

Stellungnahme des VATM

zum Referentenentwurf für ein „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ („Vorratsdatenspeicherung“, Stand 27. November 2006)



Der VATM nimmt die Gelegenheit zur Stellungnahme zu dem Referentenentwurf für ein „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ („Vorratsdatenspeicherung“, Stand 27. November 2006¹), der am 27. November 2006 vom Bundesministerium der Justiz veröffentlicht wurde, im Folgenden gerne wahr.

Vorbemerkung

Hervorzuheben ist zunächst, dass aus Sicht des VATM eine effiziente Strafverfolgung insbesondere vor dem Hintergrund drohender Gefahren durch Terroranschläge unerlässlich ist und die Telekommunikationsbranche bereit ist, auch weiterhin ihren Beitrag zur Prävention und Aufklärung von Straftaten zu leisten. Allerdings müssen damit in Zusammenhang stehende gesetzliche Verpflichtungen den Verhältnismäßigkeitsanforderungen des Grundgesetzes entsprechen. Dies bedeutet, dass die Belastungen, die die Vorratsdatenspeicherung für Bürger und Unternehmen mit sich bringt, auf ein Mindestmaß zu beschränken sind. Der vorliegende Referentenentwurf, mit dem die Richtlinie 2006/24/EG umgesetzt wird, muss sich an diesem Grundsatz messen lassen.

Der VATM hat bereits in der Vergangenheit erhebliche Zweifel an der Verfassungsmäßigkeit der Verpflichtung zur Vorratsdatenspeicherung geäußert. Zwar geht der Referentenentwurf entsprechend des Beschlusses des Bundestages vom 16.02.2006 (BT-Drs. 16/545) nicht über die Mindestanforderungen der Richtlinie hinaus, was der VATM ausdrücklich begrüßt. Gleichwohl können dadurch die Bedenken nicht ausgeräumt werden. Es ist bereits zweifelhaft, ob der mit der Vorratsdatenspeicherung einhergehende Paradigmenwechsel im Datenschutz einer verfassungsmäßigen Prüfung standhält. Mit dem Gesetzentwurf wird das bisher geltende Verbot anlass- und verdachtsunabhängiger Datenspeicherung aufgehoben, die Nutzer von Telekommunikationsdiensten werden unter den vielseitig verwendeten Begriff des „Generalverdachts“ gestellt. Darüber hinaus ist fraglich, ob die im Entwurf vorgesehene Bestimmung der Datenspeicherung „zum Zweck der Strafverfolgung“ in dieser allgemeinen Fassung ausreichend und zulässig ist². Insbesondere vor dem Hintergrund der jüngsten Verfassungsgerichtsrechtsprechung zur präventiven polizeilichen Rasterfahndung (BVerfG-

¹ Im Folgenden „Richtlinie 2006/24/EG“.

² So die Entwurfsbegründung IV Ziffer 5, letzter Absatz (Seite 69).

Stellungnahme des VATM

zum Referentenentwurf für ein „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ („Vorratsdatenspeicherung“, Stand 27. November 2006)



Beschluss vom 04.04.2006 – 1 BvR 518/02) sowie zum Niedersächsischen Polizeigesetz (Urteil vom 27.07.2005 – 1 BvR 668/04) dürfte dies eher zu verneinen sein. Diese Fragen werden im Gesetzgebungsverfahren ausführlich diskutiert werden müssen und möglicherweise letztlich ebenfalls zur Anrufung des Bundesverfassungsgerichts führen.

Daneben begründet die fehlende bzw. unzureichende Entschädigung der betroffenen TK-Unternehmen für die von ihnen durchzuführenden Maßnahmen die Verfassungswidrigkeit ihrer Inanspruchnahme. Für die im Zuge der Vorratsdatenspeicherung entstehenden Belastungen gilt dies noch mehr als für bereits bestehende Überwachungsmaßnahmen, da diese zusätzlichen Tatbestände im ausschließlichen Interesse des Staates liegen. Der Aufwand, der auf die TK-Unternehmen infolge der Verpflichtung zur Vorratsdatenspeicherung zusätzlich zu den bereits bestehenden Belastungen für aktuelle Überwachungsmaßnahmen zukommt, ist immens. Es wird nicht allein ausreichen, mehr Speicherkapazität zur Verfügung zu stellen. Kostenintensiv sind insbesondere die erforderlichen Systemumstellungen bzw. die Anschaffung neuer Systeme sowie im Anschluss der personelle Aufwand, der zur Bearbeitung der Anfragen der Strafverfolgungsbehörden erforderlich wird. Auch die Ankündigung des Bundesjustizministeriums, zeitnah eine entsprechende Entschädigungsregelung zu erarbeiten³, kann erstens aufgrund der zu erwartenden zeitlichen Verzögerung und zweitens aufgrund der Tatsache, dass die Sachverhalte, die im Zusammenhang mit der Vorratsdatenspeicherung zusätzlich entstehen, zunächst ausgeklammert werden sollen, die Verfassungswidrigkeit der Regelungen nicht beseitigen. Zur Wahrung der Verfassungsmäßigkeit des Gesetzes ist vielmehr der zeitgleiche Erlass von Entschädigungsregeln erforderlich.

Die TK-Unternehmen werden davon abgesehen mit einer steigenden Skepsis der Nutzer von Telekommunikationsdiensten zu kämpfen haben. Die Tatsache, dass künftig alle näheren Umstände eines Telekommunikationsvorgangs dokumentierbar werden in Verbindung mit einer generellen Missbrauchsgefahr, wird das Vertrauen der Kunden in die TK-Dienste erheblich reduzieren. Dieser Vertrauensverlust geht zu Lasten der Branche, die noch immer als Wachstumsmotor der Wirtschaft gilt.

³ Vgl. Entwurfsbegründung X Ziffer 3 (Seite 73).

Stellungnahme des VATM

zum Referentenentwurf für ein „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ („Vorratsdatenspeicherung“, Stand 27. November 2006)



Zu den einzelnen Bestimmungen des Entwurfs:

1. Zu Artikel 1 – Änderung der Strafprozessordnung

Zu § 100 b StPO-E – Verfahren für Telekommunikationsüberwachungen

In § 100 b StPO-E werden die Voraussetzungen und das Verfahren für Telekommunikationsüberwachungen geregelt.

In Abs. 1 Satz 3 erfolgt mit der Aufstellung eines Beweisverwertungsverbotes für Daten, die aufgrund einer Eilanordnung der Staatsanwaltschaft erhoben wurden, diese Anordnung jedoch nicht binnen drei Werktagen gerichtlich bestätigt wurde, erfreulicherweise eine eindeutige gesetzliche Regelung der bereits geübten Praxis, die u.a. darin bestand, dass Nachlieferungen von Daten aus unbestätigten Anordnungen nach Ablauf der Bestätigungsfrist nicht erfolgen dürfen. Dies ist zu begrüßen.

Bedauerlicherweise wird in Abs. 2 Satz 1 Nr. 1 die bisherige Pflichtangabe des Namens des Betroffenen unter den Vorbehalt „soweit möglich“ gestellt. Bei der Schwere dieses Eingriffs in die Grundrechte des Betroffenen darf auf die Notwendigkeit einer ausreichenden Identifikation des Betroffenen nicht verzichtet werden. Hierbei ist hervorzuheben, dass nicht nur in die Grundrechte der Betroffenen, sondern darüber hinaus in die unbeteiligter Dritter eingegriffen werden könnte. Die Angabe des Namens muss daher zwingend als Voraussetzung angegeben werden, die Worte „soweit möglich“ sind zu streichen.

Gem. Abs. 2 Satz 2 Nr. 2 muss in der Überwachungsanordnung die Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses angegeben sein. Hier sollte entsprechend der technischen Entwicklung die Kennung als eindeutiger Oberbegriff definiert werden, da bereits heute Anschlüsse (z.B. DSL) ohne Rufnummer bestehen und diese künftig an Bedeutung gewinnen werden. Darüber hinaus ist infolge der getrennten Vermarktung reiner DSL-Anschlüsse und der notwendigen Dienste ohne Anschlüsse auch das alleinige Kriterium der Kennung eines „Anschlusses“ nicht ausreichend. Hier ist zusätzlich der Begriff des zu überwachenden „Dienstes“ aufzunehmen, um eine eindeutige Zuordnung des Überwachungsgegenstandes vornehmen zu können. Ohne das Erfordernis eindeutiger Angaben würde bewusst in Kauf genommen, dass falsche Anschlüsse überwacht werden, was zu Schadensersatzforderungen der Betroffenen führen kann. Auf den Unternehmen jedenfalls

3

Stellungnahme des VATM

zum Referentenentwurf für ein „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ („Vorratsdatenspeicherung“, Stand 27. November 2006)



dürfen derartige Forderungen letztlich nicht lasten, denn der Gesetzgeber ist verpflichtet, durch präzise Formulierungen den Schutz der betroffenen Interessen sicherzustellen.

Hinzuweisen ist ferner auf den Umstand, dass im Mobilfunk der in Abs. 2 Satz 2 Nr. 2 geforderte Nachweis der alleinigen Zuordnung zum zu überwachenden Endgerät letztlich unmöglich sein dürfte. Da die IMEI als Kennung wegen der nach wie vor bestehenden Fälschungsmöglichkeit nicht eindeutig einem Endgerät zugewiesen werden kann, läuft die Vorschrift ins Leere.

Auch in Abs. 2 Satz 2 Nr. 3 sollte statt des Begriffs der „Dauer“ das konkrete Enddatum aufgenommen werden. Die damit einhergehende Rechtsklarheit führt letztlich zu einer gestärkten Rechtssicherheit bei der Umsetzung der Maßnahmen sowohl bei den ermittelnden Behörden als auch bei den verpflichteten Unternehmen.

Aus gleichen Gründen muss hier zusätzlich der „Typ“ der Überwachungsmaßnahme als notwendiges Kriterium angegeben werden, da allein mit der Angabe der „Art“ der Maßnahme nicht klar wird, welche Dienste genau zu überwachen sind (Telefonie und DSL? Nur Telefonie? Nur DSL? Telefonie und E-Mail? Nur E-Mail? DSL und E-Mail oder nur E-Mail?). Diese Konkretisierung ist erforderlich, um sowohl die Rechte der von der Überwachung betroffenen Kunden zu schützen und gleichzeitig den operativen Aufwand bei den Unternehmen und damit den Eingriff in ihre Rechte so gering wie möglich zu halten.

