Stellungnahme des Sachverständigen Dr. Rainer Liedtke, Datenschutz- und Sicherheitsbeauftragter E-Plus-Mobilfunk GmbH

Öffentliche Anhörung des Rechtsausschusses des Deutschen Bundestags zu dem Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG – 21. September 2007, BT-Drs. 16/5846

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.

Albrechtstraße 10 A
10117 Berlin-Mitte
Tel. +49. 30. 27576-0
Fax +49. 30. 27576-400
bitkom@bitkom.org
www.bitkom.org

Präsident
Prof. Dr. Dr. h. c. mult. August-Wilhelm Scheer

Hauptgeschäftsführer
Dr. Bernhard Rohleder

1 Datenschutzrechtliche Grundfragen der Vorratsdatenspeicherung

Im Laufe der vergangenen Jahre haben sich die Übermittlungspflichten der Anbieter von Telekommunikationsdiensten an Polizei und Justiz deutlich erweitert. Sicherheitsbehörden und leider auch zunehmend darüber hinaus, haben zwischenzeitlich oftmals weitergehende Rechte als die Kunden bezüglich ihrer eigenen Daten. Sicherlich ist eine angemessene Ausweitung der Zugriffsmöglichkeiten auf TK-Daten durch Sicherheitsbehörden vor dem Hintergrund sich wandelnder Modi operandi von Kriminellen erforderlich und absolut gerechtfertigt.

Dabei galt aber immer der Grundsatz, dass nur die Daten übermittelt werden können und damit übermittelt werden müssen, die die Provider zu eigenen Zwecken erhoben haben. Dieser Grundsatz ist erstmalig aufgeweicht worden, als mit Novellierung des TKG im Jahre 2004 die Erhebungspflicht für einige Bestandsdaten eingeführt wurde. Diese Daten unterliegen jedoch nicht dem Fernmeldegeheimnis und führten nur in geringerem Maße zu einer Ausweitung der Datenerhebung. Dennoch stellt sich bereits hier die Frage, ob diese Regelung verfassungsgemäß ist, widerspricht sie doch dem vom Bundesverfassungsgericht im Urteil zur Rasterfahndung deutlich gemachten Verbot einer Sammlung personenbezogener Daten auf Vorrat.

Der nunmehr vorliegende Gesetzesentwurf geht nun aber noch einen deutlichen Schritt weiter: Er dehnt die Erhebungs- und Speicherpflicht auf Daten aus, die als Verkehrsdaten dem Fernmeldegeheimnis unterliegen, darunter eben auch Daten, die die Provider zu eigenen Zwecken gar nicht erheben. Das immer wieder zur Abschwächung der Eingriffsschwere vorgebrachte Argument, es handele sich hierbei nicht um Inhalte sondern „nur“ um Verkehrsdaten, ist schlichtweg irreführend: Der § 88 des TKG bezieht in den Schutzbereich des Fernmeldegeheimnisses ausdrücklich auch die näheren Umstände der Telekommunikation und explizit auch die erfolgloser Verbindungsversuche mit ein. Und dies ist auch sachlich gerechtfertigt. Verkehrsdaten dokumentieren Kommunikationsbeziehungen, die als solche ebenso schützenswert sind, wie der vielleicht belanglose Inhalt der Kommunikation. Darüber hinaus bieten

die Verkehrsdaten durch die heute übliche Vielfalt der Kommunikationsbeziehungen einen ganzen Strauss von detaillierten, personenbezogenen Informationen, aus denen sich ein umfassendes Bild der betrachteten Person zusammenstellen lässt.

Vor diesem Hintergrund braucht kaum noch erwähnt zu werden, dass eben nicht nur das Fernmeldegeheimnis, sondern zugleich auch das Recht auf informationelle Selbstbestimmung, wie es das Bundesverfassungsgericht aus Art. 2 des Grundgesetzes ableitet, tangiert ist. Die Vorratsdatenspeicherung greift also tief in verbürgte Grundrechte ein.

2 Paradigmenwechsel im Datenschutzrecht

Aus Sicht des Datenschutzes ist entscheidend, dass mit der Vorratsdatenspeicherung ein deutlicher Paradigmenwechsel im Datenschutzrecht einhergeht, dessen langfristige Auswirkungen heute noch kaum absehbar sind. Das deutsche Datenschutzrecht war über Jahrzehnte geprägt vom Grundsatz der strengen Zweckbindung . Dieses Fundament wird mit der Vorratsdatenspeicherung unterhöhlt, denn die bloße Möglichkeit einer künftigen Strafbarkeit ist kein konkreter Zweck in diesem Sinne. Tatsächlich werden künftig Datensätze von Millionen von Bürgern vorgehalten werden, die niemals ins Visier der Ermittlungsbehörden gelangen werden. Hierin liegt gerade das Wesen der Vorratsdatenspeicherung und im Übrigen auch der Grund, weshalb vorherige nationale politische Initiativen nie erfolgreich waren. Eine solche „Speicherwut“ lässt sich mit den datenschutzrechtlichen Grundsätzen der Datensparsamkeit und Datenvermeidung nicht in Einklang. Es stellt sich die Frage, mit welchem Recht der Staat vollständige Bewegungsprofile aller Bürger – nahezu jeder trägt heute ein Mobiltelefon mit sich – ohne jeden konkreten Verdacht speichern lassen darf. Ohne Belang ist dabei die Frage, ob die Daten von den Providern gespeichert werden oder unmittelbar an die Sicherheitsbehörden übermittelt werden. Man darf gespannt sein, wie das Bundesverfassungsgericht die Rechtslage hier einschätzt. Im Sinne des Bedürfnisses nach Rechtssicherheit ist zu hoffen, dass man sich seitens des Verfassungsgerichts vor dem Hintergrund der europäischen Richtlinie in diesem Fall nicht einfach auf einen eingeschränkten Prüfungsumfang im Sinne der „Solange“-Rechtsprechung beruft und somit die grundlegenden Fragen ausspart.

3 Maßnahmen wirksam und angemessen?

Aus datenschutzrechtlicher Sicht stellt sich daneben im Übrigen immer auch die Frage der Verhältnismäßigkeit. An dieser Stelle kommt noch anderer Aspekt mit ins Spiel, nämlich die durchaus fragliche Geeignetheit vieler der jetzt vorgesehenen Maßnahmen. Es ist schon beim Umsetzungstreffen der EU-Kommission im März darauf hingewiesen worden, dass sich ein erheblicher Teil der neuen Maßnahmen in der Praxis als „zahnloser Tiger" erweisen wird. Dies betrifft etwa die sog. IMEI-Speicherung aber auch die umfassende Protokollierung von IP-Adressen. Dies sind Kennungen, die in der Praxis kinderleicht unterlaufen werden können und die keineswegs so eindeutig sind, wie häufig dargestellt. Was die Erhebung der Handy-Gerätenummer angeht so sollte man sich vor Augen halten, dass es jedem Bürger frei steht, sich Geräte unabhängig von Telekommunikations-Verträgen bei einem Provider oder einem Elektronikmarkt zu kaufen. Dies betrifft aktuell ca. 40% der Endgeräte, mit steigender Tendenz. Die IMEI kann daneben auch technisch manipuliert werden. Aber auch IP-Adressen sind ohne allzu spezifisches technisches Know-How ohne weiteres zu verschleiern oder eben gar zu fälschen. Wer sich also wirklich im Bereich schwerer Straftaten bewegt, wird die Maßnahmen weitgehend zu umgehen wissen.

Damit besteht die Gefahr, dass die Maßnahmen dieser gesetzlichen Regelung die definierte Zielgruppe, Terroristen etc. nicht erreichen werden. Dies wird aber nur schwer zu verifizieren sein, da die im Referentenentwurf noch enthaltenen Berichtspflichten zum Erfolg der Maßnahmen in den korrespondieren Änderungen zur StPO leider im Regierungsentwurf nicht mehr enthalten sind.

Abgesehen davon, dass damit die Verhältnismäßigkeit der schwerwiegenden Eingriffe nicht mehr gegeben ist, stellt sich noch ein weiteres Problem: Über die Fälschung der genannten Daten lassen sich in gewissem Umfang sogar falsche elektronische Spuren legen: Nutze ich etwa ein auf dem Flohmarkt erworbenes Handy, dass noch unter einem anderen Nutzer registriert ist, ist es plötzlich dieser, der möglicherweise ins Visier der Verfolgungsbehörden gerät. Ähnliches gilt für IP-Adressen.

4 Der Entwurf als Minimalumsetzung der Richtlinie?

Der Deutsche Bundestag hatte im Februar 2006 beschlossen[1], sich bei der Umsetzung der Richtlinie auf deren Minimalanforderungen zu beschränken. Leider ist diese Linie nicht konsequent eingehalten worden. Zu konstatieren ist zunächst zwar, dass insbesondere bei den Speicherfristen die Beschränkung auf sechs Monate durchgehalten wurde. Der Entwurf regelt aber eine ganze Reihe von Dingen neu, für die sich keinerlei Verpflichtung aus der Richtlinie ergibt. Und wo die Richtlinie Auslegungsspielräume lässt, wurden diese teilweise sehr extensiv interpretiert. Im Einzelnen geht der Entwurf an folgenden Punkten über die Vorgabe der Richtlinie hinaus:

- **Begriff der „schweren Straftat" als Anknüpfungspunkt für den Zugriff auf die Vorratsdaten:**

  Die Richtlinie definiert in Erwägungsgrund 21 als Ziel der Vorratsdatenspeicherung die Verfolgung „schwerer Straftaten" („*serious crime*"). Der Regierungsentwurf ermöglicht den Zugriff dagegen jetzt über § 100g StPO letztlich umfassend bei Straftaten von *erheblicher Bedeutung* sowie vor allem pauschal immer dann, wenn irgendeine Straftat mittels Telefon oder Internet begangen wurde. Der Entwurf erfasst damit also auch die einfache Beleidigung am Telefon oder im Internet. Da die Bewertung der Richtlinie nicht allein auf den eigtl. Speicherumfang beschränkt vorgenommen werden kann, sondern der Blick auch auf die Verwendung der Daten gerichtet werden muss, liegt hierin eine klare Ausweitung gegenüber der Richtlinie. Dies auch deshalb, weil die Ausdehnung der Ermächtigungsgrundlage direkte Folgen in der Praxis nach sich ziehen wird, nämlich einen erheblich höheren Abfrageumfang. Dabei spielt natürlich auch eine Rolle, dass der § 100 g StPO-E im Rahmen seiner abgesenkten Eingriffsvoraussetzungen nunmehr auch die „kleine TÜ", also eine Echtzeit Übermittlung der Verkehrsdaten umfasst, wenn auch ohne Standortinformationen.

