Von daher ist der im Gesetzentwurf vorgesehene Zeitraum bis zum Inkrafttreten der Anwendung der Ordnungwidrigkeitentatbestände am 1. Januar 2009 zu lang. Ein Zeitraum von drei Monaten nach dem Inkrafttreten des Gesetzes am 1. Januar 2008 ist ausreichend.

R entfällt bei Annahme von Ziffer 49

50. Zu Artikel 2 Nr. 9 (§ 150 Abs. 12b TKG)

Der Bundesrat bittet, im weiteren Verlauf des Gesetzgebungsverfahrens zu prüfen, ob der Zeitpunkt für die Anwendung des § 149 vorgezogen werden kann.

Begründung:

Durch die vorgesehene Regelung werden Verstöße gegen die Speicherpflicht erst zum 1. Januar 2009 sanktioniert. Die dadurch faktisch gewährte Übergangsfrist für den Beginn der Speicherfrist führt zu weit reichenden Folgen.

Betroffen sind alle Verkehrsdaten, insbesondere auch die gespeicherten IP-Adressen. Sie sind aber für die Strafverfolgung bei Delikten im Zusammenhang mit der Internetnutzung, wie etwa die Verbreitung kinderpornografischer Darstellungen, unverzichtbar, da sie meist den einzigen Ermittlungsansatz bieten. Eine zeitnahe Umsetzung der Verpflichtung zur Mindestspeicherfrist ist daher geboten.

Verkehrsdaten sind bereits aktuell immer seltener verfügbar. Durch die

Verbreitung von Flatrate-Tarifen speichern die Anbieter die entsprechenden Daten oft nur noch wenige Tage. Es steht daher zu befürchten, dass die Straftäter zukünftig ihre Kommunikation vorrangig über das Internet abwickeln, um den Zeitraum bis zur Umsetzung der Mindestspeicherfrist zu nutzen. Dadurch können erhebliche Ermittlungslücken entstehen.

Zwar zieht die Speicherpflicht für die Verpflichteten erhebliche technische und finanzielle Investitionen nach sich. Sie konnten sich aber bereits seit dem Inkrafttreten der Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, auf diese Verpflichtung einstellen. Auch ist zu berücksichtigen, dass ein Großteil der betroffenen Daten bereits jetzt temporär gespeichert wird und folglich die Technik und Logistik weit gehend vorhanden sind.

Fz 51. Zu Artikel 3 Nr. 2 Buchstabe d (§ 370 Abs. 3 Satz 2 Nr. 5 AO)

Der Bundesrat bittet, zur Vermeidung von Problemen bei der Verwertung von Erkenntnissen aus Telekommunikationsüberwachungsmaßnahmen (TKÜ) nach § 100a Abs. 2 Nr. 2 Buchstabe a StPO-E im weiteren Verlauf des Gesetzgebungsverfahrens zu prüfen, ob die Beschränkung des § 370 Abs. 3 Satz 2 Nr. 5 AO-E allein auf die Umsatz- bzw. Verbrauchsteuerhinterziehung entfallen kann.

Begründung:

Die Einschränkung des § 370 Abs. 3 Satz 2 Nr. 5 AO-E allein auf die Umsatz-/Verbrauchsteuer hat auf den Anwendungsbereich des § 100a Abs. 2 Nr. 2 Buchstabe a StPO-E und auf die steuerstrafrechtliche und steuerliche Verwertung der aus TKÜ gewonnenen Erkenntnisse erhebliche Auswirkungen.

Durch die Bezugnahme des § 100a Abs. 2 Nr. 2 Buchstabe a StPO-E auf den § 370 Abs. 3 Satz 2 Nr. 5 AO-E wären TKÜ nur in Fällen der bandenmäßig durchgeführten Umsatz-/Verbrauchsteuerhinterziehung erlaubt. Danach blieben weiterhin entsprechende Maßnahmen wegen schwerer Hinterziehung anderer Steuerarten unzulässig. Durch diese Einschränkung werden die bislang bestehenden Probleme bezüglich der steuerstrafrechtlichen und steuerlichen Verwertbarkeit von Erkenntnissen aus TKÜ nicht beseitigt, sondern gegebenenfalls vielmehr verstärkt. So können Informationen, die aus einer bezüglich des Verdachts der schweren Umsatzsteuerhinterziehung durchgeführten TKÜ gewonnen wurden, z.B. für den Bereich der Ertragsteuer, weiterhin weder im Steuerstrafverfahren noch im Besteuerungsverfahren verwertet werden. Entsprechend dem BFH-Beschluss vom 21. Februar 2001 - VII B 265/00 - bedarf es einer gesetzlichen Legimitation zur Durchbrechung des in Artikel 10 Abs. 1 GG geschützten Bereichs. Diese Berechtigung wird mit dem Gesetzentwurf je-