In Abs. 3 wird eine Mitwirkungspflicht der TK-Dienstleister über die Ermöglichung der TK-Überwachung hinaus normiert. Die Pflicht, „die erforderlichen Auskünfte zu erteilen“, führt zu einer Beratungshotline. Die auf diesem Wege abgefragten Informationen müssen auf die Daten beschränkt bleiben, die zur Beschreibung der konkreten Maßnahme erforderlich sind. Weitergehende Informationen, z.B. Erläuterungen zu den Datenformaten, sind den Behörden aus anderen Quellen zugänglich. Eine entsprechende Konkretisierung ist erforderlich.

Die mit den Abs. 5 und 6 definierte Übernahme der Berichtspflichten durch die Länder und den Generalbundesanwalt sowie die anschließende Ergebnisveröffentlichung durch das Bundesamt für Justiz (BfJ) ist sehr zu begrüßen. Allerdings möchten wir dem in der Begründung (Einleitung Ziffer E a.E., Seite 8) entstehenden Eindruck, dass mit dem Wegfall dieser Berichtspflicht auf Seiten der Unternehmen die durch die Vorratsdatenspeicherung entste-

Stellungnahme des VATM

zum Referentenentwurf für ein „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ („Vorratsdatenspeicherung“, Stand 27. November 2006)



henden Belastungen kompensiert würden, entschieden widersprechen⁴. Durch diese Regelung werden die betroffenen Unternehmen zwar entlastet – allerdings nicht in dem Maße, wie die Ausführungen im Referentenentwurf vermuten lassen. Der Aufwand, der infolge der Vorratsdatenspeicherung entsteht, ist im Vergleich zu dem einmal jährlich auszufüllenden Formular bedeutend höher und insofern keinesfalls als Entlastung oder gar Kompensation für die Belastungen, die durch die Verpflichtung zur Vorratsdatenspeicherung entstehen, zu sehen.

Klargestellt werden sollte aus Sicht des VATM auch, dass auch die in den Berichten an das BfJ enthaltenden Daten Bestandteil der Veröffentlichung sein müssen. Dies gilt insbesondere für die Ergebnisbewertung.

Forderungen:

- Streichung der Worte „soweit möglich“ in § 100 b Abs. 2 Satz 2 Nr. 1.
- Streichung der Worte „Rufnummer oder eine andere“ und entsprechende Änderung des § 100 b Abs. 2 Satz 2 Nr. 2: „2. die ~~Rufnummer oder eine andere~~ Kennung des zu überwachenden Anschlusses *oder Dienstes* oder des Endgerätes, wenn diese allein dem zu überwachenden Endgerät zuzuordnen ist“.
- Ersatz des Wortes „Dauer“ durch „Enddatum“ in 100 b Abs. 2 Satz 2 Nr. 3.
- Aufnahme des Kriteriums des „Typs“ der Überwachungsmaßnahme in § 100 b Abs. 2 Nr. 3.
- Konkretisierung der Mitwirkungspflicht der Unternehmen in § 100 b Abs. 3.
- Klarstellung in § 100 Abs. 6, dass auch die in den Berichten an das BfJ enthaltenden Daten, insbesondere die Ergebnisbewertung, Bestandteil der Veröffentlichung sein müssen.

Zu § 100 g StPO-E – Erhebung von Verkehrsdaten

Nach Abs. 1 Nr. 2 wird eine Einschränkung bei der Erhebung von Verkehrsdaten eingefügt, soweit Straftaten betroffen sind, die „mittels Telekommunikation“ begangen werden. Die Maßnahme soll künftig gem. Abs. 1 Satz 2 nur noch zulässig sein, wenn die Erforschung des

⁴ Vgl. bzgl. der angeblichen Entlastung der TK-Unternehmen auch unsere Anmerkungen zu § 100 g a.E. zum Zielsuchlauf.

Stellungnahme des VATM

zum Referentenentwurf für ein „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ („Vorratsdatenspeicherung“, Stand 27. November 2006)



Sachverhaltes oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos wäre und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht.

Dies ist grundsätzlich begrüßenswert, da die Maßnahme generell geeignet ist, um den aktuell vermehrt auftretenden Beschlüssen für minder schwere Straftaten zu entgegen. Allerdings ist aus Sicht des VATM fraglich, ob die Erlaubnisnorm dem Verhältnismäßigkeitsgrundsatz im engeren Sinn entspricht. Sie lässt ihrem Wortlaut gemäß zu, dass schwerwiegende Eingriffe in grundgesetzlich geschützte Rechte auch aufgrund von einzelnen Bagatelldelikten möglich sind (beispielhaft ist ein Online-Auktions-Betrugsfall im Wert von 25 Euro zu nennen). Es wird nicht bezweifelt, dass die o.g. Einschränkung in Abs. 1 Satz 2 des Entwurfs bezweckt, dieses Missverhältnis zu beseitigen (vgl. die Begründung Seiten 113f). Ob die aufgestellten Kriterien aber auch praxistauglich sind, ist zweifelhaft. Offen bleibt z.B. die Frage, wann die Erforschung des Sachverhaltes als aussichtslos betrachtet werden darf? Welche Versuche müssen von wem unternommen werden, bevor die Erhebung von Verkehrsdaten als ultima ratio erfolgen darf? Welche Kriterien sind bei der Beurteilung der Verhältnismäßigkeit heranzuziehen? Welche Folgen hat ein Verstoß gegen diese Verhältnismäßigkeitsprüfung im Einzelfall? Derartige Unklarheiten gehen sowohl zu Lasten der betroffenen Nutzer, die keineswegs sicher sein können, dass ihre Daten nur dann gespeichert werden, wenn dies auch tatsächlich erforderlich ist, als auch zu Lasten der TK-Anbieter, bei denen ein erhöhter operativer Aufwand entstehen wird. Wir regen daher eine entsprechende Überprüfung der Regelung vor dem Hintergrund ihrer Unbestimmtheit an.

Positiv zu bewerten ist die mit Abs. 1 Satz 3 vorgenommene ausdrückliche Beschränkung zur Erhebung aktueller Standortdaten auf Taten nach § 100 a StPO.

Die in der Begründung zu § 100 g Abs. 1 Satz 3 angesprochene Auslegung, über § 100 g StPO-E auch die Echtzeitübermittlung von Verkehrsdaten, also die sog. „kleine TKÜ“ zu realisieren, konterkariert die o.g. Beschränkung allerdings gänzlich.

Es ist unverständlich, warum bei der Echtzeit-Übermittlung der Verkehrsdaten von einer geringeren Eingriffsintensität gegenüber der „Vollüberwachung“ ausgegangen wird und damit die geringeren Eingriffsschranken des § 100 g StPO-E gelten sollen. Der Schutz des Fernmeldegeheimnisses gem. Art. 10 GG und gemäß § 88 Abs. 1 TKG gilt ohne Einschränkung gleichermaßen für Inhalt und für Verkehrsdaten. Nach der Rechtsprechung des Bundesver-

Stellungnahme des VATM

zum Referentenentwurf für ein „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ („Vorratsdatenspeicherung“, Stand 27. November 2006)



fassungsgerichtetes sind neben dem Inhalt der Telekommunikation auch die näheren Umstände des Fernmeldevorgangs vom Schutzbereich des Fernmeldegeheimnisses geschützt. In seiner Entscheidung vom 2. März 2006 (2 BvR 2099/04) stellt das Gericht fest, dass der grundrechtliche Schutz unvollständig wäre, wenn er nicht auch die Verbindungsdaten erfassen würde. Denn diese dokumentieren, ob, wann und wie oft zwischen welchen Personen oder Endeinrichtungen Telekommunikationsverkehr stattgefunden hat oder versucht worden ist. Weiter heißt es, dass Häufigkeit, Dauer und Zeitpunkt von Kommunikationsverbindungen Hinweise auf Art und Intensität von Beziehungen gäben und auf den Inhalt bezogene Schlussfolgerungen ermöglichen.

Diese Vorgaben führen dazu, dass eine Echtzeitüberwachung allenfalls nach §§ 100 a, b StPO erfolgen darf. Das Gesetz muss klarstellen, dass Echtzeitüberwachung auf Basis von § 100 g StPO unzulässig ist. Damit wird auch das Ziel, die Vorgaben des Übereinkommens über Computerkriminalität umzusetzen, nicht gefährdet, da nicht das Ob, sondern lediglich die Voraussetzungen an die Echtzeitüberwachung verfassungskonform ausgestaltet werden. Eine geringere Eingriffsintensität kann höchstens für die zeitlich verzögerte Übermittlung von Verkehrsdaten in der heute praktizierten Form gem. §§ 100g, h StPO angenommen werden.

Hinzu kommt, dass eine Echtzeitüberwachung technisch wie eine TKÜ ausgestaltet werden muss. Die TKÜ- Systeme befinden sich heute bereits im oberen Bereich ihrer Leistungsfähigkeit und müssten auf Grund des zu erwartenden Anfrageaufkommens einschließlich der Netzelemente erheblich ausgebaut werden.

Für die Parameter der sog. Funkzellenabfrage („räumlich und zeitlich hinreichend bestimmte Bezeichnung“) in Abs. 2 fehlen nach wie vor sinnvolle Beschränkungen, die eine handhabbare Umsetzung und damit eine effizientere Ermittlungsarbeit zur Folge hätten. Rein theoretisch kann unter den Begriff der bestimmten Bezeichnung eine Anordnung fallen, die die Abfrage von allen Funkzellen im Bundesgebiet für einen Zeitraum von einem Tag umfasst⁵. Da dies aber praktisch kaum zu bewältigen ist, ist auch der Ermittlungserfolg gefährdet, womit

⁵ Dieses Beispiel ist bewusst überzogen, um die Untauglichkeit der Regelung zu verdeutlichen. Allerdings gibt es tatsächliche Fälle aus der Praxis, die bspw. die Abfrage aller Funkzellen entlang einer bestimmten Bahnstrecke über einen Zeitraum von mehreren Stunden betrafen.

Stellungnahme des VATM

zum Referentenentwurf für ein „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ („Vorratsdatenspeicherung“, Stand 27. November 2006)



wiederum die Geeignetheit der Maßnahme in Frage gestellt ist. Wir regen daher eine Ergänzung der Regelung um einschränkende Konkretisierungsmerkmale an.

