

23.02.04

Gesetzesantrag der Länder Hessen, Bayern

Entwurf eines Gesetzes zur Verbesserung der Überwachung der Telekommunikation (TKÜ-Verbesserungsgesetz)

A. Problem

Bei der Überwachung der Telekommunikation handelt es sich um ein wichtiges und unabdingbares Ermittlungsinstrument, mit dem insbesondere im Bereich der Organisierten Kriminalität nachvollziehbare und grundlegende Erfolge erzielt werden. Bereits seit längerer Zeit werden aus der Strafverfolgungspraxis Forderungen nach einer Einstellung zusätzlicher Verdachtstatbestände in den Katalog des § 100a StPO erhoben, die in den Stellungnahmen der Bundesregierung zu entsprechenden Gesetzesinitiativen des Bundesrates jeweils unter Hinweis auf ein Forschungsvorhaben zur "Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation" zurückgestellt worden sind. Ein Änderungsbedarf ergibt sich vor allem hinsichtlich einer Berücksichtigung von Korruptionsdelikten, schweren Straftaten aus dem Bereich der Wirtschaftskriminalität sowie bestimmten Sexualdelikten, die bisher von dem Katalog des § 100a StPO nicht erfasst werden. Dabei ist auch der Gesichtspunkt einer Harmonisierung der Deliktskataloge in den §§ 100a und 100c Abs. 1 Nr. 3 StPO sowie der Beseitigung von Wertungswidersprüchen ausschlaggebend.

B. Lösung

Nach Vorlage des Forschungsberichtes des Max-Planck-Instituts für ausländisches und internationales Strafrecht in Freiburg steht einer legislativen Umsetzung von Verbesserungsvorschlägen zur Überwachung der Telekommunikation im Bereich des Strafverfahrens nichts im Wege. Der Gesetzentwurf schlägt die Ergänzung des Deliktskataloges in § 100a Satz 1 StPO um

- die gewerbs- oder bandenmäßige Fälschung von Zahlungskarten, Schecks und Wechseln (§ 152a Abs. 3 StGB) und die Fälschung von Zahlungskarten

mit Garantiefunktion und Vordrucken von Euroschecks (§ 152b des Strafgesetzbuches),

- die Verbrechen gegen die Menschlichkeit und Kriegsverbrechen nach dem Völkerstrafgesetzbuch (§§ 6 bis 12 VStGB),
- die besonders schweren Fälle des Betruges, des Computerbetruges, des Subventionsbetruges und des Bankrotts (§ 263 Abs. 3 Satz 2, Abs. 5, § 263a Abs. 2, § 264 Abs. 2 Satz 2, Abs. 3, § 283a Satz 2 StGB) und
- die Korruptionsdelikte der Vorteilsannahme, der Bestechlichkeit, der Vorteilsgewährung sowie der Bestechung (§§ 331 bis 334 StGB)

sowie die Berücksichtigung aller Formen des sexuellen Missbrauchs von Kindern, aller Formen des schweren Menschenhandels sowie des Umgangs mit kinderpornographischen Schriften nach § 184b Abs. 1 und 2 StGB vor.

Der Gesetzentwurf hat schließlich Verbesserungen auch zum Anordnungsverfahren sowie zu anderen Ermittlungsmaßnahmen im Bereich der Telekommunikation zum Gegenstand.

C. Alternativen

Keine

D. Kosten der öffentlichen Haushalte

Durch die Anordnung von Telefonüberwachungsmaßnahmen können den Ländern Mehrkosten entstehen. Diese Kosten dürften allerdings durch Einsparungen auf Grund zu erwartender kürzerer Ermittlungen zumindest teilweise kompensiert werden. Gleiches gilt für einen zunächst zu erwartenden erhöhten Vollzugaufwand bei den Polizeibehörden, Staatsanwaltschaften und Gerichten.

E. Sonstige Kosten

Durch einen denkbaren Anstieg der Anordnungszahlen im Bereich der Überwachung der Telekommunikation sind im Rahmen der Mitwirkungspflichten der Netzbetreiber gewisse Mehrbelastungen für die Telekommunikationswirtschaft denkbar, die sich jedoch nicht näher quantifizieren lassen.

23.02.04

Gesetzesantrag
der Länder Hessen, Bayern

Entwurf eines Gesetzes zur Verbesserung der Überwachung der Telekommunikation (TKÜ-Verbesserungsgesetz)

Der Hessische Ministerpräsident

Wiesbaden, den 20. Februar 2004

An den
Präsidenten des Bundesrates
Herrn Ministerpräsidenten
Dieter Althaus

Sehr geehrter Herr Präsident,

die Bayerische Staatsregierung und die Hessische Landesregierung haben beschlossen, dem Bundesrat den beigefügten

Entwurf eines Gesetzes zur Verbesserung der Überwachung
der Telekommunikation (TKÜ-Verbesserungsgesetz)

mit dem Antrag zuzuleiten, seine Einbringung beim Deutschen Bundestag gemäß Artikel 76 Abs. 1 des Grundgesetzes zu beschließen. Ich bitte Sie, die Vorlage gemäß § 36 Abs. 2 der Geschäftsordnung des Bundesrates in die Tagesordnung der Bundesratssitzung am 12. März 2004 aufzunehmen und sie anschließend den Ausschüssen zur Beratung zuzuweisen.