- **Erweiterungen der Speicherung von Bestandsdaten:**

  Was die Richtlinie überhaupt nicht regelt, ist die Behandlung von Bestandsdaten. Der Regierungsentwurf sieht hier dagegen auch Neuerungen vor, die erhebliche Auswirkungen auf die betroffene Branche haben. Die §§ 111 und 112 TKG regeln die Verpflichtung der Unternehmen, bestimmte Bestandsdaten zu speichern und für ein automatisiertes Auskunftsverfahren abrufbar zu machen. § 111 TKG soll

[1] BT-Drs. 16/545.

nun dahingehend erweitert werden, dass dies künftig etwa auch die Gerätenummer (IMEI) bei Mobiltelefonen umfassen soll. Da diese Daten heute nicht flächendeckend erhoben und für das automatisierte Auskunftsverfahren vorgehalten werden, müssen die Anbieter hier die Datenbanken umstellen und auch die Erfassungsprozesse über die gesamte Vertriebskette neu strukturieren. Im Einzelnen hieße das, es müsste eine technik-gestützte Erfassung implementiert werden, z.B. durch das Einscannen der Nummer, um die Daten überhaupt verwertbar zu machen. Eine manuelle Eingabe der 15stelligen IMEI würde zu einer erheblichen Fehlerrate führen und die Daten unbrauchbar machen. Damit werden die Unternehmen jetzt faktisch gezwungen, die technische Ausstattung auch kleiner Vertriebspartner erheblich zu verbessern, was enorme Kosten verursachen würde.

Dies alles geschieht für eine Speicherung, deren Zweck mehr als fraglich ist – schließlich kann jeder ein Endgerät auch im normalen Zubehörhandel ohne Vertrag erwerben – dies sind aktuell 40% der Geräte -, so dass diesem Endgerät gar kein Besitzer zugeordnet werden kann. Warum dies, wie in der Begründung ausgeführt, zu einer besseren Identifikation von Beschuldigten führen soll, erschließt sich nicht. Letztlich führt dies zu einer Wettbewerbsverzerrung zwischen Händlern, über die auch TK-Verträge abgeschlossen werden können und dem Geschäft direkt daneben, das nur Zubehör ohne Verträge verkauft.

Im Übrigen sollen die entsprechenden Bestandsdaten künftig auch von E-Mail-Diensteanbietern gespeichert und dem Auskunftsverfahren zugänglich gemacht werden. Zwar greift die Speicherpflicht zumindest nach der Entwurfsbegründung nur, wenn diese Daten sowieso erhoben werden – tut ein Anbieter dies allerdings, so ist zumindest die Verpflichtung zur Vorhaltung für das automatisierte Auskunftsverfahren für ihn neu. Da hierfür eigenständige Datenbanken mit den entsprechenden Schnittstellen aufgebaut werden müssen, bedeutet auch dies einen ganz erheblichen Aufwand, der mit der Umsetzung der Richtlinie nicht begründet werden kann.

- **Erweiterungen des Adressatenkreises**

  Ebenfalls ohne entsprechendes Pendant in der Richtlinie ist die in § 113 a Abs. 6 TKG-E vorgesehene Speicherpflicht, für denjenigen der „Angaben verändert“, wie es die Vorschrift formuliert. Adressiert sind damit zumindest auch sog. Anonymisierungsdienste, was gemeinhin zur Legitimation der Vorschrift herangezogen

wird. Dabei bleibt allerdings außen vor, dass solche Anonymisierungsdienste regelmäßig aus dem Ausland agieren und damit gar nicht über die Vorschrift verpflichtet werden können. Wo als wirklich schwere Kriminalität im Raum steht, dürfte auch diese Vorschrift ein stumpfes Schwert bleiben.

Gleichzeitig ist die Vorschrift so allgemein formuliert, dass der jeweilige Diensteanbieter entscheiden muss, ob etwa bestimmte technisch bedingte Prozesse im Netz mit Änderungen in diesem Sinne einhergehen, so dass hier noch zusätzliche Speicherpflichten zu entstehen drohen. Die Vorschrift ist insofern auch ein gutes Beispiel dafür, dass für die Unternehmen die konkreten Folgen des Entwurfs noch gar nicht zu überblicken sind. Die Begründung hilft hier auch nicht weiter. Dort findet sich nur die äußerst extensive Anmerkung, dass es gleichgültig sei, in welcher Weise das ursprüngliche Datum verändert wird und es nicht darauf ankomme, ob die Zwischenschaltung des Diensteanbieters etwa aus technischen oder wirtschaftlichen Gründen durch die an der Erbringung der Telekommunikationsdienste geschieht oder die Zwischenschaltung vom Endnutzer veranlasst wurde.

- **Lage der Funkantennen und Hauptstrahlrichtung**

  Schließlich ist auch die in § 113 Nr. 7 des Entwurfs geplante Speicherpflicht für Daten zur Lage von Funkantennen und deren Hauptstrahlrichtung von der Richtlinie nicht vorgesehen. Hier handelt es sich also um ein echtes zusätzliches Datenfeld, dass allein durch die vorgesehene nationale Umsetzung zum implementieren wäre. Auch der Aufwand, den die Mobilfunkbetreiber hierfür betreiben müssen, ist erheblich. Berücksichtigt werden muss, dass Netze laufend optimiert werden und sich damit natürlich auch diese Parameter ändern. Wahrscheinlich wird man also nicht umhin kommen, derartige dynamische Parameter unmittelbar jedem Gesprächsdatensatz zuzuordnen. Das hierfür ein sehr hoher Aufwand erforderlich ist, dürfte auch dem Laien verständlich werden. Letztendlich multipliziert sich an dieser Stelle der Umfang der von der Richtlinie vorgesehenen, schon für sich genommen problematischen Verpflichtung zur Speicherung von Standortdaten, nochmals. Bislang werden entsprechende Daten nicht erfasst.

5 Zu den Verwendungszwecken nach § 113b TKG-E

Der Regierungsentwurf enthält gegenüber dem Referentenentwurf eine maßgebliche Erweiterung insoweit, als in § 113b TKG-E nunmehr neben dem Zweck der Strafverfolgung auch die Zwecke der Gefahrenabwehr sowie die Nutzung für geheimdienstliche Zwecke vorgesehen ist. Zunächst ist zu betonen, dass auch dies ein Aspekt ist, an welchem der Entwurf über die Richtlinienvorgaben hinausgeht. Die Bundesregierung war sich dessen auch bewusst, denn die Gesetzesbegründung enthält hierzu ausführliche juristische Erörterungen zur Vereinbarkeit mit der Richtlinie, die ein gewisses Unbehagen erkennen lassen. Abseits dieser juristischen Detailfragen ist die Erweiterung aber auch aufgrund ihrer praktischen Folgen problematisch. Denn der Umfang der Anfragen wird hierdurch stark steigen. Das Gefahrenabwehrrecht der Länder arbeitet an vielen Stellen mit weiten, manchmal zu weiten Generalklauseln. Wenn die Länder hier auch im Bereich der Beauskunftung aus der Vorratsdatenspeicherung weite Tatbestände schaffen, könnte die Gefahrenabwehr künftig sogar zu einem der Hauptanwendungsbereiche der Nutzung der Vorratsdaten werden. Die betroffenen Unternehmen würden also zukünftig immer stärker von verschiedenen Seiten in die Pflicht genommen, wobei die rechtlichen Grundlagen immer unüberschaubarer würden, weil jedes Land seine eigenen Befugnisse schaffen könnte. Letztendlich darf man sich natürlich auch fragen, wie bis zu sechs Monate alte Verkehrsdaten bei der Abwehr künftig drohender Gefahren nützen können.

6 Zum Inkrafttreten der Verpflichtungen

Nach dem jetzigen Stand der Dinge müssten die betroffenen Unternehmen die neuen Pflichten am 1. Januar 2008 technisch umgesetzt haben. Diese Zeit wird für die technische Umsetzung der Verpflichtungen kaum ausreichen, was im Kern offenbar auch der Bundesregierung bewusst ist. Denn der Regierungsentwurf sieht ausdrücklich vor, dass eine Sanktionierung als Ordnungswidrigkeit bei Nichteinhaltung der Pflichten erst ab 1. Januar 2009 erfolgen können soll. Hiermit wird aber unterschlagen, dass die Verpflichtungen als solche auf dem Weg des Verwaltungszwangs trotzdem durchgesetzt werden können und zwar mit Zwangsgeldern bis zu 500.000 €, der Sanktionsdruck besteht also gleichwohl. Die Verschiebung des Ordnungswidrigkeitsrahmens ist daher eher als Beruhigungspille zu verstehen. Darüber hinaus besteht die Möglichkeit, dass Mitarbeiter von Unternehmen persönlich – nicht das Unternehmen oder deren Verantwortliche - mit einem Verfahren wegen Strafvereitelung konfrontiert

werden. Dies betrifft in aller Regel die unmittelbar mit den Aufgaben betrauten Mitarbeiter, für die dies eine erhebliche persönliche Belastung bedeutet.

Insgesamt entsteht leider der Eindruck, dass der technische wie personelle Aufwand, der durch die neuen Pflichten entsteht, seitens der Politik weitgehend unterschätzt oder aber ignoriert wird. Es reicht in der Praxis eben nicht aus, eine Software auf die Schnelle anzupassen. Die betroffenen Unternehmen müssen vielmehr umfassend Datenbanken neu aufsetzen, müssen zusätzliche Bandbreiten für die Übertragung der immensen zusätzlichen Datenmengen aus den dezentralen Netzelementen bereitstellen und nicht nur für die neuen Speicherpflichten, sondern auch für die Abfrage neu aufstellen. Das alles bedeutet einen erheblichen Personalaufwand und nicht zuletzt auch die Einschaltung externer Dienstleister. Im Übrigen wird der Umfang der zu speichernden Daten schlicht und einfach massiv steigen, was selbstverständlich auch eine massive Aufrüstung der Hardware-Kapazitäten zur Folge hat. Und für alle diese Maßnahmen stehen uns nach den aktuellen Plänen nunmehr wahrscheinlich 2 Monate inklusive der Weihnachtszeit zur Verfügung.