Deutlich zu widersprechen ist an dieser Stelle die im Gesetzentwurf (S. 7 unter E – Sonstige Kosten) enthaltene Vermutung, dass die im aktuell geltenden § 100 g Abs. 2 StPO geregelte Zielwahlsuche vermutlich weitgehend entbehrlich werde, weil infolge der Speicherverpflichtungen für Verkehrsdaten auch die Kennung des ankommenden Anrufs erfasst werde. Diese Vermutung, die als Argument für die Entlastung der Unternehmen angeführt wird, geht fehl. Denn die Verpflichtung zur Speicherung der anrufenden Rufnummern besteht nur für den Fall, dass diese Daten auch von den Unternehmen verarbeitet werden⁶. Viele Unternehmen verarbeiten und speichern diese Daten allerdings nicht. Im Fall einer Zielwahlsuche schränkt sich für diese Unternehmen die Menge der zu durchsuchenden Daten folglich nicht ein (infolge einer „Verknüpfung“ mit der gespeicherten anrufenden Nummer), so dass für sie der Aufwand für Zielwahlsuchen vielmehr erheblich höher ist, weil künftig alle über einen Zeitraum von sechs Monaten gespeicherten Datensätze nach den fraglichen Daten durchsucht werden müssen. Gerade weil es Unternehmen gibt, die die anrufende Rufnummer nicht speichern, wird auch das Ermittlungsinstrument „Zielwahlsuche“ keinesfalls entbehrlich werden.

Gem. Abs. 4 ist jährlich eine Übersicht über die Erhebung von Verkehrsdaten zu erstellen. Der Vollständigkeit halber sollte hierbei auch eine Auskunft erfolgen über die Fälle, in denen die Maßnahmen zum Ermittlungserfolg geführt haben.

Forderungen

- Überprüfung und Konkretisierung der Kriterien für die gem. § 100 g Abs. 1 Satz 2 vorgesehene Einzelfallprüfung auf ihre Bestimmtheit.
- Verbot der Echtzeitübermittlung nach § 100 g Abs. 1 Satz 3.
- Erweiterung des § 100 g Abs. 2 um Beschränkungen für eine effizientere Ermittlungsarbeit.
- Aufnahme von § 100 g Abs. 4 Ziffer 6: „6. eine quantitative und qualitative Bewertung über die Wirksamkeit der Maßnahmen“.

⁶ Vgl. die Entwurfsbegründung zu § 100 g Abs. 2, 2. Spiegelpunkt, Seite 116 mit Verweis auf Art. 2, Nummer 5, § 110 a Abs. 2 Nr. 1 TKG-E).

Stellungnahme des VATM

zum Referentenentwurf für ein „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ („Vorratsdatenspeicherung“, Stand 27. November 2006)



Zu § 100 i StPO-E – [IMSI-Catcher]

Es ist nicht nachvollziehbar, warum die in Abs. 5, Sätze 2 und 3 für die Einsatzdauer des IMSI-Catchers festgelegte sehr lange Maximalfrist von sechs Monaten mit einer Verlängerungsoption für weitere sechs Monate bestehen bleiben soll, während in § 100 b Abs. 1 eine Verkürzung auf zwei bzw. einen Monat vorgesehen ist. Im Falle einer langfristigen Observation gem. § 163 f StPO-E sollen sogar nur Fristen von einem Monat zulässig sein. Diese Unterscheidung ist weder sachlich, noch vor dem Hintergrund, dass der Einsatz des IMSI-Catchers zwangsweise auch zur Erhebung von Daten führt, die durch das Fernmeldegeheimnis geschützt sind, gerechtfertigt. Ferner ist zu berücksichtigen, dass der Einsatz von IMSI-Catchern auch zur Observation unbeteiligter Dritter führt und mit dem Einsatz der Geräte eine unvermeidbare Störung des Mobilfunkverkehrs verbunden ist, die seinerseits zu schwerwiegenden Folgen unbeteiligter Dritter führen kann (beispielsweise ist die Notruffunktion beeinträchtigt). Eine Anpassung der unterschiedlichen Überwachungszeiträume ist daher erforderlich.

Ferner muss die in Abs. 6 Satz 1 definierte Mitwirkungspflicht der Unternehmen aus Verhältnismäßigkeitserwägungen unter den Vorbehalt gestellt werden, dass die Daten auch bekannt sind.

Schließlich sollte aufgrund der dargestellten Auswirkungen der eingesetzten Technik auf die Mobilfunknetze auch hier eine Berichtspflicht entsprechend § 100 b Abs. 5 eingefügt werden, um eine Effektivitätskontrolle der Maßnahmen zu gewährleisten. Dies liegt sowohl im Interesse der Strafverfolgungsbehörden als auch der betroffenen Unternehmen, da damit ggf. eine ungerechtfertigte Belastung der betroffenen Netzbetreiber festgestellt werden kann. Eine Regelung sollte als neuer Abs. 7 hinzugefügt werden.

Forderungen:

- Änderung des § 100 i Abs. 5 Sätze 2 und 3: „Die Anordnung ist auf höchstens ~~sechs~~ zwei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als ~~sechs~~ zwei weitere Monate ist zulässig, soweit die in den Absätzen 1 bis 3 bezeichneten Voraussetzungen fortbestehen“.

Stellungnahme des VATM

zum Referentenentwurf für ein „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ („Vorratsdatenspeicherung“, Stand 27. November 2006)



- Ergänzung des § 100 i Abs. 6 Satz 1: „... Kartennummer mitzuteilen, *sofern sie ihm bekannt sind.*“
- Aufnahme einer Berichtspflicht entsprechend § 100 b Abs. 5 in § 100 i Abs. 7 (neu).

Zu § 101 StPO-E – Allgemeine Verfahrensregelungen bei verdeckten Ermittlungsmaßnahmen

In Abs. 4 sind als Beteiligte in den Fällen des Satzes 3 Nr. 3, 6, und 9 auch Personen zu benachrichtigen, die zwar nicht Ziel der ursprünglichen Maßnahme gewesen sind, über die sich jedoch im Rahmen der Maßnahmen Erkenntnisse ergeben haben, die zu weiteren Verfahren abseits vom ursprünglichen Verfahren geführt haben. Um Rechtsklarheit zu schaffen, ist klarzustellen, dass die Ermittlungsbehörden und nicht die TK-Unternehmen zur Benachrichtigung verpflichtet sind.

Forderung:

- Klarstellung in § 101 Abs. 4, dass die Ermittlungsbehörden zur Benachrichtigung verpflichtet sind.

Zu § 110 StPO-E – Durchsicht von Papieren

Das mit Abs. 3 eröffnete unbeschränkte Durchsichts- und Speicherrecht von elektronischen Daten auf räumlich getrennten Speichermedien, für die der Betroffene Zugriffsrechte besitzt, ist zu undifferenziert. Es berücksichtigt nicht in ausreichendem Maß die Fragen nach der Art der Daten und der Zugangsberechtigung, die für die praktische Durchführung erforderlich sind. Eine entsprechende Konkretisierung ist zur Schaffung von Rechtsklarheit notwendig.

Forderung:

- Konkretisierung der Voraussetzungen bzgl. der Art der Daten sowie dem Kriterium der Zugangsberechtigung.

Stellungnahme des VATM

zum Referentenentwurf für ein „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ („Vorratsdatenspeicherung“, Stand 27. November 2006)



2. Zu Artikel 2 – Änderung des Telekommunikationsgesetzes

Zu § 99 TKG-E – Einzelverbindungs nachweis

Wir regen eine Überprüfung der in § 99 enthaltenen Bestimmungen im Hinblick auf die Möglichkeit der Vereinfachung der Datenschutzformulierungen an. Dies gilt insbesondere für die ausufernde Beschreibung der Benachrichtigungspflichten der Empfänger von Einzelverbindungs nachweisen. Die Formulierungen stammen aus Zeiten, in denen ein Telefon kein individuell persönlicher Gegenstand war, in denen kein Anspruch auf einen Einzelgesprächsnachweis bestand und dieser selbstverständlich kostenpflichtig war. Heute existiert für nahezu jeden Anschluss ein solcher Nachweis. Deshalb sollte es anstelle der detaillierten Informationspflichten der Sätze 3 bis 5 des Abs. 1, die im übrigen durch Satz 6 ausgehebelt werden, ausreichen, wenn der Teilnehmer bestätigt, dass er alle aktuellen und künftigen Mitbenutzer über den Einzelverbindungs nachweis informieren wird und bei betrieblich genutzten Anschlüssen die Vertretungen der Mitarbeiter in notwendigem Rahmen beteiligen wird.

Forderung:

- Streichung der Sätze 3 bis 3 des § 99 Abs. 1 und Ergänzung des Satzes 1: „...einen Einzelverbindungs nachweis verlangt *und bestätigt* hat, *alle aktuellen und künftigen Mitbenutzer über den Einzelverbindungs nachweis zu informieren.*“

Zu § 110 TKG-E – Technische Umsetzung von Überwachungsmaßnahmen

Dass die derzeitige Berichtspflicht der TK-Unternehmen gem. Abs. 8 der geltenden Fassung infolge der neu aufgenommenen Pflichten des BfJ gem. § 163 Abs. 5 und 6 StPO entfallen, ist sehr zu begrüßen. Im Vergleich zu den Belastungen, die infolge der Vorratsdatenspeicherung für die Unternehmen entstehen, fällt dies aber kaum ins Gewicht⁷.

⁷ Vgl. unsere oben stehenden Ausführungen zu § 100 b Abs. 5 und 6 StPO.

Stellungnahme des VATM

zum Referentenentwurf für ein „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ („Vorratsdatenspeicherung“, Stand 27. November 2006)



Zu § 110 a TKG-E – Speicherungspflichten für Verkehrsdaten

Gem. Abs. 1 Satz 1 erfolgt die Speicherung der Verkehrsdaten „zum Zwecke der Strafverfolgung“. Ob diese sehr allgemein gefasste Zweckvorgabe mit den grundgesetzlichen Voraussetzungen vereinbar ist, ist nach Auffassung des VATM zweifelhaft⁸.