Mit freundlichen Grüßen

Roland Koch

**Entwurf eines Gesetzes zur Verbesserung der Überwachung der Telekommunikation
(TKÜ-Verbesserungsgesetz)**

Der Bundestag hat das folgende Gesetz beschlossen:

**Artikel 1
Änderung der Strafprozessordnung**

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

1. § 100a Satz 1 Nr. 2 wird wie folgt geändert:

- a) Nach der Angabe "(§§ 146, 151, 152 des Strafgesetzbuches)," werden die Wörter "eine gewerbs- oder bandenmäßige Fälschung von Zahlungskarten, Schecks und Wechseln (§ 152a Abs. 3 des Strafgesetzbuches) oder eine Fälschung von Zahlungskarten mit Garantiefunktion und Vordrucken von Euroschecks (§ 152b des Strafgesetzbuches)," eingefügt.
- b) Die Wörter "einen schweren sexuellen Missbrauch von Kindern nach § 176a Abs. 1 bis 3 oder 5 des Strafgesetzbuches oder einen sexuellen Missbrauch von Kindern mit Todesfolge nach § 176b des Strafgesetzbuches" werden ersetzt durch die Wörter "einen sexuellen Missbrauch von Kindern (§§ 176 bis 176b des Strafgesetzbuches)".
- c) Nach der Angabe "§ 181 Abs. 1" wird die Angabe "Nr. 2, 3" gestrichen.
- d) Die Angabe "§ 184b Abs. 3" wird durch die Angabe "§ 184b Abs. 1 bis 3" ersetzt.
- e) Die Wörter "oder einen Völkermord (§ 6 des Völkerstrafgesetzbuches)" werden durch die Wörter ", einen Völkermord, ein Verbrechen gegen die Menschlichkeit oder ein Kriegsverbrechen (§§ 6 bis 12 des Völkerstrafgesetzbuches)" ersetzt.
- f) Nach der Angabe "§ 261 Abs. 1, 2 oder 4 des Strafgesetzbuches," werden in einer neuen Zeile die Wörter "einen Betrug (§ 263 des Strafgesetzbuches) oder einen Computerbetrug (§ 263a des Strafgesetzbuches) unter den in § 263 Abs. 3 Satz 2 oder Abs. 5, jeweils auch in Verbindung mit § 263a Abs. 2 des Strafgesetzbuches genannten Voraussetzungen, einen Subventionsbetrug (§ 264 des Strafgesetzbuches) unter den in § 264 Abs. 2 Satz 2 oder § 263 Abs. 5 in Verbindung mit § 264 Abs. 3 des Strafgesetzbuches genannten Voraussetzungen oder einen besonders schweren Fall des Bankrotts unter den in § 283a Satz 2 des Strafgesetzbuches genannten Voraussetzungen," eingefügt.

g) Nach der Angabe "der §§ 316a oder 316c des Strafgesetzbuches" werden in einer neuen Zeile die Wörter "eine Vorteilsannahme (§ 331 des Strafgesetzbuches), eine Bestechlichkeit (§ 332 des Strafgesetzbuches), eine Vorteilsgewährung (§ 333 des Strafgesetzbuches) oder eine Bestechung (§ 334 des Strafgesetzbuches) " eingefügt.

2. § 100b wird wie folgt geändert:

a) In Absatz 2 Satz 2 werden nach dem Wort "Telekommunikationsanschlusses" die Wörter "oder des Endgerätes" eingefügt.

b) In Absatz 6 wird nach Satz 1 folgender Satz eingefügt:

„Die Vernichtung kann ohne Beisein eines Vertreters der Staatsanwaltschaft erfolgen.“

3. § 100c Abs. 1 wird wie folgt geändert:

a) In Nr. 1 Buchstabe b werden nach dem Wort „Observationszwecke“ die Wörter „oder zur Ermittlung des Standortes eines aktiv geschalteten Mobilfunkendgerätes und zur Ermittlung der Geräte- und Kartennummern“ eingefügt.

b) In Nr. 3 Buchstabe a werden nach den Wörtern "eine Wertpapierfälschung (§§ 146, 151, 152 des Strafgesetzbuches)" ein Komma sowie die Wörter "eine gewerbs- oder bandenmäßige Fälschung von Zahlungskarten, Schecks und Wechseln (§ 152a Abs. 3 des Strafgesetzbuches)" eingefügt und die Wörter "oder einen Völkermord (§ 6 des Völkerstrafgesetzbuches)" durch die Wörter ", einen Völkermord, ein Verbrechen gegen die Menschlichkeit oder ein Kriegsverbrechen (§§ 6 bis 12 des Völkerstrafgesetzbuches)" ersetzt.

4. In § 100d wird folgender Absatz 7 angefügt:

"(7) Auf Grund einer Anordnung nach § 100c Abs. 1 Nr. 1 Buchstabe b hat jeder, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, dem Richter, der Staatsanwaltschaft und ihren im Polizeidienst tätigen Hilfsbeamten (§ 152 des Gerichtsverfassungsgesetzes) die für die Ermittlung des Standortes des Mobilfunkendgerätes erforderliche Geräte- und Kartennummer mitzuteilen."

5. § 100g wird wie folgt geändert:

a) Absatz 1 wird wie folgt geändert:

aa) In Satz 1 werden nach dem Wort „unverzüglich“ die Wörter „und unentgeltlich“ eingefügt.

bb) In Satz 3 wird der abschließende Punkt durch ein Semikolon ersetzt und folgender Halbsatz angefügt:

„gleichfalls darf die Aufzeichnung zukünftiger Daten im Sinne des Absatzes 3 angeordnet werden.“

b) In Absatz 3 Nr. 1 werden die Wörter „im Falle einer Verbindung“ gestrichen.

c) Folgender Absatz 4 wird angefügt:

„(4) Auskunftersuchen nach allgemeinen Bestimmungen, die an Diensteanbieter im Sinne von § 2 Nr. 1 des Teledienststedatenschutzgesetzes gerichtet werden, bleiben unberührt (§ 5 Satz 2, § 6 Abs. 5 Satz 5 des Teledienststedatenschutzgesetzes).“

6. § 100h wird wie folgt geändert:

a) Absatz 1 wird wie folgt geändert:

aa) In Satz 1 werden nach dem Wort "Telekommunikationsanschlusses" die Wörter "oder des Endgerätes" eingefügt

bb) In Satz 2 werden nach den Wörtern „des Sachverhaltes“ die Wörter „oder die Ermittlung des Aufenthaltsortes des Beschuldigten“ eingefügt.

b) Absatz 2 wird aufgehoben.

c) Der bisherige Absatz 3 wird Absatz 2.

