TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Informatik Institut für Systemarchitektur

Professur für Datenschutz und Datensicherheit

Technische Universität Dresden, 01062 Dresden

An den
Präsidenten des Bundesverfassungsgerichts
Herrn
Prof. Dr. Dr. h.c. mult. Hans-Jürgen Papier
als Vorsitzender des Ersten Senats
Postfach 1771
76006 Karlsruhe

Prof. Dr.
Andreas Pfitzmann

Telefon: 0351 463-38277
Telefax: 0351 463-38255
Mobiltel.: 0173 148 5074
E-Mail: Andreas.Pfitzmann@tu-dresden.de

Sekr.: 0351 463-38247
E-Mail: Martina.Gersonde@tu-dresden.de

AZ:

Dresden, 10. Juni 2009

1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08

Sehr geehrter Herr Präsident, sehr geehrte Damen und Herren,

bevor mein Mitarbeiter, *Dipl.-Inf. Stefan Köpsell* und ich Ihre Fragen der Reihe nach beantworten, zunächst in einem Durchgang möglichst kurz, danach in einem zweiten Durchgang ausführlicher, möchten wir aus unserer Sicht als Informatiker den Gegenstandsbereich einordnen und die aus unserer Sicht „großen“ Fragen aufwerfen.

Zur Einordnung des Gegenstandsbereiches empfehlen wir

> Andreas Pfitzmann: Möglichkeiten und Grenzen der Nutzungsüberwachung von Informations- und Kommunikationssystemen in einer freiheitlichen demokratischen Gesellschaft (dem Gericht schon am 26.09.2007 als Vorbereitung zur Verhandlung über die sogenannte Online-Durchsuchung vorgelegt, 1 BvR 370/07, 1 BvR 595/07, hier nochmals beigefügt)

An diesem Text ist auch aus heutiger Sicht nichts zu ändern und ihm ist auf seiner Betrachtungsebene auch nichts hinzuzufügen. Er ist im Informatik-Spektrum Band 31, Heft 1 (Februar 2008) S. 65-69 erschienen – *der* Zeitschrift der Informatiker im deutschsprachigen Raum. Ihm wurde von Informatikern nach unserem Kenntnisstand nicht widersprochen.

Für Rückfragen und weitergehende Fragen stehen Stefan Köpsell und ich jederzeit zur Verfügung.

Mit freundlichen Grüßen

Postadresse (Briefe)
TU Dresden, Fakultät Informatik
Institut für Systemarchitektur
01062 Dresden

Postadresse (Pakete u.ä.)
TU Dresden, Fakultät Informatik
Institut für Systemarchitektur
Helmholtzstraße 10
01069 Dresden

Besucheradresse
Sekretariat:
01187 Dresden
Nöthnitzer Str. 46
Zi. 3070

Internet
http://dud.inf.tu-dresden.de

Die „großen“ Fragen und Abwägungen sind aus unserer Sicht:

- Die weitgehende Unsicherheit der Informationstechnik (IT) wird auf absehbare Zeit nicht zu vermeiden sein, d. h. alle durch IT bereitgestellte Funktionalität wird auch von Unbefugten genutzt werden. Hieraus folgt als Empfehlungen:

  Sicherheitslücken der IT für Strafverfolgung und Verbrechensvorbeugung nutzen: vielleicht.
  Weitere Sicherheitslücken (wie z. B. Vorratsdatenspeicherung) in IT einbauen: Nein!

- Die Trennung von Verkehrsdaten/Protokolldaten einerseits und Inhaltsdaten der Kommunikation andererseits ist zunehmend unklar (Bsp.: URLs enthalten Informationen über die Inhalte der Webseite; Bewegungsmuster enthalten Informationen über privates wie auch dienstliches Leben). So zu tun, als würde diese Trennung für künftige Kommunikationsdienste klarerweise bestehen bleiben, ist mehr als mutig (um nicht zu sagen: vollkommen gedankenlos).

- Die erreichbare Sicherheit auf Vorrat gespeicherter Daten hängt extrem davon ab, was unter „ohne schuldhaftes Zögern“ verstanden wird. Wenn dies bedeutet, dass der Auskunftsprozess mehrere Tage dauern darf, dann können mehrere Menschen gemeinsam den Auskunftsprozess durchführen und insoweit kann dann auch eine technisch keineswegs sichere IT ziemlich sicher betrieben werden. Zugespitzt ist also die Frage: Bestimmt ein Zeitraum, der sich aus der Definition der Bedarfsträger oder Gerichte ergibt, was unter „ohne schuldhaftes Zögern“ verstanden wird, die erreichbare Sicherheit. Oder bestimmt eine Definition, was unter „genügend sicher“ zu verstehen ist, die Zeiträume, die dann unter „ohne schuldhaftes Zögern“ verstanden werden.