Ferner weisen wir auf einen aus unserer Sicht bestehenden Widerspruch bzgl. der Beschränkung des Adressatenkreises hin: Die Begründung stellt klar, dass gem. Abs. 1 Satz 1 keine Speicherpflicht für den nicht-öffentlichen Bereich besteht. Beispielhaft werden hier E-Mail-Server von Universitäten genannt. Vor dem Hintergrund, dass die sog. „Schläfer“ der Terroranschläge vom 11. September 2001 als Studenten an Universitäten eingeschrieben waren und die Vorratsdatenspeicherung in erster Linie mit der Terrorismusbekämpfung begründet wird, ist diese Einschränkung fragwürdig.

Im Hinblick auf den Umfang der Speicherverpflichtung sollte aus Sicht des VATM grundsätzlich eine Ausnahme für Verkehrsdaten von massenhaft und unverlangt zugesandten E-Mails (SPAM) gelten. Denn dies würde zu einer enormen Mehrbelastung der Verpflichteten führen und die Effektivität der Arbeit der Strafverfolgungsbehörden infolge der enormen Datenmengen wesentlich erschweren. Eine entsprechende Klarstellung wäre wünschenswert.

Die ebenfalls in Abs. 1 Satz 1 festgelegte Speicherfrist von sechs Monaten entspricht der in der Richtlinie 2006/24/EG vorgegebenen Mindestspeicherfrist. Unter Aufrechterhaltung seiner oben genannten verfassungsrechtlichen Zweifel an der generellen Zulässigkeit der Vorratsdatenspeicherung begrüßt der VATM, dass der Referentenentwurf nicht über die europäischen Mindestvorgaben hinausgeht und damit den Beschluss des Deutschen Bundestages vom 16.02.2006 (BT-Drs. 16/545) umsetzt.

Abs. 1 Satz 1 regelt, dass die Verkehrsdaten im Inland zu speichern sind. Diese Beschränkung ist nicht nachvollziehbar, da es für die Verpflichtung zur Herausgabe der Daten sachlich nicht darauf ankommt, ob die Daten im In- oder Ausland gespeichert werden. Hierfür ist allein maßgeblich, dass der Verpflichtete auf sie zugreifen kann. Mit dieser Vorgabe wird massiv in die (Netz-) Planungsfreiheit der TK-Anbieter eingegriffen. Dies gilt in besonderem Maße für europäisch oder international ausgerichtete Unternehmen. Derartige Eingriffe in die wirtschaftlichen Belange der Verpflichteten dürften einen Eingriff in die von Art. 12 GG ge-

⁸ Vgl. unsere Anmerkung in der Vorbemerkung.

Stellungnahme des VATM

zum Referentenentwurf für ein „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ („Vorratsdatenspeicherung“, Stand 27. November 2006)



schützte Berufsausübungsfreiheit darstellen. Die Festlegung widerspricht zudem dem Geist des EU-Binnenmarktes, der ja gerade auf eine Öffnung der ehemals nationalen Märkte abzielt. Es ist geradezu widersinnig, wenn ein nationales Gesetz, das eine Europäische (!) Richtlinie umsetzen soll, Regelungen festschreibt, die dem europäischen Gedanken offensichtlich entgegenlaufen. Da für diese Beschränkung auf das Inland keine Rechtfertigung ersichtlich ist, ist sie zu streichen.

Gem. Abs. 1 Satz 2 sind TK-Diensteanbieter, die keine eigene TK-Anlage betreiben, verpflichtet sicherzustellen, dass die ihre Dienste betreffenden Verkehrsdaten gespeichert werden. Dies soll gegenüber der Bundesnetzagentur nachgewiesen werden. Abgesehen davon, dass offen bleibt, wie der Nachweis erfolgen soll, dürfte diese Verpflichtung unnötige Bürokratie darstellen. Der mit der Regelung beabsichtigte Zweck ist die Speicherung der Verbindungsdaten, die für einen bestimmten Teilnehmer anfallen. Wegen der nach der EU-Richtlinie 2006/24/EG geltenden Maßgabe, dass eine Doppelspeicherung möglichst vermieden werden soll⁹, ist hier von der Sicherstellung einer *einmaligen* Speicherung auszugehen. Damit ist der Fall, dass ein Anbieter ohne eigene TK-Anlage solche Daten, die er zum jetzigen Zeitpunkt nicht speichert, künftig selbst speichern soll, ausgeschlossen. Dieser hat vielmehr gem. § 110 a Abs. 1 Satz 2, 1. Halbsatz sicherzustellen, dass die Verkehrsdaten seiner Kunden bei dem TK-Anbieter, über dessen TK-Anlage er seine Angebote realisiert, gespeichert werden. Der Zweck der Regelung ist mit dieser Speicherung erfüllt. Eine zusätzliche Nachweispflicht gegenüber der BNetzA bewirkt keinen Mehrwert in Bezug auf die Zweckerfüllung. In der Praxis wird eine derartige Auftragsdatenverarbeitung vertraglich und entsprechend der Vorgaben des BDSG schriftlich fixiert, was im Übrigen bereits im ureigensten Interesse sowohl des Anbieters ohne als auch des Anbieters mit eigener TK-Anlage liegt. Der mit einer Nachweispflicht einher gehende Aufwand sowohl bei den Anbietern als auch bei der Bundesnetzagentur ist folglich nicht gerechtfertigt. Die Nachweispflicht muss daher als unnötige weitere Belastung entfallen.

Die in Abs. 2 definierten Daten des Telefondienstes sind zum Teil nur mit erheblichem Aufwand oder gar nicht erfassbar. Vorab ist in Bezug auf die in Abs. 2 aufgeführten Daten hervorzuheben, dass ausweislich der EU-Richtlinie 2006/24/EG und dessen Erwägungsgrund

⁹ Vgl. Erwägungsgrund 13 Satz 2.

Stellungnahme des VATM

zum Referentenentwurf für ein „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ („Vorratsdatenspeicherung“, Stand 27. November 2006)



23 zur Wahrung der Verhältnismäßigkeit Anbieter elektronischer Kommunikationsdienste „nur solche Daten auf Vorrat speichern müssen, die im Zuge der Bereitstellung ihrer Kommunikationsdienste erzeugt oder verarbeitet werden. Soweit derartige Daten nicht von diesen Anbietern erzeugt oder verarbeitet werden, besteht auch keine Pflicht zur Vorratsdatenspeicherung.“ In der Begründung des Referentenentwurfs zu § 110 a Abs. 1 wird dies auch als „vor die Klammer gezogene“ Maßnahme dargestellt, was bei der Ausgestaltung des Abs. 2, der die konkreten Datenarten aufzählt, zu berücksichtigen ist. Leider sind die Formulierungen in Abs. 2 aber oft missverständlich, so dass stellenweise sogar ein Widerspruch zwischen Gesetzestext und der Vorgabe der Richtlinie bzw. der Begründung besteht. Da es sich bei der Festlegung der konkret vorzuhaltenden Daten aber um den Kern der Verpflichtung zur Vorratsdatenspeicherung handelt, dürfen derartige Unklarheiten nicht bestehen bleiben. Sie gingen andernfalls zu Lasten der Nutzer von Kommunikationsdiensten und zu Lasten der betroffenen TK-Unternehmen. Entsprechende Klarstellungen seitens des Gesetzgebers sind daher zur Vermeidung dieser Folgen unbedingt vorzunehmen.

Im Einzelnen:

Zunächst ist darauf hinzuweisen, dass die Umsetzung der Verpflichtung zur Vorhaltung der A- und B-Rufnummer sowie der Ziel-Rufnummern bei Um- und Weiterschaltungen gem. Abs. 2 Nr. 1 Änderungen auch in den Netzelementen erfordert und daher zu einer enormen Ausweitung der zu speichernden Datenmengen führt. Damit einher geht ein erheblicher Aufwand bei den Verpflichteten. Bezüglich des Umfangs der Verpflichtung ist eine Klarstellung im Gesetzeswortlaut erforderlich, aus der hervorgeht, dass die Speicherpflicht unter dem Vorbehalt der Verfügbarkeit der Daten auf Seiten des Verpflichteten steht. Bei netzübergreifenden Gesprächen beispielsweise sind die erforderlichen Daten nicht vollständig vorhanden, so dass sich die Herausgabepflicht auch nur auf die tatsächlich vorhandenen Daten, über die der Verpflichtete auch eine Verfügungsmöglichkeit hat, beziehen kann. Keinesfalls kann die Verpflichtung bedeuten, dass die TK-Anbieter verpflichtet werden, Daten, über die sie selbst nicht verfügen, zusammenzuführen. Zur Vermeidung späterer Rechtsunsicherheit muss dies direkt aus dem Gesetzeswortlaut hervorgehen¹⁰.

¹⁰ Vgl. oben, Vorbemerkung zu § 110 a, Abs. 2.

Stellungnahme des VATM

zum Referentenentwurf für ein „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ („Vorratsdatenspeicherung“, Stand 27. November 2006)



Gem. Abs. 2 Nr. 3 sind in Fällen, in denen im Rahmen des Telefondienstes unterschiedliche Übermittlungsdienste genutzt werden können, Angaben zu dem jeweils genutzten Dienst zu machen. Entsprechend der eingangs erwähnten Maßgabe ist dies so auszulegen, dass hierunter nur die Datendienste sowie die Dienstmerkmale zu verstehen sind, die technisch auch tatsächlich signalisiert werden. Dass hier teilweise Unschärfen zu erwarten sind, weil aus diesen Angaben nicht immer eindeutig hervorgeht, ob es sich beispielsweise um ein Fax oder einen Datendienst handelt, kann nicht zu Lasten der Verpflichteten gehen. Keinesfalls darf aus diesem Umstand eine zusätzliche Speicherverpflichtung geschlussfolgert werden, da diese gem. Erwägungsgrund 23 der EU-Richtlinie 2006/24/EG unverhältnismäßig wäre.

In Abs. 2 Nr. 4 lit. a und b werden spezifische Mobilfunkdaten von der Speicherpflicht erfasst. Es sollen die IMSI und IMEI-Nummern sowohl des A- als auch des B-Teilnehmers vorgehalten werden. Auch hier ist eine Änderung in den Netzelementen erforderlich, was ebenfalls zu einer erheblichen Ausweitung des Datenvolumens und entsprechenden Belastungen bei den TK-Unternehmen führt. Abgesehen davon sind die geforderten Daten bei netzübergreifenden Gesprächen auch hier nicht vollständig vorhanden. Es ist daher ebenfalls eine wie bereits zu Abs. 2 Nr. 1 geforderte Klarstellung im Gesetzestext erforderlich, um Unklarheiten bei der Anwendung des Gesetzes zu vermeiden.

