

Stellungnahme

Berlin, den 13. Juli 2009

eco nimmt gerne die Gelegenheit wahr, zu den im Rahmen der Verfassungsbeschwerden 1 BvR 256/08, 263/08 und 586/08 vom Bundesverfassungsgericht gestellten Fragen Stellung zu nehmen.

I. Allgemeine Anmerkungen

Zur Einhegung und rechtsstaatlichen Kontrolle erachten wir eine konsequente Anwendung und Beachtung des Erfordernisses einer richterlichen Anordnung für den Zugriff auf die im Rahmen des § 113a TKG gespeicherten Daten aufgrund der damit einhergehenden Eingriffe in das Fernmeldegeheimnis für zwingend erforderlich. Dies sollte insbesondere für Auskunftersuchen gelten, bei denen die erforderlichen Auskünfte nur unter Verwendung von Verkehrsdaten erteilt werden können (§ 113b S. 1 Hs. 2 i.V.m. § 113 TKG).

Bereits zum gegenwärtigen Zeitpunkt ist festzustellen, dass es Bestrebungen gibt sowohl hinsichtlich einer Ausweitung der im Rahmen des § 113a TKG zu speichernden Datenarten (keine Beschränkung auf Telekommunikationsdienste, sondern Ausweitung auf Dienste der Informationsgesellschaft im Sinne der EU-Richtlinien) als auch hinsichtlich einer Erweiterung des Kreises der berechtigten Stellen, die einen Zu- und Rückgriff auf die gespeicherten Daten erhalten sollen.

Insgesamt hat die Einführung der anlass- und verdachtsunabhängigen Speicherung von Verkehrsdaten bei den Nutzern von Telekommunikationsdiensten aber insbesondere auch bei den TK-Unternehmen zu einer erheblichen Rechtsunsicherheit geführt. Mangels klarer Vorgaben und unterschiedlicher Auslegung besteht Unklarheit darüber, wer zum Kreis der Verpflichteten gehört und welche Datenarten von der Speicherungsverpflichtung erfasst sind. Bedauerlicherweise hat auch die von der Bundesnetzagentur zu erarbeitende Technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation (TR-TKÜ) nicht zu einer Klärung beigetragen. Für die betroffenen Unternehmen wirkt sich die bestehende Rechtsunsicherheit besonders gravierend aus. Die Unsicherheit über die Feststellung, ob das Unternehmen beziehungsweise ein angebotener Dienst der Pflicht zur Vorratsdatenspeicherung unterliegt, trägt der Anbieter. Einerseits begeht er eine Ordnungswidrigkeit, die mit einer Geldbuße bis zu 500.000 EUR geahndet werden kann, wenn er nicht auf Vorrat speichert, obwohl er hierzu verpflichtet ist (§ 149 Abs. 1 Nr. 36 TKG). Andererseits begeht er eine Ordnungswidrigkeit, die mit einer Geldbuße bis zu 300.000 EUR geahndet werden kann, wenn er auf Vorrat speichert, obwohl er nicht hierzu verpflichtet ist (§ 149 Abs. 1 Nr. 17 TKG). Nicht zuletzt vor dem Hin-

tergrund dieser Sanktionsmöglichkeiten begegnet die Bestimmtheit des Anwendungsbereichs der Vorschriften zur Vorratsdatenspeicherung verfassungsrechtlichen Bedenken.

Abschließend erlauben wir uns den Hinweis darauf, dass die Frage nach einer Erstattung der Anschaffungs- und Betriebskosten, die im Zusammenhang mit der Einführung der anlass- und verdachtsunabhängigen Speicherung von Verkehrsdaten anfallen, nach wie vor ungeklärt ist. Aus verfassungsrechtlichen Gründen muss eine Erstattung der Anschaffungs- und Betriebskosten für die Heranziehung der TK-Unternehmen erfolgen. Bei der Sicherheitspolitik, der Gewährleistung der öffentlichen Sicherheit und der Strafverfolgung handelt es sich um originär staatliche Aufgaben, die der Staat grundsätzlich aus Mitteln des öffentlichen Haushalts zu bestreiten hat. Die Indienstnahme Privater für originär staatliche Aufgaben ist zu entschädigen, anderenfalls ist die Verpflichtung zur Vorratsdatenspeicherung, zur Ermöglichung der Überwachung der Telekommunikation und zur Erteilung von Auskünften unverhältnismäßig. Der Gesetzgeber ist daher aufgefordert, zur Schaffung verfassungsgemäßer Zustände eine Erstattung der Anschaffungs- und Betriebskosten vorzusehen.

II. Fragenkatalog des Bundesverfassungsgerichts zu den Verfassungsbeschwerden 1 BvR 256/08, 263/08 und 586/08

Zu den Verkehrsdaten im Allgemeinen:

Frage 1: Welche Verkehrsdaten fallen im Rahmen der Telekommunikation an, werden aber von § 113a TKG nicht erfasst?