doch allein für den Bereich der Umsatzsteuer geschaffen. In der Praxis müssten somit die Informationen hinsichtlich ihrer Verwertbarkeit gefiltert werden. Auch sind Informationen aus TKÜ im Rahmen von Ermittlungen bezüglich anderer Delikte nur bedingt verwertbar, da nach § 100a Abs. 2 Nr. 2 StPO-E nur bei bandenmäßig begangener Umsatzsteuerverkürzung eine TKÜ zulässig ist. Der ebenfalls geänderte § 477 Abs. 2 StPO-E stellt diesbezüglich klar, dass die "Umwidmung" der durch verdeckte Ermittlungsmaßnahmen erlangten Daten zur Verwendung als Beweismittel in anderen Strafverfahren nur dann zulässig ist, wenn die betreffende Maßnahme nach der StPO bei Verdacht bestimmter Straftaten zulässig ist und sich der neue Verwendungszweck ebenfalls auf Straftaten bezieht, die die Anwendung der Maßnahme nach der StPO erlauben. Insoweit wäre eine Verwendung grundsätzlich nur in Steuerstrafverfahren wegen bandenmäßig begangenen Umsatz-/ Verbrauchsteuerbetrugs zulässig.

Eine Verbesserung der Rechtslage bezüglich der Verwertbarkeit wird durch die geplanten Gesetzesregelungen daher nur unvollständig erreicht.

Durch die Aufnahme der bandenmäßig begangenen Steuerhinterziehung in § 370 Abs. 3 Satz 2 AO als einen Fall der besonders schweren Steuerhinterziehung sollen die gegen den § 370a AO bestehenden verfassungsrechtlichen Bedenken beseitigt werden. Im derzeit noch geltenden § 370a AO erfolgt allerdings keine Unterscheidung bezüglich der Steuerarten. Auch wenn der Umsatzsteuerbetrug - insbesondere in Form des Karussell- und Kettenbetrugs - im Fokus der Überlegungen bezüglich der Änderungen stand, ist eine Einschränkung nur auf diese Steuerarten nicht nachvollziehbar. Bei Einführung des § 370a AO im Rahmen des Steuerverkürzungsbekämpfungsgesetzes erfolgte keine Einschränkung allein auf die Umsatzsteuer, obwohl diese Vorschrift vorwiegend der Bekämpfung des Umsatzsteuerbetruges dienen sollte. In Fällen des Umsatzsteuerkarussellbetruges kommt es zudem in der Regel auch zu Steuerverkürzungen anderer Steuerarten, insbesondere der Ertragsteuer. Bei einer Bestrafung wäre auf Grund der geplanten Gesetzesänderung trotz bestehenden Sachzusammenhangs hinsichtlich der jeweiligen Straftat im Strafmaß zu differenzieren, da allein die Umsatzsteuerverkürzung als schwere Steuerhinterziehung mit einem erhöhten Strafmaß sanktioniert werden könnte.

Zur Vermeidung praktischer und rechtlicher Probleme sollte das Regelbeispiel des § 370 Abs. 3 Satz 2 Nr. 5 AO-E daher nicht auf die Umsatz-/Verbrauchsteuer beschränkt werden. Eine zwingende Notwendigkeit der Selbsteinschränkung ist nicht erkennbar. Auch im Bereich anderer Steuerarten ist die bandenmäßig begangene Steuerhinterziehung denkbar. Zudem ist Voraussetzung für die Anwendung des erhöhten Strafmaßes grundsätzlich das Vorliegen einer schweren Steuerhinterziehung. Unter § 370 Abs. 3 Satz 2 AO werden nur jene Fälle aufgeführt, in denen man "in der Regel", d.h. nicht generell, von einem schweren Fall der Steuerhinterziehung ausgehen kann. Eine Einzelfallprüfung und Gewichtung der Tat ist somit immer zwingend erforderlich. Insoweit sind etwaige Befürchtungen hinsichtlich einer verstärkten Kriminalisierung von Steuerpflichtigen auf Grund des Begriffs "bandenmäßig" nicht gerechtfertigt.