- Die Frage eines Ausgleichs zwischen Datenschutz und Überwachbarkeit kann nicht für einzelne Dienste und Technologien sinnvoll beantwortet werden, sondern nur dienst- und technologieübergreifend.

- Im Gegensatz zum Innenministerium sind wir der Meinung, dass überwachungsfreie Räume für Menschen als soziale Wesen notwendig sind (und technische Eliten sie sich und anderen sowieso schaffen werden).

Fragenkatalog

Verfassungsbeschwerden

1 BvR 256/08, 263/08 und 586/08

Zusammenfassung

Zu den Verkehrsdaten im Allgemeinen:

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

Informationen über das Ziel der Kommunikation, manche Adressen, z. B. MAC-Adressen (dies sind Adressen, die einzelnen Geräten zugeordnet und weltweit eindeutig sind. Sie werden in lokalen Netzen (LANs) verwendet.) und Port-Nummern sowie eine Vielzahl weiterer Protokollinformationen, die im Einzelnen nicht vollständig aufzählbar sind.

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

Dies können nur die jeweiligen Erbringer von Telekommunikationsdienstleistungen beantworten.

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

Hierzu liegen uns keine Informationen vor.

Zu einzelnen Verkehrsdaten:

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.

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

Ja, insbesondere aus den Absender-IP-Adressen.

    - 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?

Ja, die gemäß §113a Absatz 2 Satz 1 Nr. 1-4 spezifizierten Angaben für öffentliche Telefondienstanbieter in Kombination mit den in §113a Absatz 4 Satz 1 Nr. 1-3

spezifizierten Angaben für Anbieter von Internetzugangsdienst sind zu speichern. Aus den gespeicherten Daten lassen sich Bewegungsprofile durch die Benutzung mautpflichtiger Strassen erzeugen.

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

Aus theoretischer Sicht ist dies nicht zwingend notwendig – aus praktischer Sicht bei den heutigen Mobilkommunikationssystemen schon.

- 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?

Ja, bezüglich des Erzeugens von Verkehrsdaten. Darüber hinaus sind uns keine Informationen bekannt.

5. Kommt in der Praxis der in § 113a Abs. 2 Satz 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?

Der Fall kommt nicht vor. Über die Bedeutung für Strafverfolgung kann nur spekuliert werden.

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?

Hierbei fällt die vom Endgerät verwendete und in der Regel durch den Hot Spot vergebene Absender-IP-Adresse an. Diese alleine sind einer einzelnen Person nicht zuordenbar. Im Falle eines kommerziellen Dienstes besitzt der Anbieter aber regelmäßig weitere Informationen, mit deren Hilfe eine Zuordnung zu einer Person üblicherweise ermöglicht wird.

Zu den zur Speicherung Verpflichteten:

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

Dies ist bisher unklar. In der Praxis existiert kein einheitliches Vorgehen.

8. Wie wird in der Praxis behandelt, wer (wie Unternehmen für ihre Mitarbeiter, Vereine für ihre Mitglieder oder Universitäten für ihre Angehörigen) Telekommu-

nikationsdienste nur für einen begrenzten Nutzerkreis anbietet? Wird insoweit von öffentlich zugänglichen Telekommunikationsdiensten ausgegangen, deren Erbringer zur Vorratsdatenspeicherung verpflichtet sind?

Nein, es besteht nach unserer Kenntnis keine Verpflichtung zur Vorratsdatenspeicherung.

Zu mittels Telekommunikation begangenen Straftaten:

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?

Dazu liegen keine belastbaren Informationen vor.

Zur Auskunftserteilung nach § 113 TKG:

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

Hierzu ist nichts bekannt. Im übrigen wird auch nicht gesehen, dass § 113b S. 1 Hs. 2 i. V. m. § 113 TKG für die Zuordnung von IP-Adressen relevant ist.

Zur Sicherung der Vorratsdaten gegen unbefugte Zugriffe:

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?

Es existiert eine Vielzahl von Dokumenten über mögliche Maßstäbe der „erforderlichen Sorgfalt“. Allein es mangelt an verpflichtenden Vorschriften.

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 Maßnahmen kommen kryptographischen Verfahren zur Verschlüsselung und zur Integritätssicherung in Kombination mit organisatorischen Maßnahmen in Betracht. Diese Maßnahmen sind auf eine regelmäßig Überprüfung und Aktualisierung angewiesen. Ein wirklich sicherer Schutz der Vorratsdaten scheint in Praxis jedoch nicht möglich zu sein. Dies insbesondere dann nicht, wenn die gespeicherten Daten im Falle ihrer Anforderung durch Bedarfsträger unverzüglich übermittelt werden oder gar in deren Online-Zugriff sein sollen.