Gleiches gilt für die in Abs. 2 Nr. 4 lit. c geforderte Angabe zur Speicherung der Standortdaten von A- und B-Teilnehmer. Auch hier wird ein erheblicher Anstieg der zu speichernden Datenmengen zu verzeichnen sein. Die geforderten Daten sind selbst bei Gesprächen innerhalb eines Netzes nur bei der Weiterleitung innerhalb einer Vermittlungsstation vorhanden. Ob mit diesen „lückenhaften“ Daten überhaupt der angestrebte Ermittlungserfolg erreicht werden kann, dürfte fraglich sein, was die Verhältnismäßigkeit der Verpflichtung insgesamt in Frage stellt. Die bereits geforderte Klarstellung, dass nur die tatsächlich in den Systemen vorhandenen Daten vorzuhalten sind, muss aber in jedem Fall auch Abs. 2 Nr. 4 lit. c umfassen.

Die gem. Abs. 2 Nr. 4 lit. d vorzuhaltenden Daten bei Prepaid-Diensten (Datum, Uhrzeit und Standort bei erster Aktivierung) sind in dieser Verknüpfung bei den Netzbetreibern nicht vorhanden. Die Aktivierung des Dienstes erfolgt im sog. Home Location Register (HLR) im Mobilfunknetz. Bei dieser Aktivierung wird lediglich der zeitlich erste Call in Form seiner Verkehrsdaten dokumentiert. Ein über die zeitliche Angabe hinausgehendes Datum wird hinge-

Stellungnahme des VATM

zum Referentenentwurf für ein „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ („Vorratsdatenspeicherung“, Stand 27. November 2006)



gen nicht erhoben, so dass nicht bekannt ist, wo sich die SIM oder der Kunde zu diesem Zeitpunkt befinden. Insofern wird der Standort zum Zeitpunkt der Aktivierung, wie im Gesetzentwurf gefordert ist, derzeit nicht erhoben. Auch hier muss daher eine Beschränkung im Gesetzestext auf tatsächlich vorhandene Daten erfolgen, Abs. 2 Nr. 4 lit. d ist zu streichen.

Hinzuweisen ist auf den Umstand, dass die in Abs. 3 Nr. 1 geforderte Speicherung der Benutzerkennung des Absenders je nach Dienstangebot nicht immer gespeichert wird (z. B. E-Mail-Dienste ohne Authentifizierung). Nach Maßgabe der oben genannten Auslegung zu Abs. 2 sind auch hier nur die tatsächlich vorhandenen Daten vorzuhalten.

Die in den Abs. 3 und 4 enthaltene Verpflichtung zur Speicherung der IP-Adressen erweist sich im Mobilfunk als nahezu unmöglich. Aufgrund des knappen IP-Adressraumes kann die Zuordnung der Zugangsdaten nur temporär und zum Teil nur bezogen auf einen Request erfolgen. Die Differenzierung der wenigen zuordnenbaren Adressen zwischen den Nutzern erfolgt oftmals nur auf Basis zusätzlicher Angaben des Ports am Gateway. Dieses Datum wird in der Regel im Internet nicht mitgeschrieben. Hier muss daher ebenfalls eine Klarstellung auf tatsächlich vorgehaltene Daten erfolgen.

Gem. Abs. 3 Nr. 3 ist der Beginn und das Ende der Nutzung eines Dienstes zu speichern. Die Formulierung birgt Unklarheiten in sich, da nicht abgrenzbar ist, was genau unter dem Begriff des „Dienstes“ zu verstehen ist. Für den Anbieter eines Internetportals beispielsweise, der auf diesem Portal unter anderem einen E-Mail-Dienst anbietet, stellt sich die Frage, ob die Anmeldung und Authentifizierung in das Portal oder das Angebot, E-Mails empfangen und verschicken zu können, als Dienst im Sinne der Vorschrift gilt. Tatsächlich wird in diesem Fall eine IP-Adresse lediglich beim Log-In/bei der Authentifizierung in das Portal erhoben. Entscheidet sich der Nutzer im Anschluss daran, den E-Mail-Dienst zu nutzen, so erfolgt mangels erneuter Authentifizierung keine weitere Zuweisung einer IP-Adresse. Ein entsprechendes Datum, das den Beginn der Nutzung des E-Mail-Dienstes im engen Sinn dokumentiert, kann also nicht gespeichert werden.

Ähnlich gelagert ist die Problematik bei Unternehmen, deren Geschäftsmodell im gleichzeitigen Angebot von E-Mail-Diensten gem. Abs. 3 und Internetzugangsdiensten gem. Abs. 4 besteht. Hier sollte möglichst im Gesetzestext klargestellt werden, dass die geforderten Daten nur einmal zu speichern sind. Andernfalls liefe der Grundsatz der Richtlinie 2006/24/EG der Vermeidung von Doppel- oder Mehrfachspeicherung ins Leere.

Stellungnahme des VATM

zum Referentenentwurf für ein „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ („Vorratsdatenspeicherung“, Stand 27. November 2006)



Nach dem Verständnis des VATM muss für die genannten Beispielfälle folgendes gelten: Da das maßgebliche, in Abs. 3 Nr. 3 zu speichernde Datum die IP-Adresse ist, kann es im Fall des Internet-Portal-Anbieters nur auf den Zeitpunkt der ersten Zuweisung einer IP-Adresse ankommen. „Dienst“ im Sinne des Gesetzes wäre damit „die Anmeldung im Rahmen des Portals“. Dies ist bereits mit dem Log-In in das Portal erfüllt. Auf die tatsächliche Nutzung des E-Mail-Dienstes kommt es folglich nicht an, da dies eine Erhebung und Speicherung zusätzlicher, derzeit nicht vorhandener Daten bedeuten würde. Zu erheben und zu speichern ist nach dieser Auslegung somit nur die IP-Adresse beim Log-In in das Portal. Wir bitten um Prüfung dieser Auslegung und Klarstellung seitens des Gesetzgebers.

Im Fall des gleichzeitigen Angebots von Internetzugangs- und E-Mail-Dienst muss in Erfüllung des Gebotes der Vermeidung doppelter Datenerhebung eine Erhebung gem. Abs. 3 Nr. 3 (Log-In für E-Mail-Dienst) unter dem Vorbehalt stehen, dass keine Erhebung gem. Abs. 4 Nr. 3 (Log-In für Internetzugangs-Dienst) vorangegangen ist.

Forderungen:

- Klarstellung, dass sich die Speicherverpflichtung des § 110 a Abs. 1 nicht auf die Verkehrsdaten bezieht, die infolge von SPAM-Nachrichten anfallen.
- Streichung der Worte „im Inland“ in § 110 a Abs. 1 Satz 1.
- Streichung des § 110 a Abs. 1 Satz 2 letzter Halbsatz („~~und dies der Bundesnetzagentur gegenüber nachzuweisen~~“)..
- Klarstellung im Gesetzestext (in § 110 a Abs. 1 Satz 1 oder in Abs. 2), dass nur die Daten von der Speicherungspflicht erfasst sind, über die der Verpflichtete auch tatsächlich in seinen Systemen verfügt und keine Verpflichtung zur Speicherung zusätzlicher Daten begründet wird. (gilt für die Bestimmungen in § 110 a Abs. 2 Nr. 1, Nr. 3 und Nr. 4 lit. a, b und c, Abs. 3 und 4).
- Streichen des § 110 a Abs. 2 lit. d.
- Überprüfung der Auslegung des Begriffs der „Nutzung eines Dienstes“ in § 110 a Abs. 3 Nr. 3 und der konkreten Speicherverpflichtung im Fall eines Plattformbetreibers, der auch E-Mail-Dienste anbietet.

Stellungnahme des VATM

zum Referentenentwurf für ein „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ („Vorratsdatenspeicherung“, Stand 27. November 2006)



- Ergänzung des § 110 a Abs. 3 Nr. 3: „3. den Beginn und das Ende der Nutzung des Dienstes unter der zugewiesenen Internetprotokoll-Adresse nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone, *soweit der Verpflichtete die Erhebung nicht bereits aufgrund seiner Verpflichtung gem. Abs. 4 Nr. 3 durchgeführt hat.*

Zu § 110 b TKG-E – Verwendung der nach § 110 a gespeicherten Daten

Nach Abs. 1 Satz 1 hat der Verpflichtete die nach § 110 a gespeicherten Verkehrsdaten den berechtigten Stellen für die Verfolgung von Straftaten zu übermitteln. Angesichts der Sensibilität der betroffenen Daten und der damit tangierten Grundrechte der Betroffenen (Nutzer) ist auch bei der Umschreibung der Datenverwendung jede Ungenauigkeit in der Gesetzesformulierung zu vermeiden, die bei der späteren Anwendung der Vorschriften zu Auslegungsschwierigkeiten und Rechtsunsicherheit führen könnte. Aus Sicht des VATM sind aus diesen Gründen zwei Konkretisierungen in Abs. 1 Satz 1 erforderlich.