7. § 100i wird aufgehoben.

Artikel 2

Änderung des Gesetzes zur Änderung der Strafprozessordnung vom 20. Dezember 2001

Das Gesetz zur Änderung der Strafprozessordnung vom 20. Dezember 2001 (BGBl. I S. 3879) wird wie folgt geändert:

1. Artikel 2 wird aufgehoben.

2. Der bisherige Artikel 3 wird Artikel 2.

3. Der bisherige Artikel 4 wird Artikel 3 und wie folgt gefasst:

„Artikel 3

Inkrafttreten

Dieses Gesetz tritt am 1. Januar 2002 in Kraft.“

Artikel 3
Einschränkung von Grundrechten

Das Brief-, Post- und Fernmeldegeheimnis (Artikel 10 des Grundgesetzes) werden nach Maßgabe dieses Gesetzes eingeschränkt.

Artikel 4
Inkrafttreten

Dieses Gesetz tritt am ... in Kraft.

Begründung

I. Allgemeines

Die Überwachung der Telekommunikation hat mit der Expansion des Telekommunikationsmarktes als Ermittlungsinstrument im modernen Strafverfahren erheblich an Bedeutung gewonnen. Mit Blick auf die seit mehreren Jahren zunehmenden Anordnungszahlen und den Stellenwert des grundrechtlichen Schutzes des Fernmeldegeheimnisses hat das Bundesministerium der Justiz ein Forschungsvorhaben zur "Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen" in Auftrag gegeben, dessen Ergebnisse in einem Forschungsbericht des Max-Planck-Instituts für ausländisches und internationales Strafrecht vorliegen. Als eine der zentralen Aussagen lässt sich dem Forschungsbericht entnehmen, dass die Überwachung des Fernmeldeverkehrs "als ein wichtiges und unabdingbares Ermittlungsinstrument einzuschätzen" ist, das in bestimmten Bereichen – in der Untersuchung als "Transaktionskriminalität" bezeichnet – nachvollziehbare und grundlegende Erfolge erzielt. Die Überwachung der Telekommunikation finde insoweit zielgerichtet und umsichtig Verwendung. Zwar würden die Gesprächsaufzeichnungen häufig nicht als unmittelbares Beweismittel, sondern als mittelbarer Ansatz für weitere zielführende Sekundärermittlungen genutzt. Der Erkenntniswert sei aber gleichwohl hoch; häufig würden Erkenntnisse erlangt, ohne die ein Fortgang des Ermittlungsverfahrens nicht möglich wäre.

Die Untersuchung belegt, dass die gerichtliche und staatsanwaltschaftliche Praxis trotz der in absoluten Zahlen festzustellenden Zunahme der Anordnungen hinreichend sensibel und verantwortungsbewusst mit der Befugnis zum Eingriff in das Fernmeldegeheimnis umgeht. Im internationalen Vergleich bewegt sich die Strafverfolgungspraxis der Bundesrepublik Deutschland hinsichtlich der Anzahl der Telekommunikationsüberwachungsmaßnahmen allenfalls in einem Mittelfeld. Die steigenden Anordnungszahlen sind vor dem Hintergrund eines vor allem im mobilen Fernsprechverkehr explosionsartig anwachsenden Marktes und eines sich grundlegend wandelnden Kommunikationsverhaltens der Bevölkerung zu sehen. Der Forschungsbericht weist nach, dass die Relation von überwachten und angemeldeten Telekommunikationsanschlüssen tatsächlich einen Rückgang der Überwachungsdichte belegt. Vor diesem Hintergrund wird ersichtlich, dass die Zunahme der Überwachungsmaßnahmen im Wesentlichen die Entwicklung des Telekommunikationsmarktes und des Konsumverhaltens der Bevölkerung nachzeichnet.

Bereits seit längerem werden aus der Strafverfolgungspraxis Forderungen nach einer Erweiterung des Straftatenkatalogs in § 100a StPO insbesondere hinsichtlich schwerer Vermögensdelikte, Korruptionsdelikte sowie gravierende Formen von Sexualstraftaten erhoben. Es

handelt sich dabei um Straftaten, die dem im Forschungsbericht geprägten Begriff der "Transaktionskriminalität" unterfallen und deren Aufklärung häufig das Eindringen in entsprechende Organisations- und Kommunikationsstrukturen durch verdeckte Ermittlungsmaßnahmen erforderlich macht.

Korrekturbedarf ergibt sich im Übrigen hinsichtlich einer Harmonisierung der Deliktskataloge in den §§ 100a und 100c Abs. 1 Nr. 3 StPO. So liegt in der Anerkennung von Korruptionsdelikten als Anlasstat einer Wohnraumüberwachung einerseits und der Nichtberücksichtigung in den Voraussetzungen der Telekommunikationsüberwachung andererseits ein klarer Wertungswiderspruch. Mit dem Gesetz zur Einführung des Völkerstrafgesetzbuches wurden die Kataloge allein hinsichtlich der neuen Verortung des Verbrechenstatbestandes des Völkermordes angepasst, im Übrigen aber eine – der Sache nach unbestrittene – Einstellung auch weiterer schwerer Verbrechen nach dem Völkerstrafgesetzbuch noch nicht berücksichtigt; auch insoweit besteht ein Korrekturbedarf.