Nach der Legaldefinition des § 3 Nr. 30 TKG handelt es sich bei Verkehrsdaten um Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden. Dementsprechend stehen Verkehrsdaten in einem direkten Zusammenhang zur Inanspruchnahme eines Telekommunikationsdienstes. Die Vorschrift des § 113a TKG enthält die Grundvoraussetzungen der Speicherungsverpflichtung und bestimmt, welcher Diensteanbieter welche Datenarten im Rahmen der Nutzung des jeweiligen Telekommunikationsdienstes zu speichern hat. Nicht erfasst von der Speicherungspflicht nach § 113a TKG sind beispielsweise folgende Verkehrsdaten:

- Rein technisch bedingte und für die Kommunikation im Internet bei der Inanspruchnahme eines Telekommunikationsdienstes automatisch anfallende Daten. Hierzu zählen beispielsweise Daten, die über von Netzbetreibern bereitgestellte Übertragungswege von anderen Diensteanbietern transportiert werden.
- Die von einem Nutzer bei der Inanspruchnahme eines Internetzugangsdienstes aufgerufenen Internetseiten.
- Bei Anbietern von Internetzugangsdiensten können Verkehrsdaten über die von einem Nutzer genutzte Bandbreite der Internetverbindung und die übertragene Datenmenge anfallen.
- Die MAC Adresse (Media-Access-Control-Address), die die Kennung einer Netzwerkkarte (LAN oder WLAN) darstellt und anhand derer ein Gerät im Netzwerk identifiziert werden kann. Hierbei handelt es sich um eine Gerätekennung und nicht um eine Anschlusskennung im Sinne des § 113a Abs. 4 Nr. 2 TKG.

Frage 2: Welche Verkehrsdaten werden sonst, insbesondere auf der Grundlage von § 96 Abs. 2 TKG, zu welchen Zwecken und für welche Zeitdauer gespeichert?

Eine Verwendung der Verkehrsdaten nach Ende der Verbindung hinaus orientiert sich an den gesetzlichen Vorgaben des § 96 Abs. 2 Satz 1 TKG. Hiernach muss

die Verwendung der Verkehrsdaten für die Entgeltermittlung und Entgeltabrechnung oder für die Erstellung eines Einzelbindungsnachweises erforderlich sein, der Erkennung oder Beseitigung von Störungen von Telekommunikationsanlagen oder der Bekämpfung des Missbrauchs von Telekommunikationsdiensten sowie der Durchführung einer Fangschaltung dienen.

Darüber hinaus sieht die Vorschrift vor, dass gespeicherte Verkehrsdaten über das Ende der Verbindung hinaus auch „für die durch andere gesetzliche Vorschriften begründeten Zwecke“ erhoben und verwendet werden dürfen. Mit dem Verweis auf andere gesetzlich begründete Zwecke wird die Zulässigkeit der Verwendung der Verkehrsdaten für Auskunftersuchen der Strafverfolgungs- und Sicherheitsbehörden begründet und geht damit über die rein betrieblich bedingte Verwendung hinaus. Die Erteilung von Auskünften über Verkehrsdaten an die Strafverfolgungs- und Sicherheitsbehörden und entsprechende Auskunftsansprüche finden sich beispielsweise in bundesgesetzlichen Regelungen wie der Strafprozessordnung, dem Bundeskriminalamtgesetz, dem Zollfahndungsdienstegesetz, dem Bundesverfassungsschutzgesetz, dem BND-Gesetz und dem MAD-Gesetz, aber zunehmend auch in Polizei- und Verfassungsschutzgesetzen der Länder.

Mit der Verabschiedung des Gesetzes zur Bekämpfung der Kinderpornografie in Kommunikationsnetzen (BT Drucksache 16/13411 und BR Drucksache 604/09) hat die Vorschrift des § 96 TKG eine Änderung erfahren. Inwieweit sich diese Änderung auf den vorliegenden Sachverhalt auswirkt, kann derzeit noch nicht abgeschätzt werden.

Frage 3: Auf welche Weise wird die Trennung der allein nach § 113a TKG gespeicherten Verkehrsdaten von anderen Verkehrsdaten gewährleistet?

Nach unserem Kenntnisstand wird die Trennung der allein aufgrund § 113a TKG gespeicherten Verkehrsdaten von anderen Daten von den Diensteanbietern in der Praxis auf unterschiedliche Weise gehandhabt und gewährleistet. Teilweise werden die im Rahmen des § 113a TKG zu speichernden Verkehrsdaten in einer gesonderten Datenbank und damit körperlich getrennt von anderen Daten gespeichert und durch technische und organisatorische Maßnahmen sichergestellt, dass der Zugang zu diesen Daten nur besonders ermächtigten Personen möglich ist. Teilweise erfolgt die Speicherung in einer einheitlichen Datenbank, die mit unterschiedlichen Zugriffssicherungen und –berechtigungen versehen ist und damit gewährleistet, dass der Zugang nur besonders ermächtigten Personen möglich ist. Bedingt durch die jeweiligen Systemstrukturen und technischen Gegebenheiten erfolgt teilweise auch eine Speicherung der Verkehrsdaten nach § 113a TKG in unterschiedlichen Datenbanken, bei denen ebenfalls durch technische und organisatorische Maßnahmen ein Zugriffsschutz gewährleistet wird.