Es ist zunächst klarzustellen, dass mit „zuständiger Stelle“ im Sinne des Gesetzes ausschließlich öffentliche, zur Strafverfolgung berechnete Stellen gemeint sind. Darüber hinaus muss die Verwendung der gem. § 110 a gespeicherten Daten ausschließlich auf die Verfolgung von Katalogstraftaten gem. § 100 a StPO beschränkt sein. Anderes darf aus Verhältnismäßigkeitserwägungen nicht gelten. Die Rechtmäßigkeit der Vorratsdatenspeicherung an sich und die Zulässigkeit des mit ihr einhergehenden Paradigmenwechsels im Datenschutz sind ohnehin zweifelhaft. Um die Anforderungen, die das Bundesverfassungsgericht an den Schutz von Daten aufgestellt hat, nicht gänzlich zu verwässern, sind als Mindestvoraussetzungen eine eindeutige Zweckbindung sowie die genaue Bezeichnung der zur Datenverwendung Berechtigten zu fordern. Es ist erneut darauf hinzuweisen, dass auf Grund der Tatsache, dass die Vorratsdatenspeicherung anlass- und verdachtsunabhängig erfolgt, die Gefahr der Grundrechtsverletzung Unbeteiligter besonders erhöht ist. Dies bedeutet im Umkehrschluss, dass die Anforderungen an den Schutz der Daten besonders hoch sein müssen. Ohne die genannten Konkretisierungen im Gesetzestext droht die Gefahr, dass die Datenherausgabe an Private auch zur Verfolgung von Straftaten, die nicht als „schwere“ Katalogstraftat einzustufen sind, verlangt wird. Konkret ist an Herausgabeverlangen nach dem Urhebergesetz zu denken, die aber aus Verhältnismäßigkeitserwägungen keinesfalls in Betracht kommen können. Denn ein derart schwerer Eingriff in Grundrechte bedarf einer be-

Stellungnahme des VATM

zum Referentenentwurf für ein „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ („Vorratsdatenspeicherung“, Stand 27. November 2006)



sonderen Rechtfertigung, die im Fall der Vorratsdatenspeicherung mit der Schwere der zu verfolgenden Straftaten begründet wird. Zu erinnern ist an dieser Stelle daran, dass Anlass für die Einführung der Vorratsdatenspeicherung die Terrorbekämpfung war, was zur Folge hat, dass es sich bei den zu verfolgenden Straftaten um ähnlich schwere Straftaten handeln muss. Um von vornherein Rechtsstreitigkeiten zu vermeiden, ist daher eine Klarstellung im Gesetzestext vorzunehmen. Die vermeidbare Rechtsunklarheit würde vermutlich auf dem Rücken der TK-Anbieter ausgetragen werden, denn es ist zu erwarten, dass die Anzahl entsprechender Auskunftsverlangen sehr ansteigen würde. Die Unternehmen würden die Herausgabe der Daten an Private aus oben genannten Gründen verweigern und müssten entsprechende Rechtsmittel dagegen abwehren.

In der Begründung zu Abs. 1 Satz 1 wird ausgeführt, dass sich die TK-Diensteanbieter zu vergewissern haben, ob es sich bei dem die Übermittlung Verlangenden um eine für die Strafverfolgung zuständige Stelle handelt, die zur Ausübung des Übermittlungsverlangens legitimiert ist. Wie dies in der Praxis ausgestaltet werden soll, insbesondere welche Kriterien hier gelten sollen, bleibt unklar. An dieser Stelle ist – angesichts der Sensibilität der Daten und der damit möglichen erheblichen Eingriffe in Grundrechte – unbedingt zu präzisieren. Hervorzuheben ist, dass das Vertrags- und Vertrauensverhältnis zwischen Anbieter und Kunden tangiert ist, das keinesfalls leichtfertig gefährdet werden darf, indem unklare Verpflichtungen seitens des Gesetzgebers auferlegt werden.

Im Zusammenhang mit Abs. 1 Satz 3, der das Verbot enthält, die gespeicherten Daten an andere als die berechtigten Stellen zu übermitteln, ist auf die faktisch bestehende Fälschungsmöglichkeit der Auskunftsverlangen hinzuweisen. Aus Satz 3 darf keine Verpflichtung zur Echtheits- oder Rechtmäßigkeitsprüfung seitens der TK-Anbieter erwachsen. Dies fällt weder in den Aufgabenbereich der Verpflichteten noch wäre der damit verbundene Aufwand zu rechtfertigen. Insbesondere wegen der zu erwartenden Masse der Anfragen darf die Gefahr verfälschter Anordnungen nicht zu Lasten der Verpflichteten gehen. Dies ist bei der Beurteilung der Fahrlässigkeit gem. § 149 Abs. 1 Ziffer 28 d TKG zu berücksichtigen. Eine Klarstellung seitens des Gesetzgebers, beispielsweise eine Beschränkung auf grobe Fahrlässigkeit, wäre wünschenswert.

Nach Abs. 1 Satz 4 dürfen die zur Vorratsdatenspeicherung Verpflichteten die Daten ausschließlich für Zwecke der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung

Stellungnahme des VATM

zum Referentenentwurf für ein „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ („Vorratsdatenspeicherung“, Stand 27. November 2006)



eines ordnungsgemäßen Betriebes der Datenverarbeitungsanlage verwenden. Diese Beschränkung ist – wie auch in der Begründung festgestellt wird – keine zwingende europarechtliche Vorgabe. Art. 11 der Richtlinie 2006/24/EG in Verbindung mit Art. 15 Abs. 1 der Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG) sieht vielmehr vor, dass die Richtlinie insoweit keine abschließende Regelung trifft. Es ist zu vermuten, dass andere EU-Mitgliedstaaten liberalere Regelungen erlassen werden, was eine Wettbewerbsverzerrung zu Lasten der Bundesrepublik Deutschland und den hier ansässigen Unternehmen zur Folge haben kann. Um diese Konsequenz zu vermeiden, sollte eine absolute Beschränkung in Bezug auf die eigene Nutzung durch den Verpflichteten unterbleiben. Vielmehr sollte die Nutzung entsprechend der datenschutzrechtlichen Regelungen gewährt werden. Insbesondere sollte kein weiteres Hindernis für die Verpflichteten geschaffen werden, indem unterschiedliche Nutzungsmöglichkeiten für die Daten, die für Abrechnungszwecke gespeichert werden dürfen und denen, die aufgrund der Verpflichtung zur Vorratsdatenspeicherung vorgehalten werden, aufgestellt werden. Dies bedeutete einen zusätzlichen operativen Aufwand, obwohl die Daten den gleichen Sorgfaltsanforderungen unterliegen und damit ein sachlicher Grund für die Ungleichbehandlung nicht ersichtlich ist. Die in Satz 4 enthaltene Zweckbindung ist von dem Gedanken getragen, den Verpflichteten eine Nutzung der Daten für eigene Zwecke zu ermöglichen, soweit Datenschutzbelange sicherzustellen sind oder die Funktionsfähigkeit der Datenverarbeitungsanlage betroffen ist, da andernfalls die Speicherung der Daten und damit das Ziel des Gesetzentwurfs gefährdet wäre. Um letztgenannten Aspekt erfüllen zu können, sollte nicht allein die Funktionsfähigkeit der Datenverarbeitungsanlage, sondern ganz allgemein der Betrieb der Anlage des Anbieters maßgeblich sein. Denn auch ein Systemfehler jenseits der Datenverarbeitungsanlage kann die Speicherung gefährden. Die Beschränkung auf die „Datenverarbeitungsanlage“ sollte entfallen.

Das in Abs. 2 angegebene Zeitintervall ist im Sinne der Begründung ausdrücklich zu begrüßen. Es soll damit zusätzlicher Aufwand bei den Verpflichteten, der bei einer tagesgenauen Vorgabe entstünde, vermieden werden. Für die derzeit identischen Lösungsfristen für Verkehrsdaten nach § 97 Abs. 3 (die für die Abrechnung benötigten Daten dürfen höchstens sechs Monate gespeichert werden) und nach § 110 b Abs. 2 besteht die Gefahr, dass sie durch unterschiedliche Interpretationen auseinanderdriften. Dies würde zu zusätzlichen Aufwänden bei den Speicher-, Back-Up- und (zeitversetzten) Löschroutinen führen, was in der

20

Stellungnahme des VATM

zum Referentenentwurf für ein „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ („Vorratsdatenspeicherung“, Stand 27. November 2006)



Praxis erheblichen Aufwand bedeutet. Um dies zu vermeiden, schlagen wir eine Formulierung vor, die beide Vorschriften miteinander verbindet.

Gem. der Begründung soll Abs. 3 sicherstellen, dass auf die gespeicherten Verkehrsdaten ausschließlich Personal zugreifen kann, das hierzu besonders ermächtigt ist. Die Verkehrsdaten werden aber bereits durch das Datengeheimnis gem. § 5 BDSG und das Fernmeldegeheimnis gem. § 88 TKG geschützt. Ferner ist jeder Diensteanbieter gem. § 9 BDSG verpflichtet, technische und organisatorische Maßnahmen vorzuhalten, die den Schutz der personenbezogenen Daten sicherstellen müssen. Die näheren Ausgestaltungen sind in der Anlage zu § 9 BDSG beschrieben. Der Schutz der nach § 110 b vorzuhaltenden Daten ist damit bereits durch die heute bestehenden Regelungen ausreichend gewährleistet.

Der Begriff „besonders ermächtigte Personen“ ist im TKG ferner nicht näher beschrieben. Eine besondere Ermächtigung ist aus unserer Sicht schon deshalb abzulehnen, da in § 110 b Abs. 3 keine ausreichende Abgrenzung zu den nach §§ 97 und 99 bis 101 TKG gespeicherten Verkehrsdaten erfolgt. Nach dem Wortlaut des § 110 b Abs. 3 Satz 2 müssten alle Personen, die die Verkehrsdaten zu den im TKG genannten Zwecken erheben und nutzen, besonders ermächtigt werden. Sofern die Verkehrsdaten in Form einer Auftragsdatenverarbeitung gem. § 11 BDSG durch ein anderes Unternehmen verarbeitet werden (z.B. Rechnungsversand) wären auch diese Unternehmen betroffen. Eine besondere Ermächtigung ist nicht praktikabel und auch nicht erforderlich, da kein Grund ersichtlich ist, warum die nach § 110 b zu speichernden Daten ein anderes Schutzbedürfnis haben sollten als die nach § 97. Abs. 3 Satz 2 ist daher entsprechend anzupassen.

Forderungen:

- Präzisierung des § 110 b Abs. 1 Satz 1: „Für die Verfolgung von Straftaten *nach § 100 a StPO* hat der nach § 110 a Verpflichtete die gespeicherten Daten den zuständigen *zur Strafverfolgung berechtigten öffentlichen* Stellen auf deren Anordnung unverzüglich zu vermitteln.
- Konkretisierung der Überprüfungspflichten gem. § 110 b Abs. 1 Satz 1 bzgl. der Berechtigung der nachfragenden Stelle, um eine praktische Anwendung sicherzustellen.
- Klarstellung bzgl. § 110 b Abs. 1 Satz 3, dass die Verpflichteten nicht zur Rechtmäßigkeits- oder Echtheitsprüfung der Anordnungen verpflichtet sind.