Der Gesetzentwurf hat Verbesserungen auch zum Anordnungsverfahrens sowie zu anderen Ermittlungsmaßnahmen im Bereich der Telekommunikation zum Gegenstand: Mit Blick auf die aus der Praxis mitunter im Bereich der Überwachung mobiler Anschlüsse berichteten Schwierigkeiten ergibt sich ein Bedürfnis, die Überwachung der Telekommunikation auch anhand der Kennung des Endgeräts zuzulassen. Es soll klargestellt werden, dass bei Anordnungen zur Überwachung der Telekommunikation nach § 100a StPO auch die IMEI-Nummer angegeben werden kann, und dass bei der Vernichtung von Unterlagen aus einer Überwachung der Telekommunikation (§ 100b Abs. 6 StPO) kein Staatsanwalt anwesend sein muss. Schließlich werden die Regelungen zur Auskunft über Verbindungsdaten der Telekommunikation (§§ 100g, 100h StPO) sowie zum strafprozessualen Einsatz des IMSI-Catchers (§ 100i StPO) praktikabler gestaltet.

In der Diskussion um den Einsatz des sogenannten SMS-Blaster oder Stealth-Ping – es handelt sich um die Möglichkeit einer verdeckten Zusendung sogenannter SMS-Nachrichten im mobilen Fernsprechverkehr – sind Überlegungen zu einer gesetzlichen Klarstellung der Zulässigkeit angestellt worden. Tatsächlich handelt es sich bei der Maßnahme ausschließlich um die Überwachung des Echos einer (verdeckten) Signalübermittlung und damit um die Feststellung von Verbindungsdaten, die bereits de lege lata auf der Grundlage der §§ 100a, 100b, 100g, 100h StPO zugelassen ist. Der Entwurf enthält daher hierzu keine Vorschläge.

Keinen Regelungsbedarf sieht der Entwurf hingegen hinsichtlich der nachfolgenden Gesichtspunkte, die im Zusammenhang mit dem Forschungsauftrag des Max-Planck-Instituts diskutiert worden sind

- Der Forschungsbericht weist auf Defizite bei der Benachrichtigung der Betroffenen hin. So habe sich bei der Aktenanalyse in etwa zwei Dritteln der Fälle kein Hinweis auf eine Benachrichtigung gefunden. Angesichts des Gebotes in § 101 StPO, wonach die Beteiligten (§ 100a Satz 2 StPO) von der getroffenen Maßnahme zu benachrichtigen sind, sobald dies ohne Gefährdung des Untersuchungszwecks, der öffentlichen Sicherheit oder von Leib oder Leben einer Person möglich ist, handelt es sich um einen Schwachpunkt der praktischen Umsetzung und nicht der gesetzlichen Vorschriften selbst. Die erforderliche Abhilfe obliegt daher weniger dem Gesetzgeber, als vielmehr zunächst der Dienstaufsicht.
- Die Untersuchung des Max-Planck-Institutes moniert des Weiteren den Umfang der Entscheidungsgründe bei gerichtlichen Anordnungen nach den §§ 100a, 100b StPO. Klarzustellen ist, dass damit nicht die Entscheidungspraxis als solche kritisiert wird; vielmehr wird auch den Gerichten eine zielgerichtete und umsichtige Verwendung des Ermittlungsinstruments der Telekommunikationsüberwachung attestiert. Gegenstand der Kritik ist allein die Dokumentation der Entscheidungsgründe.

Der Entwurf sieht die Einfügung einer besonderen Regelung zur Begründungspflicht bei gerichtlichen Anordnungen nach § 100a StPO indes nicht vor, da eine solche Änderung unweigerlich Umkehrschlüsse für andere Entscheidungen in allen Verfahrensabschnitten nach sich ziehen würde. Die Notwendigkeit der Begründung ergibt sich bereits aus § 34 StPO. Auch insoweit weist die Strafprozessordnung eine Lücke daher nicht auf.

- Bereits im Zusammenhang mit den Beratungen zum Gesetzes zur Verbesserung der Bekämpfung der organisierten Kriminalität wurde die Frage einer mittelbaren Erstreckung der Zeugnisverweigerungsrechte auf verdeckte Ermittlungsmaßnahmen durch die Statuierung von Beweiserhebungs- und -verwertungsverboten diskutiert und für den Bereich der Wohnraumüberwachung in § 100d Abs. 3 StPO geregelt.

In seiner Entscheidung vom 12. März 2003 – 1 BvR 330/96 – (NJW 2003, S. 1787 = NStZ 2003, S. 441) hat das Bundesverfassungsgericht mittlerweile jedoch festgestellt, dass es ein verfassungsrechtliches Gebot für entsprechende Korrekturen im einfachen Recht nicht gibt. Dem Vertrauensschutz von Berufsheimnisträgern kann bei verdeckten Ermittlungsmaßnahmen einzelfallbezogen im Rahmen von Verhältnismäßigkeitserwägungen Rechnung getragen werden, ohne dass abstrakt Beschränkungen im Verfahrensrecht vorgesehen werden müssen.

Gleichwohl schlägt der Entwurf angesichts der besonderen Eingriffsintensität der in § 100c Abs. 1 Nr. 3 StPO geregelten akustischen Wohnraumüberwachung einen Verzicht auf die Regelung in § 100d Abs. 3 StPO nicht vor. Andererseits aber wird eine Einstellung entsprechender Beweisverbote auch bei den Vorschriften zur Überwachung der Telekommunikation nicht vorgesehen. Mit Blick auf das verfassungsrechtliche Gebot der Aufrechterhaltung einer funktionsfähigen Strafrechtspflege BVerfGE 74, S. 257[262]; 77, S. 65[76] und der Gefahr materiell unrichtiger und ungerechter Verfahrensergebnisse empfiehlt sich äußerste Zurückhaltung bei einer jeden zusätzlichen Beschränkung von Beweismitteln.

Mit der Streichung des § 100h Abs. 2 StPO wird der zur früheren Regelung in § 12 FAG a.F. ergangenen Entscheidung des Bundesverfassungsgerichts (NJW 2003, S. 1787 = NSTz 2003, S. 441) unmittelbar Rechnung getragen.