Zur Ausgestaltung der Nutzung:

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

Hierzu ist nichts bekannt.

Ausführliche Beantwortung der Fragen

Zu den Verkehrsdaten im Allgemeinen:

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

Für die nachfolgende Beantwortung der Frage sind zwei Vorbemerkungen notwendig: (a) ist es insbesondere bei Internet-basierter elektronischer Kommunikation oftmals schwierig zu entscheiden, ob es sich um Telekommunikation oder um Telemedien handelt. Insofern erfolgt die Beantwortung der Frage ohne diese Unterscheidung zu berücksichtigen, d.h. manche der gemachten Angaben könnten insofern hinfällig sein, sofern es sich bei dem betreffenden Dienst um ein reines Telemedium handelt. (b) ist insbesondere im Bereich der „neuen Dienste“ (die wiederum häufig Internet-basiert sind) unklar, welche Verkehrsdaten bereits durch §113a TKG erfasst sind. §113a TKG Absatz 4 Satz 1 Nr. 1 spricht zunächst ganz explizit von Internetprotokoll-Adressen (kurz: IP-Adressen). Nr. 2 erwähnt ferner „eine eindeutige Kennung des Anschlusses“. Nachfragen bei der Bundesnetzagentur, die wir bezüglich der zu speichernden Daten bei einem von uns betriebenen Anonymisierungsdienst gestellt hatten, haben ergeben, dass die BNetzA aus Nr. 2 (in Kombination mit Absatz 6) ableitet, dass „… neben der Ein- und Ausgangs-IP-Adresse jede Angabe, die … zur Rückverfolgung eines Signals erforderlich ist“ zu speichern ist. Schließt man sich dieser Auffassung an, so wären per Definition alle (relevanten) Verkehrsdaten durch §113a TKG erfasst. Im Gegensatz zur Meinung der BNetzA werden für die nachfolgende Beantwortung der oben genannten Frage nur die explizit im Gesetz erwähnten Daten (Adressen, Kennungen) berücksichtigt.

Absatz 8 regelt, dass „der Inhalt der Kommunikation und Daten über aufgerufene Internetseiten“ nicht gespeichert werden dürfen. Die Bundesnetzagentur hat im Gespräch bestätigt, dass der Begriff der „Internetseite“ allgemeiner verstanden werden kann, so dass in der Regel keine Angaben über das Ziel (Internet-basierter) Kommunikation zu speichern sind, also beispielsweise Ziel-IP-Adressen, Ziel-Portnummern etc.

Nicht zu erfassen sind bei Internet-basierter Kommunikation darüber hinaus die (eindeutigen) Geräteadressen der benutzten Endgeräte (sogenannte MAC-Adressen[1]). In jedem IP-Paket werden außerdem eine Reihe weiterer Daten übertragen, die als Protokollinformationen nicht den Inhaltsdaten zuzurechnen sind und die trotzdem gemäß §113a TKG nicht zu speichern sind. Dabei ist ferner zu berücksichtigen, dass die grundlegenden Protokolle des Internet (IP, UDP, TCP) auf eine flexible Erweiterbarkeit ausgelegt sind, d. h. dass sich die übermittelten Protokollinformationen nicht

[1] Bei einer MAC-Adresse handelt es sich um eine der Netzschnittstelle zugewiesene Adresse, die unterhalb des Internet-Protokolls verwendet wird. Die Zuweisung erfolgt in der Regel durch den Hersteller, wobei die Adresse weltweit eindeutig sein sollte. Allerdings ist oftmals eine Veränderung der MAC-Adresse durch den (technisch versierten) Nutzer möglich.

abschließend aufzählen lassen, da sich zwei Kommunikationspartner stets auf eigene, neue Protokollerweiterungen einigen können.

Letztlich können sich zwei Kommunikationspartner – dank der Offenheit und Flexibilität des Internets – auf vollkommen eigene und neue Protokolle einigen, bei denen dann auch neue Arten von Verkehrsdaten anfallen, die bisher nicht in §113a TKG erfasst sind. Dies ist sicher ein wesentlicher Unterschied zu eher „klassischen" Telekommunikationsdiensten wie Festnetz- oder Mobiltelefonie, bei denen sich die anfallenden Verkehrsdaten abschließend aufzählen lassen.