Stellungnahme des VATM

zum Referentenentwurf für ein „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ („Vorratsdatenspeicherung“, Stand 27. November 2006)



- Streichung der Worte „der Datenverarbeitungsanlage“ in § 110 b Abs. 1 Satz 4.
- Änderung des § 110 b Abs. 2: „Der nach § 110 a Verpflichtete hat die gespeicherten Daten ~~innerhalb eines Monats nach Ablauf der in § 110 a Abs. 1 genannten Frist~~ frühestens nach sechs Monaten und spätestens nach den in § 97 Abs. 3 Satz 2, 2. Halbsatz genannten Fristen zu löschen.“
- Änderung des § 110 b Abs. 3 Satz 2: „Er hat ~~durch die~~ technischen und organisatorischen Maßnahmen gem. § 9 BDSG und dessen Anlage sicherzustellen. ~~dass der Zugang zu den gespeicherten Daten ausschließlich hierzu besonders ermächtigten Personen möglich ist.~~“

Zu § 111 TKG-E – Daten für Auskunftersuchen der Sicherheitsbehörden

§ 111 soll nach den Ausführungen der Begründung sicherstellen, dass die im Bereich der Mobilfunktelefonie tätigen Diensteanbieter künftig auch die Gerätenummern der vertriebenen Mobilfunkgeräte (IMEI) erfassen und speichern, damit die berechtigten Stellen darüber verfügen können. Im Hinblick auf die in Abs. 1 Satz 1 Nr. 5 enthaltene Verpflichtung zur Speicherung der IMEI ist in Entsprechung der obigen Ausführungen zu § 110 a TKG festzustellen, dass sich diese Verpflichtung nur auf solche Daten bezieht, die auch tatsächlich von den Verpflichteten erzeugt oder verarbeitet werden. Eine Erfassung der IMEI-Nummer ist heute nur bei bestimmten Vertriebswegen und Produktarten möglich und vorgesehen. Eine flächendeckende Erfassung würde einen erheblichen Mehraufwand von der Produktkonfektionierung (insbesondere bei Prepaid-Produkten) bis zur Auftragserfassung bedeuten. Eine derartige zusätzliche Speicherpflicht wäre in Bezug auf Bestandsdaten unverhältnismäßig, vgl. Erwägungsgrund 23 der Richtlinien 2006/24/EU, der insoweit keine Beschränkung auf Verbindungsdaten enthält. Eine entsprechende Klarstellung im Gesetzestext ist aus Gründen der Rechtsklarheit geboten.

Abgesehen davon führt die Ausgestaltung des Abs. 1 Satz 1 Nr. 5 zu einer nicht vertretbaren Wettbewerbsverzerrung zu Gunsten reiner Zubehörverkäufer, da nach dem Wortlaut der Bestimmung nur TK-Diensteanbieter und dessen Vertriebspartner erfasst werden. Hinzuweisen ist schließlich auf dem Umstand, dass – entgegen der Annahme der Begründung – die IMEI nicht fälschungssicher ist. Nach wie vor ist eine Vielzahl von Gerätetypen im Einsatz, die eine Gerätenummer relativ leicht und bei geringfügiger Modifikation sogar auf „Knopf-

22

Stellungnahme des VATM

zum Referentenentwurf für ein „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ („Vorratsdatenspeicherung“, Stand 27. November 2006)



druck“, z.B. bei jedem SIM-Karten-Wechsel, zulassen. Eine etwaige Gefährdung des Ermittlungserfolges kann jedenfalls nicht zu Lasten der Verpflichteten gehen.

Ferner eröffnet Abs. 1 Satz 4 eine Reihe von Fragen für die Umsetzung in der Praxis. Umfasst die Dokumentationspflicht jede (auch einmalige) Nutzung eines anderen Endgerätes? Sollen alle mit der SIM-Karte genutzten Endgeräte dokumentiert werden? Was soll dokumentiert werden im Fall einer ge- oder verfälschten IMEI? Die hier aufgestellten Pflichten sind in der Praxis nicht mit einem vertretbaren Aufwand zu bewältigen. Insbesondere gilt dies aufgrund der gem. Abs. 5 ausgeschlossenen Entschädigung für die Datenerhebung und –speicherung.

Anzumerken ist schließlich, dass die Änderungen und Erweiterungen des § 111 Auswirkungen auch auf die Abläufe nach §§ 112 und 113 haben. Die notwendige Anpassung des automatisierten Verfahrens bedeutet sowohl operativen als auch finanziellen Aufwand, der für die Verpflichteten eine besondere Belastung bedeutet, da die Kosten gem. § 111 Abs. 1 d Abs. 5 nicht erstattet werden.

Forderungen:

- Klarstellung, dass sich die Verpflichtung zur Speicherung in § 111 nur auf Daten bezieht, die von den Anbietern tatsächlich erzeugt bzw. erhoben werden und keine zusätzliche Speicherpflicht begründet wird.
- Berücksichtigung des Umstandes, dass die Ausgestaltung des § 111 Abs. 1 Satz 1 Nr. 5 Wettbewerbsverzerrungen zu Lasten der TK-Anbieter und ihrer Vertriebspartner bedeutet.
- Konkretisierung der Pflichten in § 111 Abs. 1 Satz 4.

Zu § 149 TKG-E- Bußgeldvorschriften

Die Bußgeldvorschrift in Abs. 1 Ziffer 28 d, wonach eine Ordnungswidrigkeit vorliegt, wenn der TK-Anbieter vorsätzlich oder fahrlässig Verkehrsdaten an eine „nicht berechnete Stelle“ übermittelt, ist als zu weitgehend abzulehnen. Hier ist auf unsere obigen Ausführungen zu § 110 b Abs. 1 Satz 1 zu verweisen. Dort haben wir aus Gründen der Rechtsklarheit gefordert, den Begriff der „berechtigten Stelle“ zu konkretisieren, indem auf „zur Strafverfolgung berechnete, öffentliche Stellen“ abgestellt wird. Ferner muss die generelle Fälschungsmög-

23

Stellungnahme des VATM

zum Referentenentwurf für ein „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ („Vorratsdatenspeicherung“, Stand 27. November 2006)



lichkeit von Anordnungen sowie der zu erwartende Anstieg derselben bei der Beurteilung des individuellen Verschuldens berücksichtigt werden.

Forderungen:

- Klarstellung in § 149 Abs. 1 Ziffer 28 d, dass „nicht berechtigte Stellen“ nur solche sind, die nicht Teil der Verwaltung der Strafverfolgungsbehörden sind.
- Anpassung des Verschuldensmaßstabes an die tatsächlichen Gegebenheiten (generelle Fälschungsmöglichkeit sowie Tatsache, dass die Anfragen massiv ansteigen werden).

Zu § 150 TKG-E – Übergangsfristen

Es kann nicht davon ausgegangen werden, dass alle aus den gesetzlichen Änderungen erwachsenden technischen und organisatorischen Maßnahmen unmittelbar mit Erlangung der Gesetzeskraft für diesen Referentenentwurf umgesetzt werden können. Die technischen Änderungen betreffen auch Systeme, die Entwicklungszyklen von z.T. mehreren Jahren haben. Es kann nicht sein, dass der Gesetzgeber versucht, Fristen, die ohne Kenntnis technisch-organisatorischer Rahmenbedingungen definiert wurden, wie z.B. in der EU-Richtlinie, oder die er teilweise verstreichen ließ, ohne Aktivitäten zu entfalten, ausschließlich zu Lasten der Wirtschaft gehen sollen. Aus den Anmerkungen dieser Stellungnahme dürfte deutlich hervorgegangen sein, dass selbst nach Vorlage des Referentenentwurfs noch erhebliche Unklarheiten bezüglich der technischen Umsetzung bestehen. Absolute Gewissheit, welche Anforderungen denn tatsächlich an sie gestellt werden, haben die Verpflichteten erst mit Inkrafttreten des Gesetzes. Ohne diese Rechtssicherheit kann schon aus ökonomischen Gründen nicht verlangt werden, dass derart kostenintensive Maßnahmen durchgeführt werden. Im Übrigen könnte – selbst wenn man zum jetzigen Zeitpunkt eine derartige Rechtssicherheit unterstellen würde – nicht garantiert werden, dass die Maßnahmen mit Inkrafttreten des Gesetzes innerhalb der Umsetzungsfrist tatsächlich umgesetzt werden könnten. Es muss daher eine Übergangsfrist für alle Änderungen von mindestens 12 Monaten nach Inkrafttreten des Gesetzes eingeräumt werden.

Stellungnahme des VATM

zum Referentenentwurf für ein „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ („Vorratsdatenspeicherung“, Stand 27. November 2006)



Forderung:

- Aufnahme von Übergangsvorschriften von mindestens 12 Monaten nach Inkrafttreten des Gesetzes in § 150 Abs.11 a.

3. Zu Artikel 12 – Änderung der Telekommunikationsüberwachungsverordnung

Positiv zu beurteilen ist die in § 3 Abs. 2 Ziffer 5 TKÜV vorgesehene Anhebung der Grenze von 5.000 auf 20.000 Teilnehmer oder Nutzungsberechtigte als Kriterium für den Anwendungsbereich der TKÜV. Allerdings ist Hintergrund dieser Regelung, dass durch die Einführung der Vorratsdatenspeicherung eine große Anzahl von TKÜ-Maßnahmen überflüssig werden, da bei vielen Maßnahmen die Strafverfolgungsbehörden lediglich die Kontakte auf Basis von Verbindungsdaten des zu Überwachenden ausgewertet haben. Hierfür ist künftig eine Ermächtigung nach TKÜV nicht mehr erforderlich. Die Änderung führt zu erheblichen Kosteneinsparungen auf Seiten der Strafverfolgungsbehörden und gleichzeitig zu einem enormen Kostenanstieg bei den TK-Diensteanbietern, denn diese müssen die Vorratsdatenspeicherung umsetzen.

4. Zur Entschädigung

Die Frage der angemessenen Entschädigung der Telekommunikationsunternehmen bleibt auch nach Vorlage des Referentenentwurfs nach wie vor offen. Dies ist besonders bedauerlich, da mit dem vorgelegten Gesetz zur Neuordnung der verdeckten Ermittlungsmaßnahmen ein „harmonisches Gesamtsystem der strafprozessualen heimlichen Ermittlungsmethoden“ geschaffen werden soll¹¹. Die Gelegenheit, auch die Entschädigung zu regeln, und somit auch tatsächlich ein umfassendes Regelwerk ohne offene Fragen vorzulegen, wurde leider verpasst.