II. Zu den einzelnen Vorschriften

Zu Artikel 1 (Änderung der Strafprozessordnung)

Zu Nummer 1 (§ 100a StPO)

Der Gesetzentwurf sieht Erweiterungen zu dem Deliktskatalog des § 100a StPO vor, wie sie von der Strafverfolgungspraxis bereits seit längerer Zeit gefordert werden und verschiedentlich Gegenstand von Initiativen im Deutschen Bundestag und im Bundesrat gewesen sind (BT-Drs. 14/162, 14/1125, 14/5938, 14/6709, 14/6834, BR-Drs. 275/02, 326/02, 360/02 sowie 564/03(B)).

Zu Buchstabe a

Der Gesetzgeber hat in § 100c Abs. 1 Nr. 3 Buchstabe a StPO (in der Fassung des Fünfunddreißigsten Strafrechtsänderungsgesetzes zur Umsetzung des Rahmenbeschlusses des Rates der Europäischen Union vom 28. Mai 2001 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln (35. StrÄndG) vom 22. Dezember 2003, BGBl. I S. 2838) anerkannt, dass auch Straftaten nach § 152b StGB der professionellen bzw. Organisierten Kriminalität zuzurechnen sind, und deswegen bei einem entsprechenden Verdacht die akustische Wohnraumüberwachung zugelassen. Es erscheint nicht hinnehmbar, dass bei solchen Taten die Überwachung der Telekommunikation als gegenüber der Wohnraumüberwachung weniger einschneidender Grundrechtseingriff nicht zugelassen ist.

Ebenfalls dem Bereich der Organisierten Kriminalität zuzurechnen ist die nach § 152a Abs. 3 StGB qualifizierte Fälschung von Zahlungskarten, Schecks und Wechseln, die eine gewerbs- oder bandenmäßige Begehung voraussetzt. Auch insoweit scheint es angemessen, eine Überwachung der Telekommunikation bei einem entsprechenden Tatverdacht zu ermöglichen.

Zu Buchstaben b – d

Die Zulässigkeit der Telekommunikationsüberwachung soll grundsätzlich auf alle Formen des sexuellen Missbrauchs von Kindern, alle Formen des schweren Menschenhandels sowie den Umgang mit kinderpornographischen Schriften nach § 184b Abs. 1 und 2 erstreckt werden. Die in der geltenden Fassung des Kataloges insoweit vorgenommenen Differenzierungen werden der Bedeutung auch der bisher nicht erfassten Straftatbestände als typische Delikte der Organisierten Kriminalität nicht gerecht.

Zu Buchstabe e

Mit dem Gesetz zur Einführung des Völkerstrafgesetzbuches wurde zwar eine Berichtigung des Deliktskataloges im Hinblick auf die Neuverortung des Völkermordtatbestandes vorgenommen. Die weiteren Straftatbestände des VStGB blieben jedoch zunächst unberücksichtigt. Unbestritten handelt es sich bei den in §§ 7 ff. VStGB enthaltenen Verbrechen gegen die Menschlichkeit und Kriegsverbrechen um schwerste Verbrechen. § 100a StPO bedarf daher insoweit schon mit Blick auf das Verwertungsverbot in § 100b Abs. 5 StPO dringend der Anpassung.

Zu Buchstabe f

Mit der Aufnahme besonders schwerer Fälle des Betruges, des Computerbetruges, des Subventionsbetruges und des Bankrotts wird dem Bedürfnis nach einer effektiveren Verfolgung von Straftaten aus dem Bereich der Wirtschaftskriminalität Rechnung getragen. Es handelt sich um Delikte, die typischerweise in organisierter Form mit entsprechenden Kommunikationsstrukturen begangen werden und daher regelmäßig nur unter Einsatz verdeckter Ermittlungsmethoden aufgeklärt werden können. Der Katalog soll nicht auf den Bereich von Vermögensdelikten mit Massencharakter erstreckt werden, vielmehr ist die Erweiterung durch die Bezugnahme auf gesetzliche Regelbeispiele auf besonders schwere Fälle limitiert.

Zu Buchstabe g

Auch bei der Aufnahme der Korruptionsdelikte in den §§ 331 bis 334 StGB handelt es sich um eine bereits seit längerer Zeit erhobene Forderung der Strafverfolgungspraxis, die auf eine Verbesserung der Aufklärungsmöglichkeiten bei einer für die Organisierte Kriminalität typischen Deliktsform zielt. Zugleich dient die vorgeschlagene Korrektur der Beseitigung eines Wertungswiderspruchs, der sich aus der unterschiedlichen Behandlung der §§ 332, 334 StGB in den Katalogen des § 100a StPO einerseits und des § 100c Abs. 1 Nr. 3 StPO andererseits ergibt.

Zu Nummer 2 (§ 100b StPO)

Zu Buchstabe a

Nach § 100b Abs. 2 Satz 2 StPO ist in einer Anordnung nach § 100a StPO u.a. „die Rufnummer oder eine andere Kennung des Telekommunikationsanschlusses“ anzugeben. Nach der Rechtsprechung des Ermittlungsrichters beim BGH reicht dabei die Bezeichnung der elektronischen Gerätekenung (IMEI, International Mobile Equipment Identity) aus. Eine Erhebung der Rechtstatsachensammelstelle des Bundeskriminalamts (vgl. dazu auch Thiede, Kriminallistik 2003, 165) hat jedoch ergeben, dass es trotz dieser Entscheidung in der Praxis immer wieder zu Problemen kommt, wenn in der Anordnung nach § 100a StPO nur die IMEI-Nummer angegeben ist. Diese Probleme können durch eine entsprechende Klarstellung in § 100b Abs. 2 Satz 2 StPO vermieden werden.