Fz 52. Zu Artikel 3 Nr. 6 -neu- (§ 393 Abs. 3 -neu- AO)

Dem Artikel 3 ist folgende Nummer 6 anzufügen:

'6. Dem § 393 wird folgender Absatz 3 angefügt:

"(3) Die durch Telekommunikationsüberwachungsmaßnahmen bekannt gewordenen Tatsachen oder Beweismittel dürfen auch im Besteuerungsverfahren verwertet werden, soweit die Maßnahmen wegen einer schweren Straftat im Sinne des § 100a Abs. 2 Nr. 1 Buchstabe m oder Abs. 2 Nr. 2 der Strafprozessordnung angeordnet wurden." '

Begründung:

Erkenntnisse, die unmittelbar aus einer Telefonüberwachung in einem Strafverfahren resultieren, dürfen wegen der strikten Strafverfolgungsbezogenheit der das Grundrecht des Fernmeldegeheimnisses (Artikel 10 Abs. 1 GG) einschränkenden Regelung des § 100a StPO-E zu Besteuerungszwecken nicht herangezogen werden. Insoweit besteht ein Beweisverwertungsverbot.

Die Abgabenordnung enthält bisher weder eine eigene Befugnis für eine Beschränkung des Fernmeldegeheimnisses im Sinne des Artikels 10 Abs. 2 GG noch eine Vorschrift, die die Verwertung von Aufzeichnungen zulässt, die auf der Grundlage des § 100a StPO-E gewonnen wurden. Folglich besteht hinsichtlich solcher Informationen, die im Rahmen einer Telefonüberwachung bei strafrechtlichen Ermittlungen erlangt werden, für das Besteuerungsverfahren ein Verwertungsverbot, da die Verwertung nur in solchen Verfahren rechtmäßig möglich ist, in denen auch eine eigenständige Abhörung gesetzlich zulässig gewesen wäre.

Bisher ist eine Änderung der Abgabenordnung insoweit nicht vorgesehen. Im Hinblick auf die Bekämpfung der Umsatzsteuerhinterziehung ist dies nicht zufriedenstellend.

R
In 53. Zu Artikel 13 Nr. 2 Buchstabe a (§ 3 Abs. 2 Satz 1 Nr. 5 TKÜV)
Nr. 8 (§ 21 TKÜV)
Nr. 11 (§ 27 Abs. 8 Satz 1 TKÜV)

Artikel 13 Nr. 2 Buchstabe a, Nr. 8 und 11 sind zu streichen.

Begründung:

Im Gesetzentwurf ist vorgesehen, die Grenze für die Geltung der TKÜV in § 3 Abs. 2 Satz 1 Nr. 5 TKÜV-E anzuheben. Dies hätte zur Folge, dass die in der

Verordnung geregelten Verpflichtungen erst für Unternehmen mit 10 000 Teilnehmern und nicht wie derzeit mit 1 000 Teilnehmern gelten. Überwachungsmaßnahmen bei Anbietern unterhalb der "Teilnehmergrenze" können regelmäßig nur durch Anmietung und Implementierung von technischen Komponenten bei den jeweils Betroffenen umgesetzt werden. Dies führt zu erheblichen Erschwernissen und kann sowohl im Bereich der Gefahrenabwehr als auch der Strafverfolgung zu erheblichen Sicherheitslücken führen. Äußerst problematisch ist dabei insbesondere, dass bei diesen Unternehmen jegliche Infrastruktur fehlt (Ansprechpartner, Ausleitungskonzeptionen, Leitungsanbindung usw.). Überwachungsmaßnahmen sind somit im Regelfall erheblich zeitverzögert und nur mit beträchtlichem Aufwand zu realisieren.

Die Anhebung der Teilnehmergrenze auf 10 000 Teilnehmer ist nicht gerechtfertigt. Die in der Vergangenheit getroffenen Anordnungen erlauben keine Rückschlüsse auf die zukünftige Entwicklung des Telekommunikationsmarktes, da dieser äußerst schnelllebig und innovativ ist. Die Entwicklungen im Bereich "Neue Medien" lassen künftig vermehrt die Gründung von regionalen bzw. sogar lokalen Anbietern erwarten, z.B. im Zusammenhang mit dem neuen Breitbanddienst WiMax. Start-up-Unternehmen in der Telekommunikationsbranche könnten beispielsweise drei Tochterfirmen für diesen Dienst gründen und somit 30 000 Kunden versorgen, ohne der neuen Pflichtgrenze zu unterfallen.

Die bisherige Abstufung, die in § 21 TKÜV Abweichungen für Betreiber kleinerer Telekommunikationsanlagen vorsieht, ist demgegenüber schlüssig. Sie erfasst Betreiber, an deren Anlagen zwischen 1 000 und 10 000 Teilnehmer angeschlossen sind, und ermöglicht der Bundesnetzagentur Abweichungen zu dulden. Die bestehende Systematik ist schlüssig und berücksichtigt die Interessen der Betreiber in ausreichendem Maß.