Die von den Diensteanbietern gewählte Methode ist dabei in erster Linie abhängig von der jeweiligen Unternehmensgröße und der finanziellen Leistungsfähigkeit. In diesem Zusammenhang möchten wir darauf hinweisen, dass gerade der Internetbereich überproportional von der Einführung der Verpflichtung zur Vorratsdatenspeicherung betroffen ist. Der überwiegende Teil der in Deutschland tätigen TK-Unternehmen besteht aus kleinen und mittelständischen TK-Unternehmen. Im Bereich von Internet-Access sind etwa 80% kleine und sehr kleine Unternehmen am Markt tätig. Bei der Bereitstellung von E-Mail werden etwa 2/3 der E-Mail-Dienste von Dienstleistern angeboten, die bis zu 1.000 Kunden haben. Im Gegensatz zur klassischen Telefonie, bei der entsprechende Systeme bereits für Abrechnungszwecke vorhanden sind, sind im Internetbereich für die im Zusammenhang mit der Vorratsdatenspeicherung zu erfassenden Daten neue Systeme erforderlich. Insbesondere für kleine Unternehmen ist eine Speicherung der Vorratsdaten in einer gesonderten Datenbank wirtschaftlich nicht darstellbar. Daneben kann sich aus der Unternehmensgröße ein organisatorisches Problem bei der Implementierung von Zugriffssicherungen und –berechtigungen ergeben. Die Personalausstattung wird meist dazu führen, dass eine personelle Trennung nicht vorgenommen werden kann. Die vorstehend genannten Probleme verdeutlichen die besondere Dringlichkeit einer Entschädigungsregelung für die im Zusammenhang mit der Einführung der Vorratsdatenspeicherung entstehenden Anschaffungs- und Betriebskosten.

Zur Sicherung der Vorratsdaten gegen unbefugte Zugriffe:

Frage 4: § 113a Abs. 2 S. 1 Nr. 4 c TKG schreibt für mobile Telefondienste die Speicherung der Bezeichnung der durch den anrufenden und den angerufenen Anschluss bei Beginn der Verbindung genutzten Funkzellen vor.

1. Spiegelstrich

Lassen sich auch aus anderen nach § 113a TKG zu speichernden Daten Rückschlüsse auf das Bewegungsverhalten der Nutzer mobiler Telekommunikationsdienste ziehen?

Aus der Nutzung mobiler Telekommunikationsdienste lassen sich theoretisch Rückschlüsse auf das Bewegungsverhalten der Nutzer ziehen und Bewegungsprofile erstellen. Wir gehen für den Internetbereich allerdings davon aus, dass die entsprechenden Daten nicht von der Speicherungsverpflichtung nach § 113a TKG umfasst sind.

So ließe sich beispielsweise bei der nomadischen Nutzung eines Voice over IP-Telefoniedienstes an einem anderen Standort (z.B.: WLAN-Hotspot) anhand der IP-Adresse mittels Geo-Lokalisierung zumindest grob der ungefähre Standort ermitteln. Hieraus würden sich Rückschlüsse auf das Bewegungsverhalten

ergeben. Nach unserer Einschätzung wird von dem Anwendungsbereich der Vorschrift des § 113a Abs. 2 S. 1 Nr. 4 TKG die nomadische Nutzung eines VoIP-Dienstes jedoch nicht erfasst. Sofern über den Anwendungsbereich des § 113a Abs. 2 S. 1 Nr. 4 TKG im Hinblick auf die nomadische Nutzung von VoIP-Diensten unterschiedliche Auffassungen bestehen sollten, ist eine ausdrückliche Klarstellung erforderlich, dass keine Speicherungsverpflichtung bei der nomadischen Nutzung eines VoIP-Dienstes besteht.

Eine weitere Möglichkeit bestünde bei der mobilen Nutzung des Internet in so genannten WLAN-Hotzones (oder auch WMAN, Wireless Metropolitan Access Network), in denen in einem bestimmten Bereich ein flächendeckender Internetzugang besteht und welche eine Zone bezeichnen, in denen ein nahtloser Übergang zwischen den verschiedenen WLAN Zugangspunkten möglich ist. Würde bei der Nutzung von WLAN-Hotzones eine Speicherung von Standortwechseln erfolgen, so könnten sich hieraus Rückschlüsse auf das Bewegungsverhalten ergeben. Nach unserem Kenntnisstand findet in WLAN-Hotzones keine Speicherung von Standortwechseln statt und deren Nutzung wird auch nicht von den gesetzlichen Speicherungsverpflichtungen nach § 113a Abs. 2 S. 1 Nr. 4 TKG erfasst.

Grundsätzlich ist drauf hinzuweisen, dass bei der Speicherung von Ursprungsdaten (IP-Adresse) bei der Nutzung eines Internetdienstes unter Verwendung der Geo-Lokalisierung die Erstellung eines groben Bewegungsprofils möglich ist. Durch die im Rahmen der Vorratsdatenspeicherung erhobenen Daten wird zudem eine Datenbasis geschaffen, welche auch im nachhinein durch Abfrage der konkreten Nutzungsadresse dieses grobe Bewegungsprofil in ein detailliertes Bewegungsprofil verwandelt (z.B. bei der mobilen automatischen E-Mail Abfrage: Standort alle 5 Minuten).

Vor diesem Hintergrund lehnt eco eine erweiterte Speicherung der Nutzungsdaten durch Dienstleister ab, was auch der geltenden Rechtslage entspricht.

2. Spiegelstrich

Werden etwa im Rahmen des LKW-Maut-Systems durch den Datenaustausch zwischen der im LKW installierten Onboard-Unit und Toll-Collect Verkehrsdaten erzeugt, die nach § 113a TKG zu speichern sind? Um welche Daten handelt es sich?