Hiergegen wird oft eingewandt, dass die Pläne durch die Richtlinie ja schon länger bekannt seien. Dies greift indes aus mehreren Gründen zu kurz. Zum einen belässt es der deutsche Gesetzentwurf eben keineswegs bei den Verpflichtungen der Richtlinie, sondern geht, wie bereits erläutert, hierüber hinaus. Es lässt sich auch nicht einfach argumentieren, man könne ja den Kernbereich der Richtlinie schon implementieren und die Feinheiten später regeln. Denn in der Praxis müssen jedes Mal Prozesse neu gestaltet werden, die entsprechenden Systeme und Datenbankstrukturen angepasst und die erforderlichen Kapazitäten bis hin zu den Back-up-Systemen bereitgestellt werden. Außerdem bedarf es hierzu auch noch Testläufe. Eine schrittweise Vorgehensweise würde zusätzliche Betriebsrisiken mit sich bringen und die Kosten der Umsetzung damit drastisch anheben. Insgesamt ist es letztendlich nicht seriös machbar, technische Systeme mit massivstem Aufwand auf- und umzurüsten, ohne das der genaue Pflichtenumfang tatsächlich klar wäre. Der genaue Pflichtenkatalog aber wird frühestens nach Verabschiedung des Gesetzentwurfs im Oktober bzw. November bekannt sein, womit die verbleibende Zeit kaum mehr ausreichen wird. Allein E-Plus geht beispielsweise für Aufwände bei der Speicherung der Verkehrsdaten für die klassischen Voice-Dienste von einem Invest im mittleren einstelligen Millionenbereich aus. Dabei sind aber viele Dinge, z.B. die Prozess- und Systemänderungen für die Erhebung der IMEI noch nicht mitberücksichtigt. Für diese Projekte stehen wegen des

zwingend notwendigen Know-Hows nur wenige Experten zur Verfügung, die wiederum bei ihrer eigentlichen Aufgabe, der Integration neuer Dienste fehlen.

Schließlich ist noch auf einen anderen Umstand hinweisen, der zeigt, wie schwierig die Situation für die Betreiber heute ist: Nach dem jetzigen Stand der Dinge darf zum Beispiel bei Internet-Verbindungsdaten im Rahmen von Flatrates eine maximal siebentägige Speicherung erfolgen. Selbst dies ist datenschutzrechtlich schon ein Kompromiss – Gerichte hatten entschieden, dass hier eine Speicherung auf Basis des geltenden TKG eigentlich gar nicht erfolgen dürfe. Die Unternehmen müssen also derzeit Ihre Systeme darauf ausrichten, die Daten möglichst schnell zu löschen und gleichzeitig für Punkt 0.00 Uhr 1. Januar 2008 das genaue Gegenteil, nämlich die bislang umfassendste Datenspeicherung überhaupt realisieren. Wenn über die Umsetzungsfristen geredet wird, sollte man sich insofern auch vor Augen halten, dass diese eben auch die Vorbereitung eines technisch sauberen Umschaltszenarios beinhaltet.

Diese kurzen Fristen sind umso unverständlicher als gerade aufgrund des Drängens der Bundesregierung in der Richtlinie für Internet- und E-Mail-Dienste ein Dispens bis 15. März 2009 vorgesehen ist, der im Referentenentwurf auch weitgehend noch enthalten war. Selbst von dieser Möglichkeit hat die Bundesregierung nicht mehr Gebrauch gemacht, obgleich sie durch viele Stellungnahmen auf die Probleme, die schon mit den längeren Fristen in der alten Fassung bestanden, fundiert hingewiesen wurde. Insoweit geht die Umsetzung auch an dieser Stelle über die Richtlinienvorgaben hinaus.

Schlussendlich empfiehlt sich einen Blick in die Bundesratsempfehlungen zu diesem Entwurf vom 8. Juni 2007: Dort findet sich auf den Seiten vier und fünf in Zusammenhang mit § 100a Abs. 4 StPO, die Forderung, die vorgesehene unverzügliche Löschung von kernbereichsrelevanten Aufzeichnungen aus dem Entwurf zu entfernen. Die Begründung hierfür spricht den betroffenen Unternehmen gewissermaßen „aus der Seele“. Es wird darauf abgestellt, dass

> *„.. die Umsetzung der Vorschrift eine Neukonzeption der kompletten Archivierungsmechanismen – sowohl Software als auch Hardware – in sämtlichen TKÜ-Anlagen erforderlich machen würde. Diese Neukonzeption der Archivierung bedeutet für die Lieferanten der TKÜ-Technik aber auch für die polizeilichen Bedarfsträger eine hohen finanziellen wie zeitlichen Aufwand, um die Anforderungen in die Systeme zu implementieren.“*

Vor eben diesen Problemen stehen auch die Unternehmen bei der Umsetzung der sie treffenden Pflichten. Und hier sollten keine anderen Maßstäbe gelten, als für den Staat als Verpflichtungsadressat.

7 Die Kosten der Unternehmen und die Entschädigungsfrage

Gänzlich unberücksichtigt bleibt erneut die ebenfalls zur Wahrung der Verfassungsmäßigkeit des Gesetzes erforderliche Entschädigungsregelung für die erneute und zusätzliche Inanspruchnahme der Unternehmen für hoheitliche Zwecke.

Hierzu gab es schon 2005 es den klaren politischen Beschluss, die Unternehmen für die Aufwände im Zusammenhang mit der Überwachungs- und Speicherpflichten zu entschädigen. Es wurde im TKG eine eigene Ermächtigung für den Erlass einer solchen Regelung geschaffen und seit April 2005 liegt sogar ein Entwurf für eine Entschädigungsregelung vor. Der BITKOM hat außerdem ein verfassungsrechtliches Gutachten des Entschädigungsrechtlers *Schmidt-Preuß* vorgelegt, dass klar und deutlich die umfassende Entschädigungspflicht des Staates belegt.

Trotz all dieser Initiativen und Absichtsbekundungen fehlt bis heute diese dringend notwendige Regelung. Es gibt derzeit zwar Initiativen seitens des Bundeswirtschaftsministeriums als auch seitens des Bundesjustizministeriums. Jedoch ist klar erkennbar, dass die Schaffung der Entschädigungsregelung nicht mit der gleichen Energie vorangetrieben wird, wie der vorliegende Gesetzentwurf. Vor allem aber sollen die erheblichen Investitionskosten der Unternehmen im Rahmen dieser Initiativen offenbar von vornherein ausgeklammert werden.

Wichtig ist in diesem Zusammenhang, dass die Entschädigungsfrage nicht erst durch die Vorratsdatenspeicherung aufgekommen ist – sie wird hierdurch nur weiter verschärft. Tatsächlich leisten vor allem die Telekommunikations-Unternehmen seit Jahren ihren Beitrag zur Überwachung, ohne dass die resultierenden Kosten auch nur annähernd kompensiert würden. Derzeit wird die Branche für ihre Anstrengungen nach dem JVEG wie z.B. Zeugen eines Ladendiebstahls entschädigt – nämlich mit maximal 17 Euro. Der BITKOM hat im Frühjahr 2007 Schätzungen bei den Mitgliedsunternehmen eingeholt, aus denen sich ergibt, dass die neuen Verpflichtungen branchenweit fast 75 Mio. Investitionskosten sowie einen zweistelligen Millionenbetrag laufender Betriebskosten pro Jahr zur Folge hätten. Diese Zahlen finden Bestätigung bei Vergleichen mit dem Ausland. Aus Großbritannien wurden beim Umsetzungstref-

fen der Kommission im März zum Beispiel etwa 50 Millionen Euro an Investitionskosten und etwa 12 Millionen Euro jährlicher Betriebskosten gemeldet. Im Übrigen geht die Bundesregierung fehl in der Annahme, die Mehrkosten könnten einfach auf den Endkunden abgewälzt werden. Zum einen ist dies schon aufgrund des intensiven Wettbewerbs im Telekommunikations-Sektor nicht möglich. Zum anderen sind mittlerweile langfristige Vertragsbindungen mit den Endkunden marktüblich, die keine kurzfristigen Vertragsanpassungen zulassen.

Die Schaffung einer angemessenen Entschädigungsregelung sollte aber letztlich gar nicht von den konkreten, nur schwer prognostizierbaren Zahlen abhängen. Denn die Frage des „Ob“ einer solchen Pflicht des Staates ist bereits verfassungsrechtlich determiniert und hängt nicht von den tatsächlich anfallenden Belastungen ab. Die Entschädigungsfrage bleibt damit einer der entscheidenden Aspekte in der Diskussion. Der Anspruch der Bundesregierung muss es sein, dass die entsprechenden Vorhaben mit der gleichen Energie vorangetrieben werden, wie der eigentliche Gesetzentwurf zur TK-Überwachung und Vorratsdatenspeicherung.

Düsseldorf, den 12.09.07

Stellungnahme

zum Regierungsentwurf für ein Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG (Kabinettsbeschluss vom 18. April 2007, BR-Drs. 275/07)

22. Mai 2007

Der BITKOM vertritt mehr als 1.000 Unternehmen, davon 850 Direktmitglieder mit 120 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Geräte-Hersteller, Anbieter von Software, IT- und Telekommunikationsdiensten sowie Content.

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.

Albrechtstraße 10
10117 Berlin
+49. 30. 27576-0
Fax +49. 30. 27576-400
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner
Dr. Guido Brinkel
Referent
Telekommunikations- und Medienpolitik
+49. 30. 27576-221
Fax +49. 30. 27576-222
g.brinkel@bitkom.org

Präsident
Willi Berchtold

Hauptgeschäftsführer
Dr. Bernhard Rohleder

Zusammenfassung

Die Bundesregierung hat am 18. April 2007 einen Entwurf für ein Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vorgelegt. Der Entwurf sieht vor allem Änderungen in der Strafprozessordnung (StPO) und im Telekommunikationsgesetz (TKG) vor. Er will einerseits Regelungen im Bereich der Telekommunikationsüberwachung sowie weitere Zugriffsrechte auf Kommunikationsdaten reformieren. Andererseits setzt er die Richtlinie über die Speicherung von Kommunikationsdaten, die sog. „Vorratsdatenspeicherung“ um. BITKOM hat in seiner Stellungnahme zum Referentenentwurf (RefE) bereits ausführlich zu den geplanten Neuregelungen Stellung genommen.[1] Wo der RegE an diesen festhält, sollen daher hier nur die Kernaspekte wieder aufgegriffen werden.

Der BITKOM begrüßt zunächst, dass der Regierungsentwurf daran festhält, hinsichtlich der Speicherungsdauer nur die Minimalanforderung der Richtlinie von sechs Monaten umzusetzen und somit dem Beschluss des Bundestages vom 16. Februar 2006 (BT-Drs. 16/545) zu folgen. Daneben ist positiv hervorzuheben, dass der aktuelle Entwurf nunmehr klarstellt, dass die Speicherpflichten auch im EU-Ausland realisiert werden können. Wir gehen schließlich auf Basis des aktuellen Wortlauts davon aus, dass es keinerlei Vorgaben für eine Separierung der Daten gibt, so dass die Frage der Separierung in der Praxis den betroffenen Unternehmen überlassen bleibt. Auch dies begrüßen wir.

