

Stellungnahme

des Bundesrates

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

Der Bundesrat hat in seiner 834. Sitzung am 8. Juni 2007 beschlossen, zu dem Gesetzentwurf gemäß Artikel 76 Abs. 2 des Grundgesetzes wie folgt Stellung zu nehmen:

1. 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.

2. 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 Überwa-

chung der Telekommunikation möglich. Wie bei den Delikten aus dem Betäubungsmittelgesetz erfolgt eine Beschränkung auf besonders schwere Fälle.

3. 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,"

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.

4. 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, Nachrichtensmittler, 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 unbekanntes 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.

5. 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.

6. 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.

7. 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 zwangsläufig 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.

8. 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 Endgeräteerkennung 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 Geräteerkennung 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 Geräteerkennung 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 Endgeräteerkennung 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 Telekommunikations-

dienstleistern 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 Gerätekenung in das Mobilfunknetz - bestehen, dass die betreffende Endgerätekenung nicht allein dem zu überwachenden Endgerät zugeordnet ist.

9. 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 Auskunftersuchen 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.

10. 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.

11. 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 Internettelekkommunikation 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.

12. 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.

13. 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 Anlassstrafdaten 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.

14. 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 Verfahrenskonstel-

lationen 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.

15. 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 Entschliebung 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.

16. 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.

17. 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 Geräteummer 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.

18. Zu Artikel 2 Nr. 5a -neu- (§ 113 Abs. 1 Satz 1a -neu- bis 1c -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 Auskunftersuchen auf einen mittels dynamischer IP-Adresse und Uhrzeit eindeutig individualisierten Nutzer bezieht. Das Auskunftersuchen 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 Auskunftersuchen 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 Entscheidungen 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 Literaturlösungen hingewiesen.

In der Praxis bereitet die Durchsetzung entsprechender Auskunftersuchen 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 inhaltenden 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 Auskunftersuchen 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.

19. 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.

20. 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 Auskunftersuchens 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 Internet Providern, 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 Speicherverpflichtung 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 Verkehrsaufzeichnungen 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 scheidet 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.

21. 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 Telekommunikationsinfrastruktur 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 Abrechnung 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.

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 inkorrektter Bezugnahme in den jeweils fachgesetzlichen Normen die Herausgabe der nach § 113a TKG-E zu speichernden Daten seitens der Telekommunikationsdiensteanbieter verweigert werden könnte.

22. Zu Artikel 2 Nr. 7 (§ 115 Abs. 2 Satz 1 Nr. 1 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.

23. 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.

24. 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-/Verbrauchssteuerhinterziehung erlaubt. Danach bleiben 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 jedoch 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-/

Verbrauchssteuer 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.

25. 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.

26. 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.

27. 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.

28. 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 Eingriffintensität 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.