Für die sachdienliche Beantwortung dieser Frage liegen uns keine detaillierten Informationen vor. Wir regen daher an, sich direkt an die von der Bundesregierung beauftragte Unternehmen, die Toll Collect GmbH und den an dem System beteiligten Mobilfunkanbieter zu wenden.

3. Spiegelstrich

Müssen in der Praxis, etwa aus technischen Gründen, die Standortdaten von Mobiltelefonen auch im Standby-Betrieb gespeichert werden?

Die Funkzelle, in der ein Mobiltelefon eingebucht ist, wird auch im Standby-Betrieb gespeichert. Hierbei handelt es sich aber nicht um Standortinformationen, die nach § 113a Abs. 2 S. 1 Nr. 4 TKG zu speichern sind.

4. Spiegelstrich

Lassen sich durch den Einsatz stiller SMS oder Stealth-SMS gezielt speicherungspflichtige Verkehrsdaten erzeugen? Wird von dieser Möglichkeit in der Praxis der Strafverfolgungs- und Gefahrenabwehrbehörden sowie der Nachrichtendienste Gebrauch gemacht? Auf welcher Grundlage?

Durch den Einsatz stiller SMS oder Stealth-SMS lassen sich gezielt speicherungspflichtige Verkehrsdaten erzeugen. Die auf diese Weise generierten Verkehrsdaten können unter den Voraussetzungen des § 100g StPO abgefragt werden. Inwieweit in der Praxis von Strafverfolgungs- und Gefahrenabwehrbehörden sowie der Nachrichtendiensten von der Möglichkeit, gezielt speicherungspflichtige Verkehrsdaten zu generieren, Gebrauch gemacht wird, entzieht sich unserer Kenntnis.

Frage 5: Kommt in der Praxis der in § 113a Abs. 2 S. 1 Nr. 4 d TKG geregelte Fall im Voraus bezahlter anonymer mobiler Telefondienste vor (vgl. § 111 TKG)? Welche Bedeutung hat dabei die Speicherung der ersten Aktivierung nach Datum, Uhrzeit und Bezeichnung der Funkzelle für die Strafverfolgung, die Gefahrenabwehr und die Erfüllung der Aufgaben der Nachrichtendienste?

Nach unserem Kenntnisstand kommt der auf der Umsetzung von Artikel 5 (1) e) 2. vi) der Richtlinie 2006/24/EG beruhende und in § 113a Abs. 2 S. 1 Nr. 4d TKG geregelte Fall der im Voraus bezahlten anonymen Telefondienste aufgrund der Regelung des § 111 TKG in Deutschland in der Praxis nicht vor. Allerdings führt die Möglichkeit der Weitergabe von Prepaid-Karten dazu, dass die ursprünglich im Rahmen der Registrierung erfasste Person nicht mit dem tatsächlichen Nutzer übereinstimmt und damit die Vorschrift leerläuft. Im Übrigen gehen wir für den Bereich der nomadische Nutzung von VoIP-Diensten davon aus, dass diese nicht dem Anwendungsbereich des § 113a Abs. 2 S. 1 Nr. 4d TKG unterliegen.

Frage 6: Welche nach § 113a TKG zu speichernden Verkehrsdaten fallen bei einem Internetzugang über sogenannte Hot Spots an? Inwieweit erfassen sie zuordenbare Daten einzelner Nutzer, die über den Hot Spot Zugang zum Internet nehmen? Ist dies unterschiedlich zu beantworten je nachdem, ob der Internetzugang über einen offenen WLAN-Anschluss oder kommerzielle WLAN-Dienste erfolgt?

Grundsätzlich ist in diesem Zusammenhang zunächst zwischen der Bereitstellung des TK-Anschlusses, mit dem die Anbindung eines Hotspot an das Internet erfolgt (bzw. an dem ein Hotspot betrieben wird), dem Betrieb eines mobilen Internetzugangsdienstes und der Nutzung dieses Dienstes zu differenzieren.

Im Rahmen der Bereitstellung des TK-Anschlusses fallen bei dem Betrieb des Hotspot Verkehrsdaten an, die nach § 113a Abs. 4 TKG zu speichern sind. Hierzu gehört beispielsweise die IP-Adresse, mit der der Hotspot an das Internet angebunden ist. Sofern es sich hierbei um eine dynamische IP-Adresse handelt, ist diese nach § 113a Abs. 4 TKG zu speichern. Bei einer statischen IP-Adresse würde es sich um ein Bestandsdatum handeln, das nach § 111 TKG zu beauskunften wäre.