Gegenüber dem RefE sind aber auch eine Reihe problematischer Neuerungen vorgesehen. So verschärft die geplante einheitliche Umsetzungsfrist zum 1. Januar 2008 die durch die unrealistischen Vorstellungen über die technisch erforderlichen Umsetzungszeiten geschaffene Situation. Diese erheblichen Schwierigkeiten werden auch durch das einjährige Aussetzen vereinzelter Sanktionsvorschriften nicht kompensiert. Die jetzige Regelung zum Inkrafttreten ist insbesondere insoweit inakzeptabel, als

[1] Stellungnahme des BITKOM zum Referentenentwurf zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, abrufbar unter http://www.bitkom.org/de/themen_gremien/36535_45129.aspx

damit nunmehr der im Referentenentwurf noch vorgesehene notwendige Dispens für E-Mail und Internetdienste entfallen ist.

Nicht absehbar sind zudem die Folgen der erweiterten Datenverwendung auch für Zwecke der Gefahrenabwehr und der Geheimdienste sowie der konkrete Regelungsgehalt verschiedener Einzelregelungen. Wir plädieren an diesen Stellen für Klarstellungen im Gesetzestext, um ein Höchstmaß an Rechtssicherheit in den sensiblen Bereichen Vorratsdatenspeicherung und Telekommunikationsüberwachung zu gewährleisten.

Schließlich enthält der RegE völlig unrealistische Aussagen zur Kostenbelastung der Unternehmen – sowohl hinsichtlich der Investitionskosten als auch hinsichtlich der laufenden Aufwände. Diese Aussagen sind nicht in Einklang zu bringen mit den Kostenschätzungen der betroffenen Branche. Eine umfassende Regelung zur Entschädigung der betroffenen Unternehmen vermissen wir daher nach wie vor. Die Entwurfsbegründung verweist hierzu auf eine noch zu erarbeitende zukünftige Regelung. Aus Sicht des BITKOM ist die Entschädigungsfrage jedoch zentraler Bestandteil der Gesamtdiskussion um die Telekommunikationsüberwachung und Vorratsdatenspeicherung. Die Frage der Entschädigung darf daher weder zeitlich noch sachlich von der Umsetzung des Regierungsentwurfs entkoppelt werden. Dies gilt umso mehr, als durch die Ausweitung der Verwendung der gespeicherten Daten gegenüber dem RefE zu erwarten ist, dass Datenabfragen verstärkt auf Grund von Gesetzen der Bundesländer erfolgen werden, die in der Regel keine ausreichenden Kostenregelungen enthalten. Wir erwarten aus diesem Grund, dass zeitgleich mit dem Inkrafttreten der neuen Verpflichtungen endlich die überfällige umfassende Regelung zur Entschädigung der Unternehmen geschaffen wird.

Inhalt

1 Grundsätzliche Fragen

1.1 Übergangsvorschriften, Inkrafttreten

Der RegE sieht andere Regelungen zum Inkrafttreten der Speicherverpflichtungen als noch der RefE vor. Die Verpflichtungen sollen für alle Dienste nunmehr am 1. Januar 2008 greifen. Entfallen ist somit für Internet- und E-Mail-Dienste die Verschiebung des Inkrafttretens auf den 15. März 2009. Stattdessen ist lediglich beabsichtigt, Verstöße gegen die Speicherpflichten insgesamt erst ab dem 1. Januar 2009 als Ordnungswidrigkeit zu sanktionieren.

1.1.1 Keine Ausnahme für E-Mail und Internetdaten

Die noch im RefE vorgesehene gesonderte Umsetzungsfrist bezüglich E-Mail und Internetdaten bis zum 15. März 2009 wurde im RegE kommentarlos gestrichen, weshalb auch für diesen Bereich die Umsetzungsverpflichtung nunmehr am 1. Januar 2008 in Kraft treten würde. Diese Verkürzung ist überraschend und nicht nachvollziehbar, da die Bundesrepublik Deutschland sich ausdrücklich vorbehalten hatte, die bereits in der Richtlinie angelegte Umsetzungsfrist bis März 2009 auszunutzen und eine nationale Verpflichtung zurückzustellen. Die Bundesregierung weicht damit grundlegend von den eigenen Willensbekundungen ab, nur die Minimalanforderungen der Richtlinie umsetzen und die Umsetzungsfristen ausnutzen zu wollen. Eine Vorverlegung verkennt die besonderen Umsetzungserfordernisse und -aufwände in Bezug auf Internet- und E-Mail-Dienste. Auch weil allein die Aussetzung des Sanktionssystems bis zum 1. Januar 2009 nicht geeignet ist, diese Probleme zu kompensieren, ist aus unserer Sicht ein Festhalten an der Umsetzungsfrist bis 15. März 2009 für die genannten Dienste dringend erforderlich.

Wir geben außerdem zu bedenken, dass es möglich ist, durch den Einsatz von Proxy-Servern – ggf. in Verbindung mit entsprechenden Programmen auf dem lokalen PC – sowie durch andere Konfigurationseinstellung im Browser mit minimalem Aufwand die tatsächliche IP-Adresse schon während der Telekommunikation mit der Folge abzuändern, dass an einer IP-Adresse ansetzende Ermittlungsmaßnahmen schlicht ins Leere gehen. Zum einen kann problemlos auf anonymisierende außereuropäische Proxy-Server zurückgegriffen werden, sodass auch die Regelung zu den Anonymisierungsservern nicht greift. Zum anderen befinden sich schon jetzt mehr als 100 sog. Trojaner(familien), also Schadprogramme, mit Proxy-Server-Funktionalität im Umlauf. Diese werden zur Verschleierung der eigenen Identität durch einfache Umprogrammierung des Browsers genutzt. Diese Zweifel an der Geeignetheit der Vorratsdatenspeicherung für Internet- und E-Maildaten wurden auch auf dem von der Kommission im März 2007 veranstalteten Treffen zur Umsetzung der Richtlinie zur Vorratsdaten-

speicherung detailliert an Beispielen illustriert.[2] Die angestrebten Maßnahmen sind daher aus unserer Sicht weitgehend ungeeignet, um eine bessere Kriminalitätsbekämpfung zu erreichen. Auf der anderen Seite wird durch die Vorratsdatenspeicherung von Kommunikationsdaten von – weit überwiegend – völlig Unverdächtigen massiv in deren Grundrechte eingegriffen. Wir haben aus diesem Grund Zweifel an der Verhältnismäßigkeit dieser Verpflichtungen.

1.1.2 Umsetzung bis 1. 1. 2008, Sanktionssystem ab 1. 1. 2009

Der Zeitrahmen für die einheitliche Umsetzungsfrist zum 1. Januar 2008 ist insgesamt absolut unrealistisch. Dies ist allen Beteiligten seit Vorlage des RefE bekannt. Eine Umsetzung, die mit Kosten in erheblichem Umfang verbunden ist, kann von den Unternehmen vernünftigerweise erst dann begonnen werden, wenn die maßgebenden konkreten Verpflichtungen in allen Einzelheiten ersichtlich sind. Dies ist regelmäßig erst nach Inkrafttreten, frühestens allenfalls nach Befassung aller parlamentarischen Gremien der Fall. Im laufenden Gesetzgebungsverfahren ist dies frühestens Mitte Oktober 2007 zu erwarten. Von den Unternehmen kann keinesfalls erwartet werden, sich vorbehaltlos auf den RegE einzustellen. Es ist ihnen nicht zumutbar, auf Basis eines noch nicht verabschiedeten und damit noch Änderungen unterliegenden Gesetzestextes Aktivitäten mit hohen Kosten zu veranlassen. Mit obiger Prognose zum Gesetzgebungsverfahren würden tatsächlich weniger als drei Monate für eine Umsetzung der schließlich feststehenden Vorgaben verbleiben, was – angesichts der erheblichen notwendigen Umstellungen – eine unrealistische und unverhältnismäßige Anforderung bedeutet. Die unrealistisch kurze Zeitvorstellung führt zu einem Engpass bei den wenigen auf diese Themen spezialisierten externen Entwicklungs- und Integrationsressourcen. Dies wird zusätzlich eine preistreibende Wirkung entfalten.

Der Regierungsentwurf wälzt wissentlich das vermeintlich bestehende Problem der nationalen Umsetzungsfrist auf das persönliche Risiko der verantwortlichen Vertreter der verpflichteten Unternehmen und deren Mitarbeiter ab. Denn für diese besteht ganz persönlich das Risiko, dass gegen sie als Beschuldigte ein Ermittlungsverfahren geführt wird, wenn die Strafverfolgungsbehörden der Meinung sind, dass Daten nicht oder nicht unverzüglich herausgegeben werden und deshalb wegen Strafvereitelung ermitteln. Daran ändert auch die geplante vorübergehende Aussetzung der Sanktionierbarkeit als Ordnungswidrigkeit nichts. Selbst der Verzicht auf Sanktionen vor dem 1. Januar 2009 allein ist als Hilfskonstruktion aus Sicht des BITKOM nicht ausreichend, denn es bedürfte zumindest auch einer Ausnahme von § 115 TKG. Sonst könnte die BNetzA ab Inkrafttreten des Gesetzes die Durchsetzung mit Zwangsgeld (keine Sanktion!) in Höhe von bis zu 500.000 € betreiben. In diesem Zusammenhang sei nochmals auf die vorgezeigten strafrechtlichen Rechtsfolgen einer nichtkonformen Implementierung durch die Unternehmen hingewiesen, die ebenso nicht von der Aussetzung der Sanktionierung als Ordnungswidrigkeit betroffen sind. Diese Gesamt-

[2] Summary Report – Meeting on implementation issues surrounding the Data Retention Directive (Directive 2006/24/EC) of 14 March 2007, S. 8.

problematik ist offenkundig übersehen worden, da sie auch in der Begründung des Entwurfs nicht angesprochen wird. Damit geht die Absicht des Gesetzgebers, einen Übergangszeitraum für die verpflichteten Unternehmen zu schaffen, ins Leere. Es bedarf daher dringend einer echten Aussetzung der Umsetzungspflicht für einen angemessenen Zeitraum. Wir weisen hier nochmals darauf hin, dass zumindest für die Bereiche Internet, VoIP und e-Mail eine nationale Umsetzungsfrist auch ohne weiteres richtlinienkonform möglich wäre, ohne auf unzulängliche Hilfskonstrukte zurückgreifen zu müssen.

1.2 Kosten und Entschädigung

Wie schon in unseren Stellungnahmen zum RefE angemerkt, bleibt die Entschädigungsfrage ein zentrales Problem der Vorratsdatenspeicherung. Wir betonen, dass die Schaffung einer angemessenen Entschädigungsregelung – wie in der Entwurfsbegründung angekündigt – schnellstmöglich Gestalt annehmen muss. Die jüngst begonnen Bemühungen seitens des Bundesjustizministeriums und des Bundeswirtschaftsministeriums in diese Richtung sind immerhin zu begrüßen. Dieser positive Ansatz muss nun allerdings konsequent und schnellstmöglich weiterverfolgt werden. Dabei kann es aus Sicht des BITKOM nur darum gehen, die Frage der Entschädigung für bestehende wie auch durch den jetzigen Regierungsentwurf neu hinzukommende Verpflichtungen zeitgleich mit der Neuregelung der Telekommunikationsüberwachung zu behandeln, um den betroffenen Unternehmen endlich die verfassungsrechtlich gebotene Entschädigung zu gewähren. Maßstab der Entschädigung müssen dabei die tatsächlich anfallenden Kosten sein, so dass eine Entschädigungsregelung sowohl Investitions- als auch Betriebskosten erfassen muss.