Schwierigkeiten können sich auch durch die Schichtenarchitektur des Internets ergeben. Dabei ist es so, dass höhere Schichten niedrigere Schichten für den Datentransport benutzen. Bei diesen Daten handelt es sich sowohl um Protokolldaten (also beispielsweise Adreßinformationen) als auch Inhaltsdaten. Da die niedrigere Schicht die „Bedeutung" der Daten aber nicht kennt, stellen sich für diese Schicht die Daten insgesamt schlicht als Inhaltsdaten dar, die dann gemäß §113a TKG Absatz 8 nicht zu speichern wären. Auch aus diesem Grund bedarf es für jede (neue) Internet-basierte Anwendung einer Einzelfallentscheidung, welche Daten als Verkehrsdaten zu speichern sind und welche als Inhaltsdaten anzusehen und folglich nicht zu speichern sind. Diese Entscheidung wird insbesondere auch dann schwierig, wenn Verkehrs- und Inhaltsdaten kaum zu trennen sind. Als Beispiel sei folgende URL betrachtet: http://www.google.de/search?q=aids Auf der einen Seite handelt es sich klar um Adreßinformationen bezüglich des Ziels einer Web-Anfrage. Auf der anderen Seite enthält die URL aber auch Inhaltsdaten, da aus ihr hervorgeht, dass jemand nach dem Suchbegriff „aids" gesucht hat.

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

Vor dem Hintergrund des BSI-Gesetzesentwurfes (BT-Drucksachen 16/11967 und 16/12225) können zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen Bestands- und Verkehrsdaten so umfänglich erhoben und gespeichert werden, dass eine Eingrenzung nicht wirklich gegeben ist. Was in der Praxis wirklich erhoben wird, dürfte je nach Anbieter unterschiedlich sein.

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

Hierzu liegen uns keine Informationen vor.

Zu einzelnen Verkehrsdaten:

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.

    - Lassen sich auch aus anderen nach § 113a TKG zu speichernden Daten

Rückschlüsse auf das Bewegungsverhalten der Nutzer mobiler Telekommunikationsdienste ziehen?

Ja, dies ist unter anderem ganz allgemein an Hand der durch das Endgerät des Nutzers verwendeten IP-Adresse möglich, beispielsweise wenn der Nutzer über sogenannte Hot Spots (siehe Frage 6) auf das Internet zugreift. In der Regel erhält das Endgerät des Nutzers dabei eine IP-Adresse zugewiesen, die aus einem Adresspool kommt, den nur dieser Hot Spot verwendet (gleiches gilt für alle Zugangspunkte zum Internet, beispielsweise auch für Internet via Kabel in einem Hotelzimmer). Insofern lässt sich an Hand der zu speichernden IP-Adresse auf den verwendeten Hot Spot und somit letztlich auf den ungefähren Standort des Endgerätes schließen. Darüber hinaus lässt sich an Hand der verwendeten IP-Adresse feststellen, welcher „Zugangsanbieter" verwendet wird. Dies dürfte in der Regel für die private Nutzung zu Hause ein anderer als am Arbeitsplatz sein, so dass sich Bewegungen zwischen Arbeitsplatz und Wohnung nachvollziehen lassen. Es existieren darüber hinaus Internetdienste, die kostenfrei oder gegen geringes Entgelt, eine Zuordnung einer IP-Adresse zu einem ungefähren geographischen Standort vornehmen (beispielsweise: http://www.maxmind.com).

Eine Analyse, wie gut sich das Bewegungsverhalten an Hand von IP-Adressen analysieren lässt, ist dem Papier „Identity Trail: Covert Surveillance Using DNS" (http://petsymposium.org/2007/papers/PET2007_preproc_Identity_trail.pdf) zu entnehmen.

- 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?

Die Beantwortung der nachfolgenden Frage bezieht sich auf die im Internet frei zugänglichen Informationen über die Funktionsweise der On-Board-Unit (OBU) und deren Kommunikationsverhalten. Laut www.toll-collect.de übermittelt die OBU in regelmäßigen Abständen Daten über die zurückgelegte, mautpflichtigen Strecke an das Rechenzentrum von Toll Collect. Dazu wird vermutlich auf die im Mobilfunk (GSM) mögliche Datenübertragung zurückgegriffen[2]. Demzufolge sind die gemäß §113a Absatz 2 S. 1 Nr. 1-4 spezifizierten Angaben für öffentliche Telefondienstanbieter in Kombination mit den in §113a Absatz 4 S1. Nr. 1-3 spezifizierten Angaben für Internet-Dienst Anbieter zu speichern. Entsprechend lassen sich aus den auf Vorrat gespeicherten Daten Bewegungsprofile durch die Benutzung mautpflichtiger Strassen erzeugen.