Zu Buchstabe b

Nach § 100b Abs. 6 Satz 1 StPO sind Tü-Unterlagen „unter Aufsicht der Staatsanwaltschaft“ zu vernichten. Im Anschluss an die Ansicht von Schnarr (MDR 1987, 1, 4) geht die Praxis teilweise von der Notwendigkeit einer physischen Anwesenheit des Staatsanwaltes beim Vernichtungsvorgang aus. Hierdurch werden ohne Not personelle Ressourcen der Staatsanwaltschaft gebunden, die anderweitig sinnvoller eingesetzt werden können. Es ist daher angezeigt, eine klare gesetzliche Regelung dahingehend zu treffen, dass auf eine persönliche Anwesenheit eines Vertreters der Staatsanwaltschaft beim Lösungs- bzw. Vernichtungsvorgang verzichtet werden kann. Dabei dürfte es sich - entgegen der Auffassung von Schnarr (a.a.O.) - um eine bloße Klarstellung handeln, denn dem derzeit geltenden § 100b Abs. 6 Satz 1 StPO lässt sich nicht eindeutig entnehmen, dass die Vernichtung der Unterlagen in Gegenwart eines Staatsanwaltes erfolgen muss. Weder die Gesetzesmaterialien (BT-Drs. 5/1880 S. 13) noch der Wortlaut von § 100b Abs. 6 Satz 1 StPO zwingen zu einer sol-

chen Auslegung. Im Gegenteil spricht die Formulierung "unter Aufsicht" gerade dafür, dass nicht eine physische Gegenwart des Staatsanwalts, sondern eine übergeordnete Verantwortlichkeit und Steuerung des Vernichtungsvorgangs gemeint ist. Sinn und Zweck der Einbindung der Staatsanwaltschaft in den Vernichtungsvorgang gemäß § 100b Abs. 6 Satz 1 StPO ist es, dass die Staatsanwaltschaft den Umfang der Aussonderung bestimmt, damit nicht aus übergroßer Vorsicht zu wenig vernichtet wird, sowie, dass alles Beweiserhebliche erhalten bleibt (Schäfer in Loewe-Rosenberg, StPO, 24. Aufl., § 100b, Rdnr. 9 a). Dieser Normzweck wird durch eine physische Anwesenheit eines Staatsanwalts bei der Vernichtung der Unterlagen nicht gefördert, bei einer Abwesenheit des Staatsanwalts während der Vernichtung nicht beeinträchtigt.

Zu Nummern 3 (§ 100c StPO)

Zu Buchstabe a

Bei der Verfolgung von Straftaten kann es notwendig werden, durch einen so genannten IMSI-Catcher den Standort eines aktiv geschalteten Mobilfunkendgerätes und/oder die Geräte- und Kartenummern zu ermitteln. Eine solche Maßnahme war schon vor Schaffung von § 100i StPO zulässig. Die Bundesregierung sah insoweit §§ 100a ff, 161 StPO als Rechtsgrundlage an (vgl. BT-Drs. 14/6885), die Rechtsprechung hat auch § 100c Abs. 1 Nr. 1 Buchst. b StPO angewendet (vgl. z.B. Beschluss des AG München vom 5. September 2001, Gz. ER II Gs 9039/01).

Ohne Not hat der Gesetzgeber im Gesetz zur Änderung der Strafprozessordnung vom 6. August 2002 (BGBl I S. 3018) mit § 100i StPO eine komplizierte und viel zu restriktive Regelung zum strafprozessualen Einsatz des IMSI-Catchers geschaffen, die sich in der Praxis nicht bewährt hat. Zur Vorbereitung einer Überwachung der Telekommunikation ist der Einsatz des sog. IMSI-Catchers nach geltendem Recht nur zulässig, wenn insbes. die Voraussetzungen der Telefonüberwachung nach § 100a StPO vorliegen; zur vorläufigen Festnahme oder Ergreifung setzt der Einsatz des IMSI-Catchers nach geltendem Recht insbesondere eine Straftat von erheblicher Bedeutung voraus. Der Einsatz des sog. IMSI-Catchers wird zudem durch Subsidiaritätsklauseln, Verwendungsbeschränkungen und Lösungsverpflichtungen weiter begrenzt und unter einen Richtervorbehalt gestellt. Für alle diese Einschränkungen besteht kein Anlass. Der IMSI-Catcher ist als ein technisches Observationsmittel anzusehen. Maßnahmen nach § 100i StPO tangieren - jedenfalls nach Auffassung des Gesetzgebers - das Fernmeldegeheimnis nach Art. 10 GG nicht, denn im Gesetz zur Änderung der Strafprozessordnung vom 6. August 2002 (BGBl I S. 3018), mit dem § 100i StPO geschaffen wurde, wird Art. 10 GG nicht als einzuschränkendes Grundrecht zitiert.

Im Interesse der Inneren Sicherheit muss § 100i StPO deshalb durch eine praxistaugliche Regelung ersetzt werden, die den Anwendungsbereich des IMSI-Catchers nicht ohne Not beschränkt. Der Bundesrat hatte eine solche Regelung bereits in dem Entwurf eines Gesetzes zur Verbesserung der Ermittlungsmaßnahmen wegen des Verdachts sexuellen Missbrauchs von Kindern und der Vollstreckung freiheitsentziehender Sanktionen (BT-Drs. 14/9801) vorgeschlagen, die hier wieder aufgegriffen wird. Danach wird der Einsatz des IMSI-Catchers in § 100c Abs. 1 Nr. 1 Buchst. b StPO geregelt, wegen des Sachzusammenhanges also bei den technischen Observationsmitteln, nicht aber bei den Maßnahmen der Überwachung der Telekommunikation.