Als weitere Folgeänderung müsste auch Artikel 2 Nr. 3, 7 und 9 gestrichen werden.

Wi 54. Zu Artikel 16 (Inkrafttreten)

Der Bundesrat bittet, im weiteren Verlauf des Gesetzgebungsverfahrens sicherzustellen, dass § 111 Abs. 1 Satz 1 Nr. 5 TKG-E erst nach einer angemessenen Frist in Kraft tritt.

Begründung:

Eine Erfassung der Gerätenummer ist bislang nur bei bestimmten Vertriebswegen und Produktarten vorgesehen. Eine flächendeckende Erhebung und Speicherung der Daten ist mit einem erheblichen Mehraufwand von der Produktkonfektion bis zur Auftragserfassung verbunden. Umfangreiche systemtechnische und organisatorische Änderungen sind vorzunehmen.

Eine kurzfristige Umsetzung der Pflicht aus § 111 Abs. 1 Satz 1 Nr. 5 TKG-E

- wie sie im Entwurf vorgesehen ist - wäre allenfalls mit einem unverhältnismäßigen Aufwand möglich. Aus Gründen der Verhältnismäßigkeit ist den betroffenen Unternehmen daher eine angemessene Umsetzungsfrist einzuräumen. Dem steht die Richtlinie 2006/24/EG nicht entgegen, da sie keine entsprechenden Erhebungs- und Speicherpflichten vorgibt.

Wi 55. Zu Artikel 16 (Inkrafttreten)

Der Bundesrat bittet, im weiteren Verlauf des Gesetzgebungsverfahrens sicherzustellen, dass die Verpflichtung zur Speicherung von Verkehrsdaten betreffend Internetzugang, Internet-Telefonie und Internet-E-Mail (§ 113a Abs. 2 Satz 1 Nr. 5, Abs. 3 und 4 TKG-E) erst am 1. Januar 2009 in Kraft tritt.

Begründung:

Die Umsetzung der Speicherverpflichtungen aus § 113a Abs. 2 Satz 1 Nr. 5, Abs. 3 und 4 TKG-E stellt erhebliche technische Anforderungen an die Anbieter von Internet-Diensten. Eine kurzfristige Implementierung der erforderlichen Systeme ist nicht möglich. Dies erkennt die Richtlinie 2006/245/EG in Artikel 15 Abs. 3 ausdrücklich an und eröffnet die Möglichkeit, die Pflicht zur Speicherung von Verkehrsdaten betreffend Internetzugang, Internet-Telefonie und Internet-E-Mail erst bis 15. März 2009 umzusetzen. Deutschland hat sich vorbehalten, von dieser Option Gebrauch zu machen. Angesichts der bestehenden technischen Schwierigkeiten muss diese Option - zumindest teilweise - auch genutzt werden.

R 56. Zum Gesetzentwurf insgesamt:

Der Bundesrat bittet, soweit sachliche Gründe für eine Differenzierung nicht bestehen, im weiteren Verlauf des Gesetzgebungsverfahrens hinsichtlich der nachstehend genannten Punkte für eine einheitliche Begrifflichkeit bzw. eine einheitliche Formulierung Sorge zu tragen, um so dem Ziel des Gesetzentwurfs, der Harmonisierung der Bestimmungen über die verdeckten Ermittlungsmaßnahmen, besser gerecht zu werden.

Der Gesetzentwurf führt in § 100b Abs. 1 Satz 3 StPO-E den Begriff der "Werktage" statt "Tage" ein zur Bestimmung der Frist, innerhalb derer eine Eilanordnung richterlich zu bestätigen ist. Durch Verweisung auf § 100b Abs. 1 Satz 3 StPO-E gilt dies nicht nur für die Telekommunikationsüberwachung, sondern auch für die akustische Überwachung außerhalb von Wohnungen

(§ 100f Abs. 4 StPO-E), die Verkehrsdatenabfrage (§ 100g Abs. 2 Satz 1 StPO-E) und den Einsatz des IMSI-Catchers (§ 100i Abs. 3 Satz 1 StPO-E). Ferner wird bei den Regelungen zur längerfristigen Observation in § 163f Abs. 3 Satz 2 StPO-E der Begriff "Werktage" gebraucht.