Der Anbieter eines mobilen Internetzugangsdienstes (Hotspot-Betreiber) ist zur Speicherung von Verkehrsdaten nach § 113a Abs. 4 TKG verpflichtet, sofern diese Verkehrsdaten von ihm bei der Nutzung seines Dienstes erzeugt und verarbeitet werden (§ 113a Abs. 1 TKG). In der Regel werden bei der Nutzung eines mobilen Internetzugangsdienstes keine Verkehrsdaten im Sinne des § 113a Abs. 1, Abs. 4 TKG erzeugt oder verarbeitet. Denn dem jeweiligen Nutzer wird keine öffentliche IP-Adresse zugewiesen, sondern die Nutzer teilen sich die öffentliche IP-Adresse, mit der der Hotspot an das Internet angebunden ist (§ 113a Abs. 4 Nr. 1 TKG). Eine eindeutige Kennung des Anschlusses im Sinne des § 113a Abs. 4 Nr. 2 TKG, über den die Internetnutzung erfolgt, wird nicht vergeben. Bei der MAC-Adresse des Endgerätes, das an einem Hotspot genutzt wird, handelt es sich um eine Geräteerkennung und nicht um eine Anschlusskennung im Sinne des § 113a Abs. 4 Nr. 2 TKG. Da bei der Nutzung des Hotspot keine externen IP-Adressen vergeben werden, erfolgt auch keine Speicherung nach § 113a Abs. 4 Nr. 3 TKG. Demgegenüber wird seitens einzelner Mitarbeiter der Bundesnetzagentur die Ansicht vertreten, dass in diesem Fall die Daten des NAT-Servers (Network Access Translation) und damit die internen IP-Adressen des Hotspot gespeichert werden müssten. Unabhängig davon, dass hierzu keine gesetzliche Speicherungsverpflichtung besteht, ist dies in der Praxis nicht durchführbar.

Sofern nach § 113a TKG Verkehrsdaten gespeichert werden, sind diese in der Regel nicht einem einzelnen Nutzer zuordenbar, da die Erhebungsvorschrift des

§ 111 TKG für diesen Sachverhalt nicht einschlägig ist. Eine andere Beurteilung ergibt sich demgegenüber bei kommerziell betriebenen mobilen Internetzugangsdiensten. Die Anbieter erfassen personenbezogene beziehungsweise personenbeziehbare Daten, um die Inanspruchnahme des Dienstes abrechnen zu können. Hierzu gehört typischerweise die Erfassung des jeweiligen Nutzers und dessen Identifizierung sowie Beginn und Ende der Nutzung. Sofern der Anbieter eine anonyme Bezahlung ermöglicht (beispielsweise bei im Voraus bezahlten Prepaid-Karten), ist eine Zuordnung zu einem individuellen Nutzer allerdings nicht möglich. Sofern anfallende Nutzungsdaten nicht für Abrechnungszwecke relevant sind, sind diese nicht zu speichern. Insofern ergibt sich auch eine Unterscheidung zwischen dem kommerziellen Betrieb eines mobilen Internetzugangsdienstes und der Möglichkeit des Internetzugangs über ein so genanntes „offenes WLAN“.

Die nach § 113a TKG zu speichernden Daten haben einen Bezug zu dem Inhaber des TK-Anschlusses, sind jedoch im Regelfall nicht dem jeweiligen Nutzer direkt zuordenbar.

Zu den zur Speicherung Verpflichteten:

Frage 7: In welchem Umfang wird in der Praxis als nach § 113a TKG speicherungspflichtig auch angesehen, wer unentgeltlich Telekommunikationsdienste anbietet?

Die Frage der Pflicht zur Speicherung von Verkehrsdaten nach den Vorschriften der Vorratsdatenspeicherung für Anbieter unentgeltlicher Telekommunikationsdienste ist ungeklärt.

Voraussetzung des § 113a TKG ist lediglich das Erbringen öffentlich zugänglicher Telekommunikationsdienste für Endnutzer. § 3 Nr. 24 TKG definiert den Begriff der Telekommunikationsdienste jedoch einschränkend als „in der Regel gegen Entgelt erbrachte Dienste“. Die Bundesnetzagentur stellt in ihren „Häufig gestellten Fragen zur Vorratsdatenspeicherung“ (abrufbar auf den Internetseiten der Bundesnetzagentur) ausschließlich darauf ab, ob mittels einer TK-Anlage öffentlich zugängliche Dienste erbracht werden. Zur weiteren Abgrenzung und Eingrenzung wird auf ein räumliches Kriterium abgestellt. Danach soll keine Speicherungspflicht nach § 113a TKG für Gastronomie, Hotels, Internetcafés usw. bestehen, sofern es sich bei dem Telefon-/Internetzugangsangebot um eine lokale Mitbenutzung handelt und diese grundsätzlich auf den Herrschaftsbereich des Anschlussinhabers beschränkt ist. Demgegenüber seien diese Voraussetzungen bei Hotspot-Angeboten zur Versorgung von öffentlichen Plätzen und Verkehrsflächen in z.B. Flughäfen und Bahnhöfen nach Ansicht der Bundesnetzagentur nicht erfüllt, so dass hier eine Speicherungspflicht nach § 113a TKG bestehe.

Frage 8: Wie wird in der Praxis behandelt, wer (wie Unternehmen für ihre Mitarbeiter, Vereine für ihre Mitglieder oder Universitäten für ihre Angehörigen) Telekommunikationsdienste nur für einen begrenzten Nutzerkreis anbietet? Wird insoweit von öffentlich zugänglichen Telekommunikationsdiensten ausgegangen, deren Erbringer zur Vorratsdatenspeicherung verpflichtet sind?