Zu Buchstabe b

Die Ergänzung zu § 152a Abs. 3 StGB sowie zu den Verbrechenstatbeständen des Völkerstrafgesetzbuches entspricht den insoweit ebenfalls vorgeschlagenen Anpassungen des § 100a Satz 1 Nr. 2 StPO und berücksichtigt die bereits mit dem Fünfunddreißigsten Strafrechtsänderungsgesetz zur Umsetzung des Rahmenbeschlusses des Rates der Europäischen Union vom 28. Mai 2001 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln (35. StrÄndG) vom 22. Dezember 2003 (BGBl. I S. 2838) in Kraft getretenen Änderungen des § 100c Abs. 1 Nr. 3 StPO. Es wird dadurch dem Umstand Rechnung getragen, dass die Qualifikation der Fälschung von Zahlungskarten, Schecks und Wechseln in § 152a Abs. 3 StGB eine gewerbs- oder bandenmäßige Begehung voraussetzt und damit ebenfalls der Organisierten Kriminalität zuzurechnen ist. Das Bedürfnis für den Einsatz der akustischen Wohnraumüberwachung wird erkennbar nicht durch die nunmehr in § 152b StGB erfasste Garantiefunktion der geschützten Karten oder Vordrucke limitiert. Zum anderen wird der besonderen Schwere der in §§ 7 ff. des VStGB enthaltenen Verbrechen gegen die Menschlichkeit und Kriegsverbrechen auch für die akustische Wohnraumüberwachung Rechnung getragen.

Zu Nummer 4 (§ 100d StPO)

Der Vorschlag eines neuen Absatz 7 übernimmt die bisherige Regelung aus § 100i Abs. 4 Satz 4 StPO zu den Mitwirkungspflichten der Dienstleister im Bereich der Telekommunikation. Da die bisherige Anordnung nach § 100i Abs. 1 Nr. 2 StPO nach dem Entwurf unter den geänderten § 100c Abs. 1 Nr. 1 Buchst. b StPO fallen soll, wird auf diese Vorschrift Bezug genommen.

Zu Nummer 5 (§ 100g StPO)

Zu Buchstabe a

In § 100g Abs. 1 Satz 1 StPO-E wird klargestellt, dass Auskünfte über Telekommunikationsverbindungsdaten unentgeltlich zu erteilen sind. Die Parallelregelungen in § 8 Abs. 8 BVerfSchG, § 10 Abs. 3 MADG und § 8 Abs. 3a BNDG (jeweils in der Fassung des Terrorismusbekämpfungsgesetzes vom 9. Januar 2002, BGBl. I S. 361) regeln, dass die Auskünfte unentgeltlich sind. Dies sollte auch für das Strafverfahren gelten.

Mit § 100g Abs. 1 Satz 3 Halbsatz 2 StPO-E sollen nach dem Vorbild von § 16b WpHG in der Fassung von Art. 2 Nr. 10 des Vierten Finanzmarktförderungsgesetzes vom 21. Juni 2002 (BGBl. I S. 2010, 2316) Regelungen geschaffen werden, wonach die Unternehmen im Einzelfall verpflichtet werden können, Telekommunikationsverbindungsdaten für Strafverfolgungszwecke aufzuzeichnen. Die - abgesehen von § 16b WpHG - bestehenden Regelungen des Telekommunikationsrechtes, die sich vor allem auf die Speicherung solcher Daten für kommerzielle Zwecke beziehen, reichen nicht aus. Es sollte nicht nur - wie in § 16b WpHG vorgesehen - zur Durchsetzung der Verbote der Insidergeschäfte und der Kurs- und Marktpreismanipulation möglich sein, von einem Unternehmen die Aufbewahrung von Verbindungsdaten über den Zeitpunkt der Abrechnung hinaus zu verlangen. Vielmehr müssen auch die Strafverfolgungsbehörden die Befugnis erhalten, im Einzelfall die Aufbewahrung von Telekommunikationsverbindungsdaten anordnen zu können.

Zu Buchstabe b

§ 100g Abs. 3 Nr. 1 StPO-E greift ein Anliegen auf, das bereits im Gesetzgebungsverfahren zur Nachfolgeregelung von § 12 FAG erörtert worden ist. Hintergrund ist das de lege lata bestehende Problem einer Regelungslücke insbesondere im Bereich der Sexualdelikte auf Grund fehlender Nutzungsmöglichkeit der Standortkennung von Mobiltelefonen zu Strafverfolgungszwecken. Durch das Absehen vom Erfordernis der Telekommunikationsverbindung in § 100g Abs. 3 Nr. 1 StPO-E wird erreicht, dass die Nutzung der Standortkennung zur Aufklärung aller Straftaten von erheblicher Bedeutung, also auch der Straftaten gegen die sexuelle Selbstbestimmung, ermöglicht wird. Insbesondere wird – flankierend zur Telekommunikationsüberwachung im Rahmen der Strafvollstreckung – die zusätzliche Möglichkeit geschaffen, entflozene gefährliche Straftäter unverzüglich wieder zu ergreifen. Die Regelung knüpft systematisch an die allgemeinen Eingriffsvoraussetzungen des § 100g StPO an. Von einer Ermöglichung der inhaltlichen Überwachung von Telefongesprächen wird abgesehen und damit gleichzeitig der Grundrechtseingriff auf das erforderliche Maß begrenzt.

Zu Buchstabe c

§ 100g Abs. 4 StPO-E dient der Klarstellung. Die Parallelregelungen in § 8 Abs. 8 BVerfSchG, § 10 Abs. 3 MADG und § 8 Abs. 3a BNDG (jeweils in der Fassung des Terrorismusbekämpfungsgesetzes vom 9. Januar 2002, BGBl. I S. 361) gelten jeweils nicht nur für den Bereich der Telekommunikation, sondern auch für den Bereich der Teledienste. Damit wird bundesrechtlich für einen außerstrafverfahrensrechtlichen Bereich eine detaillierte Regelung zur Auskunftserteilung in Bezug auf Teledienstnutzungsdaten geschaffen. Hierdurch könnte die Gefahr von Umkehrschlüssen entstehen, wonach für Strafverfolgungszwecke derartige Auskünfte nicht möglich sein könnten. Zu Klarstellungszwecken erscheint daher ein Hinweis zweckmäßig, dass Auskünfte in Bezug auf die Teledienste nach den allgemeinen strafprozessualen Regelungen (z. B. Zeugenvernehmung, Beschlagnahme, § 161 Abs. 1 StPO) möglich bleiben. Eine entsprechende Bestimmung ist auch in § 5 Satz 2 und § 6 Abs. 5 Satz 5 TDDSG enthalten.