Der VATM nimmt zwar positiv zur Kenntnis, dass das Bundesjustizministerium mit der Erarbeitung eines Vorschlages für eine Entschädigungsregelung begonnen hat¹². Wir begrüßen ausdrücklich, dass zumindest das „Ob“ der Entschädigung nicht mehr angezweifelt wird. Allerdings ist dieser Vorstoß – wie wir bereits in der Vergangenheit immer betont haben – aus verfassungsrechtlichen Gründen unerlässlich und damit mehr als überfällig. Die Verhältnis-

¹¹ Vgl. Satz 1 der Einleitung zum Text des Referentenentwurfs unter A.

¹² Vgl. die Ausführungen der Begründung zum Referentenentwurf unter A VI 4. a.E. sowie unter X 3..

Stellungnahme des VATM

zum Referentenentwurf für ein „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ („Vorratsdatenspeicherung“, Stand 27. November 2006)



mäßigkeit der Inanspruchnahme der privaten TK-Unternehmen für die originär staatliche Aufgabe der Strafverfolgung ohne eine finanzielle Ausgleichsregelung wird zunehmend in Frage gestellt¹³. Mit der Einführung der Vorratsdatenspeicherung dürfte diese Auffassung noch bekräftigt werden. Denn im Gegensatz zu der Datenspeicherung im bisherigen Umfang erfolgt die Vorratsdatenspeicherung aus Sicht der Verpflichteten ausschließlich im fremden, nämlich staatlichen Interesse. Die TK-Unternehmen benötigen die erforderlichen Daten (überhaupt) nicht für ihre eigenen Geschäftszwecke, sondern sind im Gegenteil bisher vielmehr immer bemüht gewesen, diese Daten zur Vermeidung von Belastungen schnellstmöglich zu löschen.

Der infolge der Vorratsdatenspeicherung auf die Unternehmen zukommende Aufwand ist immens. Neben der reinen Erhebungs- und Speicherverpflichtung, die eben nicht nur „lediglich“ Kosten für die Kapazitätserweiterung der Speichermedien bedeutet, sondern auch zu einer erheblichen Last für die Netzelemente und deren notwendige Erweiterung führt, was wiederum mit Folgekosten verbunden ist. Insbesondere geht mit der Bearbeitung der Anfragen ein stetig anwachsender Kostenblock durch den Betrieb der notwendigen, speziellen Systeme einher. Gleiches gilt im Hinblick auf den steigenden Personalbedarf, der den finanziellen Aufwand der Unternehmen ebenfalls massiv erhöht. Der stetige Anstieg der Anzahl der Anordnungen und Auskunftersuchen der letzten Jahre wird auch in Zukunft nicht abreißen. Im Gegenteil ist infolge der Ausweitung der Katalogstraftaten in § 100 a StPO mit einem sprunghaften Anstieg der Überwachungsmaßnahmen zu rechnen.

Um einen verfassungswidrigen Zustand zu vermeiden, ist der zeitgleiche Erlass angemessener Entschädigungsregeln unerlässlich. Das Argument, die verbleibende Zeit sei nicht ausreichend, um ausgewogene und umfassende Entschädigungsregeln für alle Eingriffstatbestände zu schaffen, dürfte vor dem Hintergrund der bereits bestehenden Vorschläge, auch

¹³ So beispielsweise der Wissenschaftliche Dienst des Bundestages, der seine Zweifel anlässlich eines Gutachtens „Zulässigkeit der Vorratsdatenspeicherung nach europäischem und deutschem Recht“, August 2006, äußert. Ferner auch die Kommentierung von Klescewski zu § 110 TKG in Säcker, Berliner Kommentar zum Telekommunikationsgesetz, das MPI für ausländisches und internationales Strafrecht anlässlich des Gutachtens im Auftrag des VATM „die Neuregelung zur Auslands-kopfüberwachung gemäß § 4 TKÜV auf dem verfassungsmäßigen Prüfstand“, Juli 2006, oder bereits v. Hammerstein, „Kostentragung für staatliche Überwachungsmaßnahmen nach der TKG-Novelle“, MMR 2004, 222.

Stellungnahme des VATM

zum Referentenentwurf für ein „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ („Vorratsdatenspeicherung“, Stand 27. November 2006)



des Gesetzgebers selbst¹⁴ und der durch die betroffenen Branchenunternehmen mehrfach angebotenen Unterstützung bei der Erarbeitung entsprechender Regelungen, zumindest solange nicht glaubwürdig sein, als nicht ernsthafte Versuche zur Vorlage entsprechender Regelungen unternommen werden. Wir bieten daher auch weiterhin unsere Unterstützung in diesem Prozess an und schlagen folgende Struktur für eine pauschale Abgeltung der derzeit durchzuführenden Überwachungstatbestände vor¹⁵:

Telekommunikationsüberwachung

Einrichtung und Herstellung der Überwachungsverbindung sowie Verlängerung der Maßnahme	Pauschalen pro Kennung und Dienst (Aufgrund der unterschiedlichen Arten der zu überwachenden Dienste (E-Mail-, DSL- oder Telefonie-Überwachung) entstehen unterschiedliche Aufwände, die sich auch in den Pauschalen widerspiegeln sollten).
Übermittlung der Überwachungskopie	Pauschale pro Tag
Funktionsprüfungen	Pauschalen wie oben

Auskunftserteilung

Bestandsdaten	Pauschale pro Kundendatensatz
Verkehrsdaten nach § 100 g StPO bei bekannter Ursprungsadresse	1. Pauschale für den ersten Tag 2. Weitere Pauschale für jeden weiteren Tag, den das Auskunftsbegehren andauert
Verkehrsdaten (Zielwahlsuche)	Pauschale pro Zieladresse
Verkehrsdaten (Zellauswertung)	1. Pauschale für die ersten fünf Minuten 2. Weitere Pauschale für jede weiteren fünf Minuten
Verkehrsdaten (Standortauswertung)	Pauschale pro Auskunft

¹⁴ In der vergangenen Legislaturperiode hatte der Wirtschaftsausschuss des Bundestages unter der Drs.-Nr. 15 (9) 1867 einen Vorschlag vorgelegt, der direkt Eingang in das TKG finden sollte, infolge der vorgezogenen Neuwahlen zum Bundestag aber nicht weiter diskutiert wurde.

¹⁵ In Anlehnung an die Planungen des Bundesjustizministeriums, erst in einem zweiten Schritt über die Kosten zu sprechen, wurden zunächst bewusst keine Aufwände und Beträge zugewiesen.

Stellungnahme des VATM

zum Referentenentwurf für ein „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ („Vorratsdatenspeicherung“, Stand 27. November 2006)



Abschließend möchten wir folgende Ausführungen des vorliegenden Referentenentwurfs zur Frage der Entschädigung kommentieren.

- Gem. der Begründung (A X 2) wird keine Kostenerstattung für Speichermedien und gesteigerte Betriebskosten gewährt. Diese infolge der Vorratsdatenspeicherung anfallenden Kosten entstehen aber ausschließlich zur Erfüllung staatlicher Aufgaben, was bei der Entschädigung berücksichtigt werden muss.
- Die Angabe in der Begründung (A X 2), dass bei „einem großen Telekommunikationsdiensteanbieter mit einem Jahresumsatz von annähernd 60 Mrd. Euro Zusatzkosten für die Erfüllung der Speicherungsspflichten 0,00116% des Jahresumsatzes ausmachen“, ist irreführend. Es ist unzulässig, bei der Berücksichtigung der Auswirkungen des Gesetzes auf die Betroffenen lediglich ein Unternehmen zu betrachten, da so keine Rückschlüsse auf die gesamte Branche gezogen werden können. Hier ist unbedingt eine breite Erhebungsbasis zu wählen, die die Besonderheiten auch kleinerer und mittelständiger Unternehmen berücksichtigt. Die Aufwendungen zur Erfüllung der Speicherverpflichtungen führen bei kleineren Unternehmen zu wesentlich höheren Belastungen im Verhältnis zum Umsatz. Ferner müssen beispielsweise die unterschiedlichen Unternehmensprozesse berücksichtigt werden, da je nach dem, ob manuelle oder automatisierte Prozesse zur Erfüllung der Auskunftspflichten angewendet werden, der Aufwand und damit auch die Kosten extrem differieren. Ohne Berücksichtigung dieser Faktoren kommt es zu vermeidbaren Wettbewerbsverzerrungen.
- Die Annahme in der Begründung (A X 2.), dass die Zielwahlsuche in Zukunft weitgehend entbehrlich wird, ist unzutreffend, vgl. unsere Anmerkungen zu § 100 g StPO.
- Schließlich ist die ebenfalls unter A X 2 aufgeführte Annahme richtig zu stellen, wonach die Unternehmen infolge des Wegfalls der Berichtspflicht gem. § 110 Abs. 8 TKG (Erhebung und Ermittlung statistischer Angaben über Anordnungen nach den §§ 100 a, 100 b StPO) entlastet würden. Hier wird der Eindruck erweckt, diese Entlastungen würden die infolge der Vorratsdatenspeicherung auftre-

Stellungnahme des VATM

zum Referentenentwurf für ein „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ („Vorratsdatenspeicherung“, Stand 27. November 2006)



tenden Belastungen kompensieren. Dies ist keineswegs der Fall, vgl. unsere Anmerkungen zu § 100 b StPO.

Berlin, 19. Januar 2007

Im VATM sind mehr als 50 der im deutschen Markt operativ tätigen Telekommunikations- und Dienstleistungsunternehmen aktiv. Alle stehen im direkten Wettbewerb zum Ex-Monopolisten Deutsche Telekom AG und engagieren sich für mehr Wettbewerb im Telekommunikationsmarkt – zugunsten von Innovationen, Investitionen und Beschäftigung. Seit dem Jahr 2000 haben die Wettbewerber im Festnetz- und Mobilfunkbereich Investitionen in Höhe von über 20 Mrd. € vorgenommen. Unmittelbar sichern die neuen Festnetz- und Mobilfunkunternehmen rd. 50.000 Arbeitsplätze in Deutschland sowie zusätzlich etwa 50 % der Beschäftigung in den Zulieferbetrieben.