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

[2] Informationen über die tatsächlich genutzte Art der Kommunikation liegen nicht vor. In den durch Toll Collect veröffentlichten Dokument ist zum einen zu lesen, dass eine „abgerüstete" SIM-Karte verwendet wird, die nur Datendienste unterstützt zum anderen wird erwähnt, dass zwischen OBU und Rechenzentrum verschlüsselte SMS-Nachrichten ausgetauscht werden.

Aus theoretischer Sicht ist dies nicht zwingend notwendig. In dem Buch „Sicherheit mobiler Kommunikation“[3] gibt Prof. Dr. Hannes Federrath einen umfangreichen Überblick über die zugrundeliegenden technischen Schutzmaßnahmen. Allerdings ist nicht bekannt, dass vergleichbare Maßnahmen in den in der Praxis betriebenen Mobilfunknetzen implementiert sind. Insofern bedeutet dies für die Betreiber, dass auf Grund der momentan benutzen technischen Infrastruktur Standortdaten von Mobiltelefonen auch im Standby-Betrieb gespeichert werden müssen, da sich andernfalls der Netzbetrieb nicht aufrecht erhalten lässt.

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

Gemäß der im Internet zu findenden Informationen über die Funktionsweise stiller SMS ist klar, dass sich diese dazu benutzen lassen, gezielt speicherungspflichtige Verkehrsdaten zu erzeugen. Ob Strafverfolgungsbehörden von dieser Möglichkeit tatsächlich Gebrauch machen ist uns nicht bekannt. Ebenso auf welcher rechtlichen Grundlage dies erfolgen würde.

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?

Zunächst ist unklar, auf welche Dienste mit der Bezeichnung „im Voraus bezahlter anonymer Dienst“ abgestellt werden soll. Klarer wäre dies, wenn im Gesetz von „im Voraus anonym bezahlter Dienste“ die Rede wäre. Geht man davon aus, dass mit der Formulierung die im Mobilfunk üblichen Prepaid-Angebote gemeint sind, so ist zumindest anzumerken, dass gemäß § 111 TKG Absatz 1 Daten über den Anschlussinhaber erhoben werden müssen, so dass eine anonyme Dienstnutzung nicht möglich ist und insofern der in § 113a Abs. 2 S. 1 Nr. 4 d TKG geregelte Fall in Praxis zur Zeit nicht vorkommt. Diese Auffassung lässt sich auch der Gesetzesbegründung entnehmen: „Die Regelung des Buchstaben d kann derzeit in Deutschland auch deshalb weitgehend leerlaufen, weil anonyme Telefondienste aufgrund der bereits bestehenden Pflicht zur Bestandsdatenerhebung nach § 111 TKG kaum vorkommen dürften.“

Einzig die Tatsache, dass in Praxis die Überprüfung der zu erhebenden Bestandsdaten nicht mit der notwendigen Sorgfalt erfolgt oder Prepaid-Karten weitergegeben werden können und werden und somit leicht falsche Angaben gemacht werden bzw. entstehen können, könnte ein Indiz dafür sein, dass für die Strafverfolgung eine Bedeutung in der Speicherung der oben erwähnten Angaben liegt, da Strafverfolgungsbehörden mit Hilfe

[3] Hannes Federrath: „Sicherheit mobiler Kommunikation - Schutz in GSM-Netzen, Mobilitätsmanagement, mehrseitige Sicherheit“, DuD-Fachbeiträge, Vieweg, Wiesbaden 1999.

der gespeicherten Angaben eventuell weitere Informationen über den tatsächlichen Anschlussinhaber gewinnen können. Ob diese Vermutung zutreffend ist, kann allerdings nicht gesagt werden.

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?

Hierbei fällt die vom Endgerät verwendete und in der Regel durch den Hot Spot vergebene Absender-IP-Adresse an. Für die Benutzung eines offenen WLAN-Anschlusses ist es in der Regel nicht notwendig, persönliche Daten (etwa in Form einer Autorisierung mit Hilfe von Login/Paßwort) anzugeben. Insofern werden in diesem Fall keine einem einzelnen Nutzer zuordenbaren Daten gespeichert. Anders sieht es in der Regel bei der Benutzung eines kommerziellen WLAN-Dienstes aus. Hier ist vor Benutzung eine Authentifizierung notwendig. Speichert der Diensteanbieter die bei der Authentifizierung gemachten Angaben zusammen mit der zugewiesenen IP-Adresse, so lässt sich mit Hilfe dieser Informationen und der durch den Hot Spot auf Vorrat gespeicherten IP-Adresse üblicherweise ein Bezug zu einzelnen Nutzern herstellen.