Hinzuweisen ist in diesem Zusammenhang nochmals darauf, dass auch der RegE die Zusatzkosten der Unternehmen für die Umsetzung der Speicher- und Auskunftsverpflichtungen viel zu niedrig einschätzt. Die genannte Größenordnung zwischen „einigen Tausend und mehreren Hunderttausend Euro“ verfehlt die tatsächliche Dimension um ein Vielfaches. BITKOM hat in einer jüngsten branchenweiten Grobschätzung[3] der zukünftigen Aufwände bereits dargelegt, dass die Unternehmen für die nötige Technik ca. 50 – 75 Millionen Euro werden investieren müssen. Hinzu kommen jährliche Betriebskosten in zweistelliger Millionenhöhe. Der Regierungsentwurf geht auch fehl in der Annahme, die Mehrkosten könnten einfach auf den Endkunden abgewälzt werden. Zum einen ist dies in der genannten Höhe kaum möglich. Zum anderen sind mittlerweile langfristige Vertragsbindungen mit den Endkunden marktüblich, die keine kurzfristigen Vertragsanpassungen zulassen.

Die Größenordnung dieser voraussichtlichen Kostenbelastung, die von der Bundesregierung bislang hartnäckig ignoriert wird, findet im Übrigen Bestätigung im europäi-

[3] BITKOM Stellungnahme Vorratsdatenspeicherung - Separierung & Entschädigung vom 5. April 2007, abrufbar unter http://www.bitkom.org/files/documents/BITKOM_Stellungnahme_Vorratsdatenspeicherung_-_Separierung__Entschaedigung_070405.pdf.

schen Vergleich. So wurden bei einem von der europäischen Kommission initiierten Treffen zur Umsetzung der der Richtlinie 2006/24/EG vom UK Home Office für Großbritannien Zahlen dargelegt, nach denen die Überwachungs- und Speicherpflichten Investitionskosten von ca. 50 Millionen Euro sowie jährliche Betriebskosten von bis zu 12 Millionen Euro bei den Unternehmen verursachen.[4]

2 Einzelregelungen im TKG

Neben den aufgeführten Problemlagen grundsätzlicher Natur, enthält auch der Regierungsentwurf eine Reihe problematischer Einzelregelungen. Aus Sicht der Unternehmen ist es gerade bei sensiblen Materien wie Telekommunikationsüberwachung und Vorratsdatenspeicherung von überragender Bedeutung, durch klare Formulierungen Rechtssicherheit für alle Betroffenen herbeizuführen. Aus dieser Perspektive sehen wir bei zahlreichen der jetzt vorgesehen Formulierungen noch erheblichen Nachbesserungsbedarf.

2.1 Veränderte Pflichten nach §§ 110 - 113 TKG-E

2.1.1 Ermächtigungsgrundlage TKÜV (§ 110 Überschrift sowie § 110 Abs. 2 TKG-E)

Die Änderungen der Überschrift als auch zu Abs. 2 Nr. 1 Buchstabe a) gibt die uneingeschränkte Ermächtigung zur Regelung von organisatorischen Fragen zu allgemeinen Auskünften. Dies muss auf Auskünfte zu konkret bestehenden Überwachungsmaßnahmen eingeschränkt werden.

2.1.2 Erhebung der IMEI – Umsetzungsfrist (§ 111 Abs. 1 S. 1 Nr. 5 TKG-E)

§ 111 Abs. 1 S. 1 Nr. 5 TKG-E sieht vor, dass für die Auskunftsverfahren nach §§ 112 f. TKG-E nunmehr zusätzlich die IMEI als Bestandsdatum zu erheben ist. Dies verkennt, dass zwischenzeitlich Endgeräte in großer Zahl über den vom TKG nicht verpflichteten Zubehörhandel in den Markt gebracht werden. Dies führt zu groben Wettbewerbsverzerrungen. Darüber hinaus ist bekannt, dass die IMEI bei einer Vielzahl von Endgeräten nach wie vor mit geringem Aufwand manipuliert werden kann.

[4] Summary Report – Meeting on implementation issues surrounding the Data Retention Directive (Directive 2006/24/EC) of 14 March 2007, S. 3.

Die Erhebung dürfte daher bereits bei „mittelmäßig versierten“ Kriminellen keinerlei Auswirkungen haben, da diese auf Hardware zurückgreifen werden, die aus dem Ausland oder nicht aus Bundles stammt. Gleichzeitig steigt die Gefahr, dass Unschuldige verdächtigt werden, wenn Straftäter die im Bundle gekauften Geräte - um sich nicht zu verraten oder um falsche Fährten zu legen - an unbedarfte Bürger (etwa über Internet-Auktionsplattformen) verkaufen und selbst andere Geräte nutzen.

Ferner erzeugt diese Speicherpflicht bedeutende Mehrbelastungen für viele betroffene Unternehmen. Die IMEI des Endgerätes wird heute nicht durchgängig in allen Vertriebswegen bei Vertragsabschluss erhoben. Eine solche Erhebung ist wirtschaftlich auch nicht erforderlich. Die Einführung der IMEI in den Vertriebsprozess erfordert eine technik-gestützte Erfassung, z.B. durch das Einscannen der Nummer, um die Daten überhaupt verwertbar zu machen. Eine manuelle Eingabe der 15stelligen IMEI würde zu einer erheblichen Fehlerrate führen und die Daten unbrauchbar machen. Damit werden die Unternehmen jedoch gezwungen, die technische Ausstattung auch kleiner Vertriebspartner erheblich zu verbessern, was enorme Kosten verursachen würde. Im Rahmen des Vertriebes über die Großfläche (Multimedia-Märkte, Tankstellen, etc.) würde damit zusätzlich in die Prozesse dieser Vertriebspartner eingegriffen. Dabei kommt den TK-Unternehmen jedoch zumeist kein Mitspracherecht zu.

Weiterhin schreibt § 112 TKG-E vor, dass die nach § 111 Abs. 1 TKG-E erhobenen Daten unverzüglich in Kundendateien zu speichern sind, auf welche die BNetzA Zugriff haben soll. Notwendig wäre bei den Unternehmen demzufolge eine Änderung der entsprechenden Datenbanken. Eine solche Notwendigkeit zur Änderung ergibt sich auch aus den Modifikationen in § 112 Abs. 3 Nr. 3 TKG. Allerdings sieht der Entwurf für letztere Änderungen eine zumindest einjährige Übergangsfrist vor (§ 112 Abs. 3 Satz 4 TKG-E). Für die Speicherpflicht der Daten nach § 111 Abs. 1 Nr. 5 TKG-E fehlt dagegen eine solche Übergangszeit. Die Folge ist, dass viele betroffene Unternehmen das entsprechende Datenbanksystem innerhalb kurzer Zeit mehrfach modifizieren müssen, was deutlichen Mehraufwand bedeutet und sowohl prozess- als auch systemtechnisch in dieser Zeit nicht umsetzbar ist.

2.1.3 Nacherhebung von Stammdaten (§ 111 Abs. 1 S. 4 TKG-E)

Ein weiteres Problem stellt sich mit der geplanten Verpflichtung in § 111 Abs. 1 S. 4 TKG-E: „Wird … eine Änderung bekannt, ... hat der nach Satz 1 Verpflichtete bisher noch nicht erhobene Daten zu erheben und zu speichern …“. Diese Pflicht bedeutet nach unserer Einschätzung einen massiven Mehraufwand, wenn zukünftig bei jedem Kundenkontakt, welcher die Stammdaten verändert, nachträglich die (bisher nicht vorhandene) IMEI erfasst werden müsste.

Gänzlich abzulehnen ist insofern die Erstreckung des Kundenbestandserweiterungsverbotes nach § 115 Abs. 2 S. 2 auch auf die IMEI-Erhebung. Denn es steht zu befürchten, dass eine zeitnahe Umsetzung zum einen nicht möglich ist sowie auch nicht

bei jedem Kundenkontakt sichergestellt werden kann, dass die Daten nacherhoben werden.

Insbesondere bedarf es einer Klarstellung, wie in den Fällen der Vertragsverlängerung unter Zugabe eines neuen Endgerätes zu verfahren ist. Dabei handelt es sich rechtstechnisch um einen neuen Vertragsabschluss; bei den TK-Unternehmen wird jedoch in der Regel der Kundendatensatz fortgeschrieben. Weder der Gesetzesentwurf noch die Begründung treffen dahingehend eine Aussage, ob in einem solchen Fall die ursprüngliche IMEI zu löschen ist oder ob eine Historie angelegt werden muss. In letzterem Falle würden der Industrie erhebliche zusätzliche Kosten entstehen, da weder die Kundenverwaltungssysteme noch die Beauskunftungssysteme derzeit darauf angelegt sind, historische Daten zu verwalten.

2.1.4 Automatisiertes Auskunftsverfahren und E-Mail (§ 112 Abs. 1 S. 1 TKG-E)

Gemäß § 111 Abs. 1 Satz 3 und 4 TKG-E gilt die Speicherung von Anschlusskennungen, Namen und Anschriften und Vertragsbeginnen nun auch für geschäftsmäßige E-Maildienstanbieter, soweit diese die entsprechenden Daten speichern. Problematisch ist in diesem Zusammenhang die Tatsache, dass auch das automatisierte Auskunftsverfahren nach § 112 Abs. 1 S. 1 TKG-E sich nunmehr auf diese Daten erstrecken soll. Entsprechende Datenbanken für eine solche automatisierte Beauskunftung existieren bei den Anbietern für E-Mail-Dienste noch nicht; ihre Implementation ist höchst kosten- und zeitaufwändig. Aus unserer Sicht sollten daher E-Mail-Bestandsdaten nicht dem Verfahren nach § 112 TKG unterliegen, um die entsprechende hohe und unverhältnismäßige Kostenbelastung zu vermeiden. Im Übrigen gehen wir davon aus, dass auch für E-Mail-Bestandsdaten § 112 Abs. 3 S. 3 und 4 TKG einschlägig sind, so dass die immer noch ausstehende technische Richtlinie hierzu Vorgaben enthalten muss.

2.2 Speicherungspflichten nach § 113a TKG-E („Vorratsdatenspeicherung“)

Hinsichtlich der Speicherverpflichtung gibt es begrüßenswerte Änderungen gegenüber dem RefE. So ist der Kreis der zur Speicherung Verpflichteten enger gezogen worden und beinhaltet nicht mehr denjenigen, der an der Erbringung von TK-Leistungen lediglich "mitwirkt". Die ausdrückliche Klarstellung in § 113a Abs. 1 TKG-E, dass die Speicherung auch im EU-Ausland stattfinden darf, ist ebenfalls zu begrüßen.