Diese Fragestellung ist nicht abschließend geklärt. Nach § 113a Abs. 1 S. 1 TKG richten sich die Speicherungspflichten grundsätzlich an diejenigen, die öffentlich zugängliche Telekommunikationsdienste für Endnutzer erbringen. Ausweislich der Gesetzesbegründung besteht daher für den nicht öffentlichen Bereich keine Speicherungsverpflichtung. Hierzu sollen nach der Gesetzesbegründung unternehmensinterne Netze, Nebenstellenanlagen oder E-Mail-Server von Universitäten ausschließlich für dort immatrikulierte Studierende und Bedienstete sowie die Telematikinfrastruktur im Gesundheitswesen gehören. Hinsichtlich der Gestattung zur privaten Mitbenutzung der im Betrieb zur Verfügung stehenden Telekommunikationsmittel durch den Arbeitgeber stellt die Bundesnetzagentur in ihren „Häufig gestellten Fragen zur Vorratsdatenspeicherung“ (abrufbar auf den Internetseiten der Bundesnetzagentur) darauf ab, ob der Zugang zu dem Telekommunikationsdienst „Jedermann“ offen steht. Dies sei bei der Gestattung der Mitbenutzung durch den Arbeitgeber nicht der Fall, so dass keine Verpflichtung zur Speicherung nach § 113a TKG bestehe.

Zu mittels Telekommunikation begangenen Straftaten:

Frage 9: Welche mittels Telekommunikation zu verwirklichenden Straftatbestände oder typische Fallgruppen solcher Straftatbestände laufen ohne Rückgriff auf die nach § 113a TKG zu speichernden Daten im Wesentlichen leer?

Nach der Studie „Rechtswirklichkeit der Auskunftserteilungen über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO“ des Max-Planck-Instituts für ausländisches und internationales Strafrecht und den Polizeilichen Kriminalstatistiken des Bundeskriminalamtes ist davon auszugehen, dass bereits ohne einen Rückgriff auf die nach § 113a TKG zu speichernden Daten eine sehr gute Aufklärungsquote besteht. Die Einführung der Speicherungspflichten dürfte sich dementsprechend nur geringfügig auf die Aufklärungsquote auswirken. Beachtenswert ist, dass die Aufklärungsquote im Bereich der mittels Telekommunikation begangenen Straftaten im Vergleich zur allgemeinen Aufklärungsquote überdurchschnittlich hoch zu sein scheint. Vor diesem Hintergrund stellt sich die Frage, ob und in welchem Umfang von einem „Leerlaufen“ der Strafverfolgung ohne einen Rückgriff auf die nach § 113a TKG zu speichernden Daten auszugehen ist. In diesem Zusammenhang ist zu beachten, dass den Strafverfol-

gungsbehörden eine Vielzahl von Ermittlungsmethoden zur Verfügung stehen. Mit Einführung der anlass- und verdachtsunabhängigen Vorratsdatenspeicherung von Verkehrsdaten ist davon auszugehen, dass die berechtigten Stellen in einem erheblichen Umfang von der nunmehr zur Verfügung stehenden Möglichkeit des Rückgriffs auf die nach § 113a TKG zu speichernden Daten Gebrauch machen werden und damit dieses Instrument zu einer ermittlungstaktischen Standardmaßnahme zu werden droht. In diesem Zusammenhang stellt sich rechtspolitisch die Frage, bei welchen Delikten und unter welchen Voraussetzungen ein Rückgriff auf die nach § 113a TKG gespeicherten Daten erfolgen soll und auch unter dem Gesichtspunkt der Verhältnismäßigkeit angemessen ist.

Hierbei muss auch kritisch hinterfragt werden, welche nach § 113a TKG zu speichernden Daten für die Aufklärung von Straftaten zwingend erforderlich sind. Für den Bereich des Internet sind nach unserer Einschätzung ausschließlich die nach § 113a Abs. 4 TKG zu speichernden Daten relevant. Hierdurch wird die Zuordnung einer IP-Adresse zu einem TK-Anschluss und damit die Identifikation des Anschlussinhabers ermöglicht. Eine darüber hinausgehende dienstebezogene Speicherung des konkreten Nutzungsverhaltens (E-Mail, VoIP-Dienst) ist nicht erforderlich.

Zur Auskunftserteilung nach § 113 TKG:

Frage 10: Ist § 113b S. 1 Hs. 2 i. V. m. § 113 TKG auch für andere Zwecke von Bedeutung als für die Zuordnung von Internetprotokolladressen?

Der Vorschrift des § 113b S. 1 Hs. 2 i.V.m. § 113 TKG kommt eine zentrale Bedeutung für Auskunftersuchen der berechtigten Stellen zu. Denn damit wird die Möglichkeit geschaffen, zur Beantwortung von Auskunftersuchen der berechtigten Stellen auf die im Rahmen der Verkehrsdatenspeicherung nach § 113a TKG gespeicherten Daten zuzugreifen. Besonders problematisch hieran ist, dass seitens der berechtigten Stellen zwar ein Bestandsdatum abgefragt wird, dieses jedoch nur unter Verwendung von Verkehrsdaten ermittelt werden kann. Da es sich um eine Auskunft über Bestandsdaten handelt, unterliegt diese nicht den strengen gesetzlichen Anforderungen an eine Abfrage der nach § 113a TKG gespeicherten Verkehrsdaten. Dementsprechend ist es ausschließlich von der Gestaltung des Auskunftersuchens durch die berechtigten Stellen abhängig, nach welchen rechtlichen Anforderungen das Auskunftersuchen zu beurteilen ist. Damit einher geht eine erhebliche Ausweitung der berechtigten Stellen.