Zukünftig ist darüber hinaus vorstellbar, dass im Zug der Umstellung auf das neue Internetprotokoll der Version 6 (IPv6) jeder Nutzer eines kommerziellen Hot Spot Zugangs eine persönliche, weltweit gleichbleibende IP-Adresse zugewiesen bekommt – unabhängig davon, welchen Hot Spot er konkret verwendet. Dies ist vergleichbar dem internationalen Roaming bei mobilen Telefondiensten, bei dem die dem Telefongerät zugewiesene Telefonnummer unabhängig vom Aufenthaltsort (d.h. dem verwendeten Funkmast) ist.

Zu den zur Speicherung Verpflichteten:

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

Bezüglich der Speicherungspflicht für einen unentgeltlich angebotenen Dienst gibt es zur Zeit wenigstens zwei unterschiedliche Auffassung, die sich aus der Formulierung „in der Regel“ ergeben. Während Breyer[4] zu der Auffassung gelangt, dass es tatsächlich darauf ankommt, ob ein konkreter Dienst unentgeltlich angeboten wird oder nicht, argumentiert Mayer[5] anders, dass es auf die Branchenüblichkeit einer Entgeltpflicht ankommt. Mithin sich also die Frage stellt, ob die betreffende Dienst*art* in der Regel

[4] Patrick Breyer: *Keine Vorratsdatenspeicherung für unentgeltliche Dienste [6. Ergänzung]*, Version vom 23. November 2008, 18.03 Uhr, http://www.daten-speicherung.de/index.php/keine-vorratsdatenspeicherung-fuer-unentgeltliche-dienste/

[5] Christoph Mayer: Pflicht zur Vorratsdatenspeicherung bei unentgeltlichen E-Mail-Diensten? Die Definition des Telekommunikationsdienstes gem. § 3 Nr. 24 TKG und ihre Auswirkungen auf die Vorratsdatenspeicherung, Kommunikation & Recht, Heft 5, Jahrgang 2009, Verlag Recht und Wirtschaft, Frankfurt a. M., Mai 2009, 313-317.

gegen Entgelt angeboten wird, so dass in diesem Fall auch ein (konkreter) unentgeltlich angebotener Dienst speicherpflichtig ist.

Eine Klärung dieser Frage ist durchaus relevant, da in Praxis auf tatsächlich unentgeltliche (also auch nicht durch Werbung oder ähnliches finanzierte) Dienste durch die Vorratsdatenspeicherung erhebliche Kosten zukommen könnten. Darüber hinaus lässt sich momentan in Praxis kein einheitliches Vorgehen verschiedener Anbieter unentgeltlicher Dienste erkennen. So speichern einige Betreiber von Servern des kostenfreien Anonymisierungsdienstes „Tor“ keine Vorratsdaten, während einige Betreiber von Servern des gleichfalls kostenfreien Anonymisierungsdienstes „AN.ON“ dies tun.

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?

Die in Beantwortung von Frage 1 erwähnte Anfrage an die Bundesnetzagentur hat auf unserer Frage: „ob es zutrifft, dass Telefonanlagen von Behörden und Unternehmen keiner Speicherpflicht von Verbindungsdaten unterliegen“ als Antwort ergeben, dass: „Eine Speicherpflicht besteht in der Regel nicht. Behörden und Unternehmen sind als Endnutzer selbst zwar noch Abnehmer öffentlich zugänglicher Telekommunikationsdienste. Der darauf beruhenden Bereitstellung von Telefondiensten für ihre Mitarbeiter und Bedienstet fehlt es dagegen i.d.R. am Merkmal öffentlicher Zugänglichkeit. Dies gilt auch für eine gelegentliche Mitnutzung derart nicht-öffentlicher Telekommunikationsdienste durch Dritte. Die Grenze zur öffentlichen Zugänglichkeit ist allerdings fließend und ist im Einzelfall von der konkreten Ausgestaltung abhängig.“ Im Gespräch mit der BNetzA wurde beispielsweise der (hypothetische) Fall einer Bibliothek diskutiert, die im Lesesaal / Aufenthaltsbereich einen drahtlosen Internet-Zugang (mittels WLAN) anbietet. Auch hier besteht nach Auffassung der BNetzA in der Regel keine Verpflichtung zur Vorratsdatenspeicherung.

Die TU Dresden sieht sich ebenso als Anbieter von Telekommunikationsdiensten für eine geschlossene Benutzergruppe, so dass auch an der TU Dresden keine Vorratsdatenspeicherung erfolgt.