Abseits dieser positiven Aspekte sehen wir indes weiteren Nachbesserungsbedarf. Für die betroffenen Unternehmen ist es von außerordentlichem Interesse, dass sie den Umfang ihrer Speicherverpflichtungen unzweideutig erkennen können. Ansonsten drohen unkalkulierbare Mehrkosten, aber auch vermehrte Streitigkeiten mit den auskunftsersuchenden Behörden, wenn diese unklare Normen im Sinne einer Speicher-

pflicht für bestimmte Datentypen interpretieren. Hier ist nicht zuletzt auch das Interesse der im Einzelfall jeweils betroffenen Bürger an klaren Regelungen zu berücksichtigen. In diesem Zusammenhang ist auch die gegenüber dem Referentenentwurf vorgenommene Verkürzung der amtlichen Überschrift des § 113a TKG-E zu kritisieren. Die neue Überschrift lässt es an der erforderlichen Klarheit fehlen, da Gegenstand dieses Paragrafen die Speicherungsverpflichtungen in Bezug auf Verkehrsdaten sind. Es sollte daher wieder die ursprüngliche Überschrift aus dem Referentenentwurf „Speicherungspflichten für Verkehrsdaten“ verwendet werden.

Bei der Speicherungspflicht halten wir außerdem nach wie vor einen Zusatz für erforderlich, der klarstellt, dass die im Folgenden aufgeführten Daten nur dann zu speichern sind, sofern sie dem Diensteanbieter auch zur Verfügung stehen. Dieser Zusatz trägt dem Umstand Rechnung, dass dem Diensteanbieter nicht immer alle der aufgeführten Daten bekannt sind. Auch die zugrundeliegende Richtlinie 2006/24/EG geht in Erwägungsgrund 23 von einem solchen Verständnis aus. Der Regierungsentwurf hält diese Einschränkung ausweislich der Begründung bereits über § 113a Abs. 1 TKG-E für realisiert. Wir regen jedoch an, dies weiter klarzustellen, indem zumindest auch in Abs. 2 – 4 noch einmal „soweit erzeugt oder verarbeitet“ ergänzt wird. Sonst klingen diese Absätze isoliert so, als bestünde eine absolute Speicherpflicht. So werden etwa die Aktivierungsdaten bei im Voraus gezahlten Diensten heute z.B. nur zum Teil erzeugt, nämlich nur dann, wenn dies für den Vertrag notwendig ist (z.B. Datum). Standortdaten werden nicht hierbei erzeugt. Die IMEI-Nummern der Geräte liegen z.B. bei Prepaid-Gesprächen gar nicht vor.

2.2.1 Anbieter ohne eigene TK-Anlagen (§ 113a Abs. 1 S. 2 TKG-E)

Auch wenn die Entwurfsverfasser dies sicherlich nicht intendiert haben, so muss auf jeden Fall gesetzlich eindeutig klargestellt sein, dass Anbieter ohne eigene TK-Anlagen auch weiterhin ihre Speicherpflicht delegieren dürfen. Nach dem jetzigen, gegenüber dem Referentenentwurf veränderten, Wortlaut des § 113 Abs. 1 S. 2 TKG-E müssten Anbieter ohne eigene TK-Anlagen doch wieder eigene Daten selbst speichern, weil sie diese zumindest verarbeiten. Dies stünde im Widerspruch zu dem Grundsatz, dass die Daten nicht redundant bei zwei Anbietern gespeichert werden sollen und widerspricht damit dem Grundsatz der Datensparsamkeit.

2.2.2 Angabe der Zeitzone (§ 113a Abs. 2 Nr. 2)

Bei der in Absatz 2 Nr. 2 vorgesehenen Verpflichtung kann es nur um „systemseitige“ bzw. „netzseitige“ Zeitpunkte handeln, nicht um die Zeitpunkte aus Kundensicht. Dies sollte auch im Gesetzestext deutlich werden.

Vorschlag:

„2. den Beginn und das Ende der Verbindung nach system- bzw. netzseitig erfasstem Datum und Uhrzeit unter Angabe der zugrundeliegenden Zeitzone.“

2.2.3 IMSI / IMEI (§ 113a Abs. 2 S. 1 Nr. 4 a), b) TKG-E)

Der Gesetzestext lässt immer noch offen, was mit "Internationale Kennung … des Anschlusses" gemeint ist. "Internationale Kennung" ist kein fest definierter, sondern ein sehr interpretationsfähiger Begriff. Die Begründung erst macht klar, dass die Vorschriften auf die Speicherung der IMSI bzw. IMEI abzielen. Dies sollte durch einen Klammerzusatz klargestellt werden, damit Missverständnisse in der Praxis ausgeschlossen werden können.

Vorschlag:

„a) die internationale Kennung für mobile Teilnehmer für den anrufenden und den angerufenen Anschluss (IMSI),

b) die internationale Kennung des anrufenden und des angerufenen Endgeräts (IMEI),“

2.2.4 Speicherung von Standortkennungen (§ 113a Abs. 2 S. 1 Nr. 4c TKG-E)

Wir möchten außerdem erneut auf eine Diskrepanz zwischen den Regelungen des § 98 Abs. 2 TKG und § 113a TKG-E hinweisen. Die Regelung betrifft den Umgang mit Standortdaten im Mobilfunk. Danach können Endkunden der Verarbeitung ihrer Standortdaten bereits bei der Herstellung von Kommunikationsverbindungen widersprechen. Es ist aber fraglich, wie ein solcher Widerspruch mit der Speicherpflicht nach § 113a Abs. 2 Nr. 4 TKG-E in Einklang zu bringen ist. Es bleibt damit unklar, ob diese Daten im Falle eines Widerspruchs zu speichern sind. Der Sinn des Gesetzes spricht zwar dafür, dass Standortdaten (d.h. die geographischen Daten der Antennen-Standorte) immer, d.h. im Zweifel auch entgegen dem Widerspruch eines Endkunden, gespeichert und beauskunftet werden müssen. Dies sollte ggf. aber klarer herausgestellt werden, um Rechtssicherheit herzustellen.

2.2.5 SMS, MMS und ähnliche Dienste (§ 113a Abs. 2 S. 2 Hs. 1 TKG-E)

Die vorliegende Fassung lautet: "Satz 1 gilt entsprechend bei der Übermittlung einer Kurz-, Multimedia- oder ähnlichen Nachricht". Diese Begriffe sind ebenfalls nicht ein-

deutig definiert. Darunter könnten z.B. auch Instant Messages verstanden werden, falls diese über einen "Internet-Telefondienst" übertragen werden. Das Telekommunikationsunternehmen unterstützt diese z.B. durch das Angebot einer reinen Datenübertragung, nicht aber durch einen separaten 'Nachrichtendienst'. Ohne den Hinweis bzgl. der tatsächlich zu speichernden Verkehrsdaten könnte daraus eine den sonstigen Bestimmungen widersprechende Pflicht hergeleitet werden, Absender und Empfänger zu speichern, obwohl dies Kommunikationsinhalte und keine Verkehrsdaten wären. Um Missverständnissen in der Praxis vorzubeugen, sollten daher nur die Begriffe „SMS“ und „MMS“ verwendet werden.

Vorschlag:

"Satz 1 gilt entsprechend bei der Übermittlung einer SMS-, MMS- oder ähnlichen Nachricht."

2.2.6 Kennung des elektronischen Postfachs (§ 113a Absatz 3 Nr. 1 - 3 TKG-E)

Schließlich ist auch die "Kennung des elektronischen Postfachs" kein definierter, sondern ein sehr interpretationsfähiger Begriff, der z.B. im Sinne von „Zugangskennung“ oder „Passwort“ ausgelegt werden könnte. Erst aus der Gesetzesbegründung kann entnommen werden, dass es sich in diesem Zusammenhang um die E-Mail-Adresse handeln soll. Auch dies sollte schon im Gesetzestext klargestellt werden.

Vorschlag:

„1. bei Versendung einer Nachricht die E-Mail-Adresse, die Benutzerkennung und die Internetpotokoll-Adresse des Absenders sowie die E-Mail-Adresse jedes Empfängers der Nachricht,

2. bei Eingang einer Nachricht die E-Mail-Adresse des Absenders und des Empfängers der Nachricht sowie die Internetprotokoll-Adresse der absendenden Telekommunikationsanlage,

3. bei Abruf einer Nachricht die E-Mail-Adresse, die Benutzerkennung und die Internetprotokoll-Adresse des Abrufenden sowie die E-Mail-Adresse des Absenders der Nachricht,“

2.2.7 Daten von erfolglosen Verbindungsversuchen (§ 113 a Abs. 5 TKG-E)

Zu begrüßen ist die in Absatz 5 vorgenommene und in der Begründung erläuterte Klarstellung, dass Daten von erfolglosen Verbindungsversuchen nur dann der Pflicht nach § 113a TKG-E unterfallen, wenn diese sowieso vom Anbieter gespeichert und protokolliert werden. Allerdings wäre es wünschenswert, den derzeit lediglich in der Begründung vermerkten Hinweis, dass unter keinen Umständen eine Speicherungspflicht bei bereits gescheitertem Verbindungsaufbau besteht, in den Normwortlaut zu integrieren.

2.2.8 Änderung zu speichernder Daten (§ 113a Abs. 6 TKG-E)

Es sollte klargestellt werden, welche Daten in § 113a Abs. 6 TKG-E adressiert werden. Unklar bleibt, ob sich die Bestimmung ausschließlich auf Verkehrsdaten oder ggf. auch alle anderen Daten bezieht. Die amtliche Überschrift von § 113a TKG-E legt immerhin ein weites Verständnis nahe. Letzteres würde aber einen bedeutenden Aufwand bedeuten. Denn dann müssten alle Systeme, die Stammdaten verarbeiten, jeweils für alle in § 113a TKG-E aufgelisteten Daten komplette Historien erzeugen und vorhalten. Dies würde nicht zuletzt auch die Auskunfteien-Schnittstellen der Ermittlungsbehörden, welche auf die Daten zugreifen, betreffen. Über das eigentliche Ziel, lediglich Anonymisierungen zu vermeiden, geht der geplante Absatz jedenfalls weit hinaus.