Zu Nummer 6 (§ 100h StPO)

Hinsichtlich der Ergänzung von § 100h Abs. 1 Satz 1 StPO wird auf die Begründung der entsprechenden Ergänzung von § 100b Abs. 2 Satz 2 StPO Bezug genommen.

In § 100h Abs. 1 Satz 2 StPO wird die Möglichkeit eines Auskunftsanspruchs zum Zwecke der Ermittlung des Aufenthaltsortes des Beschuldigten aufgenommen, weil damit der Aufenthaltsort eines Beschuldigten über den Standort seines aktiv geschalteten Mobiltelefons innerhalb eines Umkreises von ca. 300 m ermittelt werden kann. Durch die Bezeichnung dieses Umkreises ist die Telekommunikation zugleich räumlich hinreichend bestimmt.

Zugleich wird die Einschränkung nach § 100h Abs. 2 StPO aufgehoben, da hierdurch die effektiven Ermittlungen erschwert werden. Die Parallelregelungen in § 8 Abs. 8 BVerfSchG, § 10 Abs. 3 MADG und § 8 Abs. 3a BNDG (jeweils in der Fassung des Terrorismusbekämpfungsgesetzes vom 9. Januar 2002, BGBl. I S. 361) sehen derartige Beschränkungen – zu Recht – nicht vor. Sie sind auch verfassungsrechtlich nicht geboten (Urteil des BVerfG vom 12. März 2003, 1 BvR 330/96 und 1 BvR 348/99). Das in § 100h Abs. 2 Satz 1 Halbsatz 1 StPO enthaltene Erhebungsverbot ist in der Praxis schon deshalb nicht handhabbar, weil bei der Erhebung von Verbindungsdaten kaum je entschieden werden kann, ob es um eine Auskunft geht, die von der Klausel „soweit das Zeugnisverweigerungsrecht reicht“ erfasst wird. So kann man den bloßen Verbindungsdaten nicht entnehmen, ob dem Zeugnisverweigerungsberechtigten in dem Ferngespräch, dessen Inhalt ja gerade nicht ermittelt werden darf, etwas „anvertraut“ wird. Es leuchtet im Übrigen nicht ein, wenn das Gesetz bei der

Überwachung des Inhalts der Telekommunikation nach § 100a StPO die Regelung des § 148 StPO für ausreichend ansieht, bei der weniger eingreifenden Auskunft über Telekommunikationsverbindungen aber Erhebungs- und Verwertungsverbote vorsieht, die noch dazu unvertretbar weit sind. So verbietet § 100h Abs. 2 Satz 1 Halbsatz 2 StPO z. B. auch, dass die Auskunft zur Verhütung oder Verfolgung eines Mordes verwendet werden darf. Auch im Übrigen ist die Regelung gerade in der aktuellen Situation, in der es darum geht, effektiv gegen den islamistischen Terror vorzugehen, kontraproduktiv. So ist der Kreis der Personen, denen ein Zeugnisverweigerungsrecht nach § 53 Abs. 1 Satz 1 Nr. 1 StPO zusteht, durchaus streitig. Teilweise wird dabei eine weite Auslegung vertreten (vgl. z. B. Haas, NJW 1990, 3253 m. w. N.), nach der auch islamische Geistliche zum privilegierten Personenkreis gehören können. Es wäre unerträglich, wenn der Kampf gegen den internationalen Terrorismus dadurch behindert würde, dass die Strafverfolgungsbehörden Auskunft über die z. B. mit einem islamistischen Zentrum geführten Ferngespräche gar nicht oder erst nach einer zeitraubenden Diskussion mit dem entsprechenden Telekommunikationsunternehmen erhalten.

Zu Artikel 2 (Änderung des Gesetzes zur Änderung der Strafprozessordnung vom 20. Dezember 2001)

Durch die Artikel 2 und 4 des Gesetzes zur Änderung der Strafprozessordnung vom 20. Dezember 2001 (BGBl. I S. 3879) wird die Geltungsdauer der mit diesem Gesetz eingeführten §§ 100g und 100h StPO bis 31. Dezember 2004 beschränkt. Ein sachlicher Grund für diese zeitliche Eingrenzung besteht nicht. Insbesondere ist schon jetzt absehbar, dass ein Bedürfnis für eine Regelung, wie sie die §§ 100g und 100h StPO enthalten, auch über den 31. Dezember 2004 hinaus fortbesteht. Die Befristung birgt vielmehr die Gefahr in sich, dass bei der Verlängerung der Regelung die Rechte des Bundesrates erneut faktisch ausgehebelt werden, wie dies bereits bei Schaffung der Regelung der Fall war. Sollte es sich in der Zukunft ergeben, dass ein Bedürfnis für eine Änderung von den §§ 100g und 100h StPO besteht, so kann diese jederzeit erfolgen. Einer Befristung der Regelung bedarf es dafür nicht.

Zu Artikel 3 (Einschränkung von Grundrechten)

Die Vorschrift trägt höchst vorsorglich dem Zitiergebot des Artikels 19 Abs. 1 Satz 2 GG Rechnung, da der Entwurf Verfahrensfragen im Zusammenhang mit der Überwachung der Telekommunikation nach §§ 100a ff. StPO regelt.

Zu Artikel 4 (Inkrafttreten)

Die Vorschrift regelt das Inkrafttreten.