<u>Zu mittels Telekommunikation begangenen Straftaten:</u>

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?

Dazu liegen keine belastbaren Informationen vor. Insbesondere sind viele von Bedarfsträgern und Politikern öffentlich angeführten Beispiele fragwürdig, da alternative Ermittlungsmethoden, seien es konventionelle oder auch high-tech Methoden der Computer-Forensik, üblicherweise nicht genannt werden.

Zur Auskunftserteilung nach § 113 TKG:

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

Derartige andere Zwecke sind nicht bekannt. Im übrigen sehen wir – als juristische Laien – auch nicht, inwiefern § 113b S. 1 Hs. 2 i. V. m. § 113 TKG relevant sein sollte für die Zuordnung von IP-Adressen. In § 113b S. 1 Hs. 2 i. V. m. § 113 TKG wird wiederum auf §§ 95 und 111 bezüglich der zu beauskunftenden Daten verweisen. Hier scheint einzig § 111 relevant. In diesem findet sich Absatz 1 Satz 1 Nr. 1 die Verpflichtung zur Speicherung (und gemäß §113 dann zur Beauskunftung) von „Rufnummern und anderen Anschlusskennungen". Gemäß § 3 Satz 1 Nr. 18 TKG ist klar, dass eine IP-Adresse keine Rufnummer ist. Eine IP-Adresse ist aber auch keine Anschlusskennung. Dies ergibt sich unter anderem aus § 113a Absatz 4 Satz 1 Nr. 1, 2. Hier ist nämlich vorgeschrieben, dass die IP-Adresse *und* die Anschlusskennung zu speichern sind – insofern kann eine IP-Adresse eben gerade nicht eine Anschlusskennung sein. Zusammenfassend lässt sich also feststellen, dass nach §113 i. V. m. § 111 keine Verpflichtung zur Speicherung von IP-Adressen oder zur Auskunftserteilung über diese besteht. Insofern kann diese Auskunft auch nicht durch § 113b S. 1 Hs. 2 i. V. m. § 113 TKG erlangt werden.

Zur Sicherung der Vorratsdaten gegen unbefugte Zugriffe:

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? –

Es existiert eine Vielzahl von Dokumenten über mögliche Maßstäbe der „erforderlichen Sorgfalt". Allein es mangelt an verpflichtenden Vorschriften wie auch realistischer Umsetzung in der Praxis.

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?

Die beiden Fragen sollen im Komplex beantwortet werden. Zu den Maßstäben bezüglich der Sorgfaltspflicht im Telekommunikationsbereich lässt sich feststellen, dass angefangen von Leitfäden von Branchenverbänden wie etwa dem „Leitfaden Verschlüsselung von Bestandsdaten aus Rechenzentrumssicht“ des BITKOM, über die verschiedenen BSI Standards, zu denen die bekannten „IT-Grundschutz-Kataloge“ gehören bis hin zu internationalen Standards etwa der ISO oder der ITU eine Vielzahl von Empfehlungen und Richtlinien existiert, aus denen sich die oben erwähnten Maßstäbe ableiten lassen. Allerdings ist unklar, welche Empfehlungen und Richtlinien auf Grund welcher gesetzlichen Regelungen für einen konkreten Telekommunikationsanbieter tatsächlich als verbindlicher Maßstab zu betrachten sind.

Bezüglich der Vorratsdatenspeicherung lässt sich hier noch am ehesten die im Rahmen der von der Bundesnetzagentur auf Grundlage der TKÜV zu erlassende Technische Richtlinie (TR TKÜV) heranziehen. Diese Richtlinie befindet sich momentan in der Überarbeitung, um die Belange der Vorratsdatenspeicherung zu berücksichtigen. Den nachfolgenden Ausführungen liegt der öffentlich verfügbare Bearbeitungsstand vom 21. April 2009 zu Grunde.[6] In diesem Entwurf ist im Teil B die „Technische Umsetzung gesetzlicher Maßnahmen zum Auskunftsersuchen für Verkehrsdaten“ geregelt. Dabei wird im Wesentlichen auf die durch das European Telecommunications Standards Institute (ETSI) veröffentlichte technische Spezifikation TS 102 657 „Lawful Interception (LI); Retained Data; Handover interface for the request and delivery of retained data“ zurückgegriffen und diese Spezifikation konkretisiert.