2.2.9 Geografische Zusatzinformationen (§ 113a Abs. 7 TKG-E)

Nach Abs. 7 sollen die Mobilfunkbetreiber auch die Daten zur geografischen Lage der die Funkzelle versorgenden Funkantennen sowie deren Hauptstrahlrichtung vorhalten. Eine solche Pflicht findet sich in der Richtlinie nicht wieder; der Entwurf geht somit entgegen der Ankündigung der Bundesregierung über die Anforderungen der Richtlinie hinaus. Tatsächlich bedeutet die Regelung einen enormen Zeit- und Kostenaufwand und stellt eine unverhältnismäßige Mehrbelastung der Mobilfunkunternehmen. Da die Verpflichtung nicht aus der Richtlinie stammt und damit nicht den nationalen Umsetzungsfristen unterfällt, sollte den Unternehmen zumindest eine angemessene Umsetzungsfrist eingeräumt werden.

2.3 Verwendung der gespeicherten Daten (113b TKG-E)

2.3.1 Erweiterung: Gefahrenabwehr und Nachrichtendienste

Wir beobachten mit Sorge, dass sich der Verwendungszweck der Daten erweitert. So sollen sie nach dem RegE nicht nur für Zwecke der Strafverfolgung, sondern nunmehr auch für die Gefahrenabwehr und die Aufgabenerfüllung der Geheimdienste zur Verfügung stehen. Für die verpflichteten Unternehmen bedeutet dies nicht nur eine Erweiterung des Kreises der berechtigten Stellen, sondern damit einhergehend auch eine Zunahme der Auskunftsanordnungen. Außerdem ist eine Begrenzung des Speicherzwecks schon aus datenschutzrechtlicher Sicht geboten. Der Regierungsentwurf macht demgegenüber nicht hinreichend deutlich, warum die Erweiterung erforderlich sein soll. Klassischerweise sind Verkehrsdaten ein Hilfsmittel für Ermittlungen im Rahmen der Strafverfolgung. Insbesondere im Bereich der Gefahrenabwehr haben wir deshalb Zweifel, wie bis zu sechs Monate alte Verkehrsdaten bei der Abwehr künftig drohender Gefahren nützen können. Auch die zugrundeliegende europäische Richtlinie 2006/24/EG sieht nach Art. 1 eine Speicherung ausschließlich zum „Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten“ vor: auch hier geht also der Entwurf über die Vorgaben der Richtlinie hinaus.

Die Gesetzesbegründung sieht insoweit zu Recht ein Problem darin, dass ein Datenzugriff der Gefahrenabwehrbehörden und der Nachrichtendienste unverhältnismäßig sein könnte. Daher soll sich die Verwendungsbefugnis gemäß § 113b Nr. 3 TKG-E auch auf die Abwehr erheblicher Gefahren beschränken. Neben der praktischen Relevanz dieser Einschränkung bleibt nach unserer Einschätzung aber höchst zweifelhaft, ob sie im Sinne der Verhältnismäßigkeit ausreichend ist.

2.3.2 keine Verwendung für andere Zwecke (§ 113b Abs. 1, S. 1, 2. HS.TKG-E)

§ 113b Abs. 1, S. 1, 2. HS.TKG-E legt fest, dass eine Verwendung für andere als die in der Vorschrift angegebenen Zwecke durch den Verpflichteten nicht zulässig sein soll. Der Referentenentwurf hatte hier noch die Verwendung für Zwecke der Datenschutzkontrolle, der Datensicherung und zur Sicherstellung eines ordnungsgemäßen Betriebs für zulässig erklärt. Die Begründung des Regierungsentwurfs schweigt zu der jetzt vorgenommenen Beschränkung. Wir halten eine begrenzte Ermächtigung zur Verwendung der Daten zu Zwecken der Missbrauchsbekämpfung in Anlehnung an § 100 Abs. 3 TKG für sinnvoll und notwendig. Insoweit regen wir zumindest eine Klarstellung an, dass § 100 Abs. 3 TKG von § 113b Abs. 1 S. 1, 2. HS unberührt bleibt, unter den dort genannten Voraussetzungen also auch auf die nach § 113a TKG-E gespeicherten Daten zurückgegriffen werden darf.

Vorschlag:

„; für andere Zwecke darf er die Daten nicht verwenden, eine mögliche Nutzung gemäß § 100 Abs. 3 TKG bleibt hiervon unberührt.“

3 Einzeländerungen der StPO

Eine im Ansatz begrüßenswerte, jedoch nicht ausreichende Änderung gegenüber dem RefE stellt die Zweimonatsfrist in § 100b Abs. 1 S. 4 StPO-E für Anordnungsverlängerungen dar. Diese ist zwar erheblich praxistauglicher, führt jedoch immer noch zu erheblichen Mehraufwänden gegenüber der aktuellen Rechtslage. Auch besteht an zahlreichen anderen Passagen des Entwurfs noch erheblicher Verbesserungsbedarf.

3.1 Voraussetzungen der Telekommunikationsüberwachung (§ 100a StPO-E)

Die Einschränkung in § 100a Abs. 1 Nr. 2 StPO, wonach die Tat auch im Einzelfall schwer wiegen muss, ist grundsätzlich begrüßenswert. Realistischerweise wird sie aber kaum zu einer angemessenen Begrenzung der Anzahl der Überwachungen führen. Bereits heute müssen Staatsanwaltschaft und Gericht die Verhältnismäßigkeit der Maßnahme prüfen. In der Praxis kommt man jedoch nicht um die Feststellung herum, dass hier großzügig verfahren wird. Nicht selten lässt sich dies auf unvollständige Information der Entscheidungsträger durch die ermittelnde Behörde, mangelndes technisches Wissen, kombiniert mit einer hohen Überlastung bei den Staatsanwaltschaften und Gerichten zurückführen. An diesen praktischen Schwachpunkten müsste neben einer Einengung des Gesetzeswortlauts angesetzt werden.

Die Erweiterung des Straftatenkatalogs insbesondere um die Betrugstatbestände wird zu einer deutlichen Erhöhung der Anzahl der Überwachungen führen und so die Kosten weiter erhöhen.

Eine Änderung gegenüber dem RefE enthält außerdem § 100a Abs. 4 StPO-E. Hier fehlt nunmehr die Vorgabe, dass bei Zweifeln über die Zugehörigkeit von Erkenntnissen zum Kernbereich privater Lebensgestaltung unverzüglich eine bindende Gerichtsentscheidung einzuholen ist. Dadurch wird der Rechtsschutz der Betroffenen in bedenklicher Weise verkürzt.

3.2 Verfahren für TKÜ (§ 100b StPO-E)

3.2.1 Staatsanwaltschaftliche Anordnung (§ 100b Abs. 1 Satz 3 StPO-E)

Der RegE lässt im Gegensatz zum RefE die Verwertung von Daten, die im Rahmen einer staatsanwaltlichen Eilanordnung erlangt wurden auch dann zu, wenn keine richterliche Bestätigung erfolgt und „Gefahr in Verzug“ vorliegt. Damit wird eine generelle Freigabe für alle staatsanwaltlichen Eilanordnungen erteilt, denn diese dürfen ja gerade erst unter dieser Voraussetzung ergehen – faktisch bedeutet dies eine vollständige Unterhöhlung des Richtervorbehalts, die dringend wieder beseitigt werden muss.

3.2.2 Bestandteile der Anordnung (§ 100b Abs. 2 StPO-E)

Auch der vorliegende Gesetzentwurf will die Anordnung einer Maßnahme schon dann ermöglichen, wenn lediglich die Endgerätekennung eines Mobiltelefons (IMEI) bekannt ist und „diese allein dem zu überwachenden Endgerät zuzuordnen ist“. Die Prüfung, ob eine IMEI mehrfach im Netz eingebucht war oder ist und damit als gefälscht gelten kann, wird so im Zweifel an die verpflichteten Unternehmen delegiert. Abgesehen von dem beispiellosen Prüfaufwand besteht immer noch die Gefahr, dass unbeteiligte Dritte ins Visier der Maßnahme geraten, nämlich dann, wenn ein Täter zufällig oder absichtlich die IMEI eines anderen nutzt, beide Endgeräte aber nicht gleichzeitig oder in unterschiedlichen Netzen eingebucht sind. Niemand kann sicherstellen, dass die Maßnahme in diesen Fällen gegenüber dem tatsächlich zu überwachenden Endgerät durchgeführt. Dadurch geraten unnötig Dritte in Gefahr. Außerdem wird der gesamte Prüfungsaufwand der Validität eines grundsätzlich zweifelhaften Datums unbillig auf die verpflichteten Unternehmen abgewälzt. Konsequenterweise muss § 100b Abs. 2 Satz 2 Nr. 2 StPO-E ersatzlos gestrichen werden.

Wie schon beim Referentenentwurf kritisieren wir außerdem, dass in der Entscheidungsformel Name und Anschrift nur noch „soweit möglich“ angegeben werden sollen, d.h., wenn sie bekannt sind. Mit dieser Unschärfe nimmt der Gesetzgeber die Gefahr in Kauf, dass unbeteiligte Personen einer Telefonüberwachung unterworfen werden. Im Hinblick auf den hohen verfassungsrechtlichen Stellenwert des Fernmeldegeheimnisses scheint diese Relativierung nicht angemessen.

Eine sinnvolle Ergänzung bildet dagegen die neu hinzugekommene Benennung des Endzeitpunkts der Maßnahme in § 100b Abs. 2 Nr. 3 StPO-E.

3.2.3 Überwachungsbezogene Auskünfte (§ 100 b Abs. 3 StPO-E)

Die Formulierung „ ... und die erforderlichen Auskünfte zu erteilen“ ist unpräzise und überflüssig und eröffnet so Spielraum für fruchtlose Diskussionen. Welche Informationen im Rahmen einer TKÜ-Maßnahme technisch zu liefern sind, spezifiziert die TKÜV. Eine allgemeine Verpflichtung zu „erforderlichen Auskünften“ sollte daher entfallen.