Nicht übernommen wurde diese Terminologie für die übrigen verdeckten Ermittlungsmaßnahmen. In den Bestimmungen über die Rasterfahndung (§ 98b Abs. 1 Satz 3 StPO), die Postbeschlagnahme (§ 100 Abs. 2 StPO), die Wohnraumüberwachung (§ 100d Abs. 1 Satz 3 StPO), die Schleppnetzfahndung (§ 163d Abs. 2 Satz 3 StPO) und die polizeiliche Beobachtung (§ 163e Abs. 4 Satz 4 StPO) geht das Gesetz nach wie vor davon aus, dass die wegen Gefahr im Verzug getroffene Anordnung binnen drei Tagen vom Gericht zu bestätigen ist. Auch beim Einsatz eines Verdeckten Ermittlers ist die Frist für die Zustimmung der Staatsanwaltschaft (§ 110b Abs. 1 Satz 2 StPO) oder des Richters (§ 110b Abs. 2 Satz 4 StPO) nach Tagen zu berechnen.

Außerdem sieht der Gesetzentwurf bei der Telekommunikationsüberwachung (§ 100a Abs. 1 StPO-E), der Wohnraumüberwachung (§ 100c Abs. 1 StPO-E) und der Verkehrsdatenabfrage (§ 100g Abs. 1 StPO-E) fast wortgleich folgende Formulierung vor, die jedoch für die Bestimmungen zur akustischen Überwachung außerhalb von Wohnungen und zum Einsatz von IMSI-Catchern nicht übernommen wurde:

"Begründen bestimmte Tatsachen den Verdacht, dass jemand als Täter oder Teilnehmer eine … Straftat begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat oder durch eine Straftat vorbereitet hat …"

Die an den Wortlaut dieser Normen angelehnte Bestimmung zur akustischen Überwachung außerhalb von Wohnungen (§ 100f Abs. 1 StPO-E) enthält weder den Zusatz "als Täter oder Teilnehmer" noch die verschiedenen Varianten der Begehung. Es heißt hier nur: "… wenn bestimmte Tatsachen den Verdacht begründen, dass jemand eine … Straftat begangen hat, …". Die Regelung zum Einsatz des IMSI-Catchers (§ 100i Abs. 1 StPO-E) lässt den Zusatz "als Täter oder Teilnehmer" vermissen.

Begründung:

Ziel des Gesetzentwurfs ist die Schaffung eines harmonischen Gesamtsystems der strafprozessualen heimlichen Ermittlungsmaßnahmen. Die entsprechenden Normen wurden daher einer umfassenden Bearbeitung unterzogen.

Neu eingeführt wird der Begriff der Werktage zur Berechnung der Frist, binnen derer eine Anordnung wegen Gefahr im Verzug richterlich zu bestätigen ist. Dies wurde jedoch nicht für alle in § 101 StPO-E als verdeckte Maßnahmen aufgeführten Ermittlungsbefugnisse umgesetzt. Im Interesse der Harmonisierung sollte eine einheitliche Fristberechnung erfolgen, soweit nicht sachliche Gründe dagegen stehen.

Harmonisiert wurde mit dem Gesetzentwurf gleichfalls der Wortlaut der Ermittlungsbefugnisse nach den §§ 100a (Telekommunikationsüberwachung), 100c (Wohnraumüberwachung), 100f (akustische Überwachung außerhalb von Wohnungen), 100g (Verkehrsdatenabfrage) und 100i StPO-E (Einsatz eines IMSI-Catchers). Die Fassung der §§ 100f und 100i StPO-E wurde an die bisher schon in den §§ 100a, 100c und 100g StPO verwendete Formulierung angeglichen. In beiden Normen fehlt jedoch die klarstellende Ergänzung, dass die Tat sowohl täterschaftlich als auch als Teilnehmer begangen worden sein kann. Ferner fehlt in den Bestimmungen über die Maßnahme der akustischen Überwachung außerhalb von Wohnungen (§ 100f StPO-E), die von der Eingriffsintensität her der Telekommunikationsüberwachung gleichgestellt ist, der Hinweis, dass die Maßnahme nicht nur im Falle der Vollendung, sondern auch im Falle des Versuchs oder der Vorbereitung durch eine Straftat zulässig ist. Demgegenüber ist eine entsprechende Formulierung Bestandteil des § 100i Abs. 1 StPO-E zum Einsatz des IMSI-Catchers. Sachliche Gründe für die Normierung unterschiedlicher Eingriffsvoraussetzungen sind nicht erkennbar. Soweit aber eine Differenzierung nicht aus sachlichen Gründen geboten ist, sollte auch für eine einheitliche Formulierung Sorge getragen werden.