Hierbei ist zu berücksichtigen, dass die Auskunft über die Bestandsdaten unter Rückgriff auf die Verkehrsdaten erteilt wird. Die Verkehrsdaten unterliegen dem Fernmeldegeheimnis und Eingriffe in das Fernmeldegeheimnis haben den

verfassungsrechtlichen Anforderungen hieran zu entsprechen. Diesen Anforderungen genügt § 113b S. 1 Hs. 2 i.V.m. § 113 TKG aus der Sicht des eco nicht. So ist insbesondere keine richterliche Anordnung für den Eingriff in das Fernmeldegeheimnis und keine Beschränkung der Eingriffe auf bestimmte Straftatbestände vorgesehen.

Das grundsätzliche Erfordernis einer richterlichen Anordnung für Eingriffe in das Fernmeldegeheimnis ist ständige Rechtsprechung des Bundesverfassungsgerichts. Sie ist ebenfalls Voraussetzung des zivilrechtlichen Auskunftsanspruchs über Bestandsdaten unter Verwendung von Verkehrsdaten gemäß § 101 Abs. 9 UrhG. Das Erfordernis eines Straftatenkatalogs für die Auskunft über Verkehrsdaten, die der Vorratsdatenspeicherung unterliegen, hat das Bundesverfassungsgericht in der einstweiligen Anordnung zur Vorratsdatenspeicherung aufgestellt (BVerfG, Beschl. v. 11.03.2008, 1 BvR 256/08). Danach muss für die Verwendung der auf Vorrat gespeicherten Daten der Verdacht einer Straftat gemäß § 100a Abs. 2 StPO vorliegen.

Vor diesem Hintergrund ist die Vorschrift des § 113b S. 1 Hs. 2 i.V.m. § 113 TKG aus verfassungsrechtlichen Gründen äußerst kritisch zu bewerten.

Zur Sicherung der Vorratsdaten gegen unbefugte Zugriffe:

Frage 11: Welche Maßstäbe werden in der Praxis an die „im Bereich der Telekommunikation erforderliche Sorgfalt“ im Sinne von § 113a Abs. 10 Satz 1 TKG angelegt? Welche möglichen Anforderungen werden darüber hinaus diskutiert?

Nach Ansicht des Verbandes der deutschen Internetwirtschaft eco hat die Regelung des § 113a Abs. 10 S. 1 TKG hinsichtlich der „im Bereich der Telekommunikation erforderlichen Sorgfalt“ lediglich deklaratorischen Charakter. Sie enthält den Hinweis auf die Verpflichtung der Anbieter auf das Fernmeldegeheimnis. Für diese Auffassung spricht auch die Begründung des Gesetzentwurfs, in der es heißt: „Absatz 10 stellt klar, dass der Verpflichtete die zu speichernden Verkehrsdaten mit der Sorgfalt zu behandeln hat, die beim Umgang mit vom Fernmeldegeheimnis geschützten Daten erforderlich ist (...)“. Diese Verpflichtung ist jedoch bereits einfachgesetzlich in § 88 TKG festgeschrieben. Von der Verpflichtung zum Fernmeldegeheimnis sind sowohl die Inhalte als auch ihre näheren Umstände erfasst, auf welche sich die Vorratsdatenspeicherung bezieht. Da der Begriff der im Bereich der Telekommunikation erforderlichen Sorgfalt gemäß § 113a Abs. 10 Satz 1 TKG nicht über den des Fernmeldegeheimnis gemäß § 88 TKG hinausgeht, ergeben sich diesbezüglich für die Anbieter von Telekommunikationsdiensten nach Auffassung von eco keine über die allgemeinen Anforderungen des TKG hinausgehenden Verpflichtungen.

Zu Frage 12: Nach § 113a Abs. 10 Satz 2 TKG hat der zur Speicherung Verpflichtete im Rahmen der im Bereich der Telekommunikation zu beachtenden erforderlichen Sorgfalt durch technische und organisatorische Maßnahmen sicherzustellen, dass der Zugang zu den nach § 113a TKG gespeicherten Daten ausschließlich hierzu von ihm besonders ermächtigten Personen möglich ist.

- **Welche technischen und organisatorischen Maßnahmen kommen insoweit in Betracht? Inwieweit sind diese Maßnahmen auf eine regelmäßige Überprüfung verwiesen und welche Vorkehrungen werden diesbezüglich getroffen? Welche Konzepte werden insoweit diskutiert, worin liegen ihre Vor- und Nachteile?**
- **Wie sicher lässt sich mit solchen Maßnahmen ein missbräuchlicher oder unbefugter Zugriff verhindern?**