3.3 Verkehrsdatenauskunft (§ 100g StPO-E) bzw. Auskunft unter Verwendung von Verkehrsdaten

Nachdrücklich müssen wir der Aussage der Entwurfsbegründung widersprechen, dass es für die Auskunft der hinter einer dynamischen IP-Adresse stehenden Person keines richterlichen Beschlusses gemäß den §§ 100g/h StPO bedürfe, da es sich nicht um eine Auskunft zu Verkehrsdaten handele. Entsprechend geht die Begründung unzutreffend davon aus, die Abfrage betreffe schließlich nur den Namen und die Anschrift des Nutzers, mithin also Bestandsdaten. Dieser Auffassung treten wir entschieden entgegen. Entscheidend ist nach § 88 Abs. 2 TKG die einer Übermittlung denknotwendig vorgelagerte *Erhebung* von Daten durch den TK-Dienstleister; diese Erhebung bezieht sich nach § 88 Abs. 1 TKG auch auf die Person, die an einem Telekommunikationsvorgang beteiligt war. Mit der Auskunft zur Person hinter einer dynamischen IP-Adresse wird immer automatisch bestätigt, dass die angefragte Person aus der Bestandsdatenbank, zu dem Datum X und der Uhrzeit Y online und somit an einem Fernmeldevorgang beteiligt war. Diese Information fällt somit unter den Schutzbereich des § 88 TKG, weshalb ihre Abfrage auch einen richterlichen Beschluss erfordert. Eine Bestandsdatenabfrage liegt immer nur dann vor, wenn der Provider die Auskunft allein auf Daten stützen, kann die bei Ihm dauerhaft im Bestand gespeichert sind. Von einer Verbindungsdatenanfrage ist hingegen dann auszugehen, wenn zur Auskunftserteilung auf Daten zugegriffen werden muss, die erst bei der Erbringung und Bereitstellung von Telekommunikationsleistungen anfallen. So liegt der Fall bei einer Auskunft zu dynamischen IP Adressen. Diese werden anders als Telefonnummern eben nicht dauerhaft im Bestand des Providers gespeichert. Bei der Auskunftserteilung muss auf diese Daten, die einen Rückschluss auf den Zeitpunkt der Beteiligung an einem Telekommunikationsvorgang erlauben, zurückgegriffen werden. Noch deutlicher wird dies, wenn die eigene Telekommunikationsinfrastruktur durch den Kunden eines Wettbewerbers genutzt worden ist. In einem solchen Fall kann der Betreiber der TK-Infrastruktur überhaupt keine Bestandsdaten erheben, weil er kein Vertragsverhältnis mit dem Kunden des Wettbewerbers hat. Er kann nur aus den ihm vorliegenden Verbindungsdaten erkennen, dass ein Kunde eines Wettbewerbers seine Infrastruktur genutzt hat.

Die Gesetzesbegründung ist weiterhin unzutreffend, soweit angeführt wird, dass es mittlerweile eine gefestigte Rechtsprechung zur Streitfrage gebe, ob eine Auskunft zur Person hinter einer dynamischen IP Adresse eine Bestandsdatenabfrage oder Ver-

bindungsdatenanfrage sei. Dem ist nicht so. Wir verweisen an dieser Stelle ausdrücklich auf mehrere Urteile, die allesamt ausdrücklich bestätigen, dass es sich bei einer solchen Anfrage um eine Anfrage handelt, die dem grundgesetzlichen geschützten Bereich des Fernmeldegeheimnisses unterfällt (vgl. LG Ulm, MMR 2005, 191; 31 QS 65/04, LG Bonn; 6 QS 100/05, LG Braunschweig; 46 QS 138/04, LG Braunschweig; 6 Qs 100/05, LG Hannover; 2 QS 173/04, LG Memmingen; 2 Qs 173/04, LG Lüneburg; 26 Qs 294/06, LG München I; 8 Qs 38/05, 931, GS AG Frankfurt am Main; 3330 JS 213527/05, 931 GS AG Frankfurt am Main; GS 57/05, AG Dessau), sowie ganz überwiegend das juristische Schrifttum.

Wenn sich der Regierungsentwurf nunmehr an der beschriebenen unzutreffenden Auffassung orientiert, wird der Schutz von Verkehrsdaten im Ergebnis deutlich reduziert. Denn bei der überwiegenden Anzahl der Auskunftsersuchen zu Internetdaten handelt es sich um Anfragen zur Person hinter einer dynamischen IP-Adresse. Diese Daten werden künftig für alle Internetnutzer 180 Tage auf Vorrat gespeichert und nach dem Willen dieses Entwurfs zukünftig auch noch ohne richterliche Kontrolle verfügbar sein. In der Gesamtschau wird mithin der Zugriff auf die Daten der Vorratsdatenspeicherung dramatisch ausgeweitet und vereinfacht.

3.4 Straftaten mittels Telekommunikation (§ 100g Abs. 1 Nr. 2 StPO-E)

Leider ermöglicht der Regierungsentwurf auch weiterhin die Erhebung von Verkehrsdaten, wenn lediglich eine Straftat vorliegt, die mittels Telekommunikation begangen wurde. Meist handelt es sich dabei um unerhebliche Straftaten. Die zusätzlichen Eingriffsvoraussetzungen nach Abs. 1 Satz 2 sollen den Fokus zwar auf solche Taten lenken, deren Bedeutung „in einem angemessenen Verhältnis“ zu einer Verkehrsdatenerhebung steht. Dieses Kriterium ist jedoch zu weich und beschränkt die Anordnungsbefugnis daher nicht wirksam. Wir fordern die Streichung des Tatbestands.

3.5 Echtzeit-Standortdaten (§ 100g Abs. 1 S. 3 StPO-E)

Die Formulierung in Satz 3 (Echtzeit-Standortdaten) unterscheidet nicht zwischen der Erhebung durch die Polizeibehörden und durch die Verpflichteten. Eine solche Unterscheidung ist jedoch wichtig. Ortungen in Echtzeit werden derzeit auf Grundlage der §§ 100a, b StPO vorgenommen. Dies entspricht zum einen den gesetzlichen Voraussetzungen, da eine Echtzeit-Ortung nur aufgrund eines aktuellen Telekommunikationsvorgangs möglich ist und somit Aufschluss über das aktuelle Bestehen einer Verbindung gibt. Ähnliches gilt für eine Echtzeitüberwachung von Verkehrsdaten: Auch sie ist technisch wie eine TKÜ ausgestaltet und sollte – anders als die Begründung ausführt – nur nach §§ 100a, b StPO erfolgen können.

3.6 Verweis auf TKÜV bei Verkehrsdatenauskunft (§ 100g Abs. 2 S. 1 StPO-E)

Während für eine Echtzeit-Ortung eine Anknüpfung an die §§ 100a, b StPO aus organisatorischen und technischen Gründen erforderlich ist, halten wir die generelle Verweisung in § 100g Abs. 2 Satz 1 auf § 100b Abs. 1 bis 4 Satz 1 StPO-E für bedenklich. Durch sie würde die TKÜV auch für Auskunftsersuchen nach § 100g StPO anwendbar (§ 100b Abs. 3 StPO), was die Verpflichtungen der Telekommunikationsdienstleister umfassend erweitern würde. Im Extremfall kann dies bedeuten, dass für eine Auskunftserteilung über ein einfaches Beleidigungsdelikt, welches mittels einer Telekommunikations-Endeinrichtung begangen wurde, wegen § 12 TKÜV ein durchgehender Bereitschaftsdienst vorgehalten werden müsste. Denn eine Begrenzung der TKÜV auf Maßnahmen zur Überwachung der Telekommunikation ist dieser nicht durchgängig zu entnehmen. Gerade bei auf Vorrat gesammelten Daten würde das ohnehin nur wenig Sinn machen. Die Anwendbarkeit der TKÜV sollte daher auf die Fälle des Abs. 3 Satz 3 beschränkt sein.

3.7 Bestimmtheitserfordernisse bei Verkehrsdatenerhebung (§ 100g Abs. 2 S. 2 StPO-E)

Soweit bei Straftaten von erheblicher Bedeutung eine räumlich und zeitlich hinreichend bestimmte Bezeichnung der Telekommunikation genügen sollen (§ 100g Abs. 2 S. 2 StPO-E), bringt diese Formulierung viele praktische Probleme mit sich: Gerade in letzter Zeit erreichen die Telekommunikationsunternehmen vage gefasste Auskunftsersuchen, in denen die zeitliche und räumliche Eingrenzung z.B. durch Übersendung eines Auszugs aus dem Fahrplan der Deutschen Bahn AG mit Abfahrts- und Ankunftszeiten oder durch Autobahnabschnitte unter Angabe der Fahrzeit geschieht (Beispiel: „Anordnung betrifft Mobilfunkverkehr im Raum Hannover über den Zeitraum von drei Monaten“). Solche Auskunftsersuchen erwecken den Anschein, als sei die Erhebung von Telekommunikationsdaten erster Ermittlungsansatz und nicht bereits Resultat von durch Vorermittlungen erhärteten Verdachtsmomenten. Bereits die Vorermittlungen werden damit auf die betroffenen Telekommunikationsunternehmen abgewälzt, bei denen sie einen beträchtlichen Aufwand verursachen und erhebliche Ressourcen über einen langen Zeitraum binden. Wir halten daher die Einfügung zeitlicher und örtlicher Obergrenzen für notwendig, um den Umfang der Anordnungen auf ein vernünftiges Maß zu beschränken.

3.8 Einsatz IMSI-Catcher (§ 100i StPO-E)

Gegenüber dem Referentenentwurf erweitert der Regierungsentwurf die Eingriffsvoraussetzungen in doppelter Hinsicht:

Zum einen lässt § 100i Abs. 1 StPO-E nun auch andere als die Katalogstraftaten gemäß §100a Abs. 2 StPO-E zur Anwendung der Maßnahme ausreichen. Dies kommt durch die neue Formulierung „*insbesondere* eine in § 100a Abs. 2 bezeichnete Straftat“ zum Ausdruck. Zum anderen ist die Standortbestimmung nicht mehr auf Maßnahmen nach § 127 Abs. 2 StPO beschränkt. Weiterhin ist die eingeschränkte Erlaubnis der Standortbestimmung sowie der Erfassung von Daten Dritter als *ultima ratio* (vormals § 100i Abs. 3 StPO-RefE) entfallen. Für diese Erweiterungen der Eingriffsbefugnis liefert der Entwurf keine hinreichende Begründung. Es spricht auch nichts dafür, die Eingriffsvoraussetzungen eines derart intensiven Eingriffs weiter zu lockern. Wir empfehlen daher dringend, wieder zur ursprünglichen Fassung des Referentenentwurfs zurückzukehren.

Unverständlich ist weiterhin die überaus großzügige Befristung der Anordnung zum Einsatz eines IMSI-Catchers gemäß § 100i Abs. 3 Sätze 2 und 3 StPO-E. Der Regierungsentwurf sieht diesbezüglich vor, dass eine Maßnahme für die Dauer von 6 Monaten angeordnet und jeweils bis zu 6 weiteren Monaten verlängert werden darf. Dies steht in krassem Kontrast zu der Verkürzung der Anordnungsfristen, die der Regierungsentwurf gleichzeitig in Bezug auf die TK-Überwachung vornimmt (Erstanordnung höchstens 2 Monate, Verlängerung jeweils bis zu 2 Monate). Hier zeigt sich ein Missverhältnis in den eingriffsbeschränkenden Bedingungen, zumal der Einsatz des IMSI-Catchers schon aufgrund der regelmäßigen Betroffenheit unbeteiligter Dritter als das einschneidendere Mittel zu bewerten ist. Die Anordnungsfristen sollten daher mindestens an das bei der TK-Überwachung gefundene Maß angeglichen werden.

Da die eingesetzte Technik Auswirkungen auf den Betrieb der Mobilfunknetze hat, muss schließlich dringend eine Berichtspflicht entsprechend § 100b Abs. 5 StPO-E aufgenommen werden.