Als technische und organisatorische Maßnahmen zur Sicherstellung, dass ausschließlich besonders ermächtigte Personen Zugang zu den nach § 113a TKG gespeicherten Daten haben, kommen insb. die im Grundschutzkatalog des BSI (www.bsi.bund.de/gshb) genannten Maßnahmen der Zutritts- (Kap. M 2.6), Zugangs- (M 2.7) und Zugriffsberechtigungen (M 2.8) in Frage. Die Zutrittsberechtigung umfasst den physischen Zutritt zu bestimmten schutzbedürftigen Räumen eines Gebäudes. Zur Überwachung der Zutrittsberechtigung können Personen (Pförtner, Schließdienst) oder technische Einrichtungen (Ausweisleser, biometrische Verfahren wie Irisscanner oder Fingerabdruck, Sicherheitstürschloss bzw. Schließanlage) eingesetzt werden. Zugangsberechtigungen erlauben der betroffenen Person oder einem autorisierten Vertreter, bestimmte IT-Systeme bzw. System-Komponenten und Netze zu nutzen. Die Zugangskontrolle erfolgt durch Identifikation (z.B. durch Name, User-ID oder Chipkarte) und Authentisierung (z.B. durch ein Passwort) des Nutzungsberechtigten. Über Zugriffsrechte wird schließlich geregelt, welche Person im Rahmen ihrer Funktion bevollmächtigt wird, IT-Anwendungen oder Daten zu nutzen. Die Zugriffsrechte (z.B. Lesen, Schreiben, Ausführen) auf IT-Anwendungen, Teilanwendungen oder Daten sind dabei von der Funktion abhängig, die die Person wahrnimmt. Die interne und unregelmäßige Überprüfung (M 2.182) ist Teil des Sicherheitskonzepts. Neben die internen Kontrollen treten diejenigen der staatlichen Aufsichtsbehörden nach § 115 TKG, die von einzelnen Anordnungen über die Verhängung von Zwangsgeldern bis zur Untersagung des Betriebes reichen. Zusätzlich wird der Verstoß gegen die Pflichten zur Vorratsdatenspeicherung gemäß § 149 Abs. 1 Nr. 36-39 TKG mit Geldbußen geahndet.

Bei der Evaluierung der Sicherheitsmaßnahmen ist aus der Sicht des eco zu berücksichtigen, dass ein ausgewogenes Verhältnis zwischen den Sicherheitsanforderungen und den Kosten für die Umsetzung der Maßnahmen gefunden

wird. Anderenfalls ist zu befürchten, dass aufgrund der Kosten der Vorratsdatenspeicherung und der hierfür zu treffenden Sicherheitsvorkehrungen der Wettbewerb zwischen großen und kleinen bzw. mittleren Unternehmen der Telekommunikationswirtschaft verzerrt wird. Denn große Unternehmen können die Kosten leichter erwirtschaften als ihre kleineren Wettbewerber. Dies gilt umso mehr, als auch nach Verabschiedung des TK-Entscheidungs-Neuordnungsgesetzes die Kosten der Unternehmen für die Anschaffung und den Betrieb der Überwachungsinfrastruktur nicht erstattet werden. Dies stellt aus der Sicht von eco einen Eingriff in die Berufsfreiheit der betroffenen Unternehmen gemäß Art. 12 GG dar, insbesondere vor dem Hintergrund, dass die Verkehrsdaten, die der Vorratsdatenspeicherung gemäß § 113a TKG unterliegen, ausschließlich für staatliche Zwecke erhoben und genutzt werden.

Ergänzend mochten wir im Zusammenhang nochmals darauf hinweisen, dass ein direkter Zusammenhang zwischen Sicherungskonzept und Sicherungsmaßnahmen zu der Unternehmensgröße und finanziellen Leistungsfähigkeit des verpflichteten Unternehmens besteht (vergleiche Frage 3).

Die Erfahrungen in der Vergangenheit haben jedoch gezeigt, dass auch ein stringentes und konsequentes Sicherungskonzept und Sicherungsmaßnahmen einen missbräuchlichen und unbefugten Zugriff auf Daten nicht verhindern, sondern allenfalls erschweren können, wenn der Zugriff unternehmensintern durch ein kollusives Zusammenwirken erfolgt.

Zur Ausgestaltung der Nutzung:

Frage 13: Welche Instrumente (z.B. Kennzeichnungs-, Löschungs- und Auskunftspflichten, Richtervorbehalte, Benachrichtigungspflichten, die eine ergänzende nachträgliche Gerichtskontrolle gewährleisten, oder – eventuell auch immaterielle – Schadensersatzansprüche bei rechtswidrigem Datenzugriff) werden zur Einhegung und rechtsstaatlichen Kontrolle der Nutzung der nach § 113a TKG zu speichernden Daten diskutiert? Worin liegen ihre Vor- und Nachteile?

Zur Beantwortung der Frage wird auf die Studie „Rechtswirklichkeit der Auskunftserteilungen über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO“ des Max-Planck-Instituts für ausländisches und internationales Strafrecht verwiesen. Im Rahmen der Studie wurden durch schriftliche Befragungen, Aktenanalysen und Expertengespräche die Erkenntnisse von Polizeibeamten, Staatsanwälten, Richtern, Verteidigern und Telekommunikationsunternehmen zur Verkehrsdatenabfrage, zur Anordnungspraxis, zu den betroffenen Delikten, zur richterlichen bzw. im Eilfall staatsanwaltschaftlichen Anordnung, zur Begründung der Anordnungen, zu Verfahrenserledigungen, zum Verhältnis der Verkehrsdaten-

abfrage zu anderen Ermittlungsmaßnahmen und zur Subsidiarität, zum Richter-
vorbehalt, zur Benachrichtigung und Löschung, zur Effizienz der
Verkehrsdatenabfrage, zu den Problemen der Implementation und zu den Kosten
zusammengetragen.