Das ETSI hat mit dem Dokument TS 102 657 einen Standard zur Abfrage und Übermittlung von auf Vorrat gespeicherten Daten veröffentlicht. Sicherheitsmaßnahmen zur Wahrung von Vertraulichkeit, Integrität und Zurechenbarkeit werden zwar vorgeschlagen, sind aber als „optional“ gekennzeichnet und deren Anwendung nationalstaatlichen Regelungen überlassen. In dem Entwurf der TR TKÜV ist dabei vorgesehen, dass die Übermittlung der Vorratsdaten mit Hilfe Internet-basierter Kommunikation erfolgt, wobei diese durch die Verwendung eines VPNs gesichert ist. Dies bedeutet, dass auf dem Übertragungswege die Daten gegen Kenntnisnahme und unbemerkte Veränderung durch Dritte geschützt sind. Allerdings sind keine Maßnahmen bezüglich der Zurechenbarkeit der übermittelten Daten auf Anwendungsebene vorgesehen. Dies bedeutet beispielsweise, dass weder Anfragen noch Auskünfte durch die jeweiligen Parteien digital signiert werden müssen. Kommt es im Nachhinein zum Streit über die Richtigkeit der übermittelten Verkehrsdaten, so lässt sich nicht mehr feststellen, ob die Daten bereits fehlerhaft durch den Absender übermittelt oder durch den Empfänger verändert wurden.

Im Teil C des Entwurfs ist ferner beschrieben, wie eine gesicherte elektronische Übermittlung von Anordnungen und Auskunftsersuchen erfolgen kann. Allerdings ist die Umsetzung optional, da „die Übermittlung der Kopie der Anordnung weiterhin auch per Telefax möglich bleibt. Dies gilt im Übrigen gemäß der aktuellen Version der

[6] Bundesnetzagentur: - Entwurf - Technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation und zum Auskunftersuchen für Verkehrsdaten (TR TKÜV), Ausgabe 6.0 (Entwurf vom 21.04.2009)

TKÜV auch für die nach Teil B der technischen Richtlinie zu übermittelnden Verkehrsdaten. Allerdings geht die Bundesnetzagentur davon aus, dass mit einer zukünftigen Änderung der TKÜV nur noch die elektronische Übermittlung zulässig ist.

Neben dem bereits erwähnten ETSI Standard 102 657 existieren noch zwei weitere ETSI Standards, die im Zusammenhang mit der Vorratsdatenspeicherung Relevanz besitzen: Das ETSI Dokument TR 102 661 „Lawful Interception (LI); Security framework in Lawful Interception and Retained Data environment“ beschreibt den organisatorischen und technischen Rahmen zur sicheren Aufbewahrung der auf Vorrat gespeicherten Daten. Das ETSI Dokument TS 102 656 „Lawful Interception (LI); Retained Data; Requirements of Law Enforcement Agencies for handling Retained Data“ beschreibt die Anforderungen aus Sicht von Strafverfolgungsbehörden an das Auskunftsverfahren über auf Vorrat gespeicherte Daten. Insofern könnten auch diese Dokumente Relevanz bezüglich der nationalen Regelungen zur technischen Umsetzung der Vorratsdatenspeicherung erlangen – allerdings werden sie bisher weder durch den Entwurf der TR TKÜV noch durch die ETSI Spezifikation TS 102 657 referenziert.

Insbesondere das Dokument ETSI 102 661 beschreibt recht umfangreich, welche organisatorischen und technischen Maßnahmen zur Sicherung der auf Vorrat gespeicherten Daten vorzunehmen sind. Wären alle der dort beschriebenen Vorkehrungen verpflichtend für die Anbieter von Telekommunikationsdiensten, so könnte man von einem durchaus akzeptablen Grundschutz der auf Vorrat gespeicherten Daten sprechen.

Zusammenfassend kann man zunächst feststellen, dass in Praxis durchaus viele sinnvolle Maßnahmen diskutiert werden – allein es fehlen die klaren Verpflichtungen diese Maßnahmen auch umzusetzen.

Nachfolgend soll darauf eingegangen werden, welcher Schutz der Vorratsdaten aus wissenschaftlicher Sicht theoretisch möglich ist und wo die jeweiligen Schwierigkeiten bei einer praktischen Umsetzung liegen. Letztere ergeben sich dabei zum einen auf Grund der vorliegen gesetzlichen Regelungen und sind zum anderen inhärent technischer Natur.

Zu ersterem lässt sich anmerken, dass ein genereller Konflikt besteht zwischen der Forderung „durch technische und organisatorische Maßnahmen sicherzustellen, dass der Zugang zu den gespeicherten Daten ausschließlich hierzu von ihm besonders ermächtigten Personen möglich ist.“ auf der einen Seite und auf der anderen Seite zu verlangen, dass „Die Speicherung der Daten … so zu erfolgen [hat], dass Auskunftsersuchen der berechtigten Stellen unverzüglich beantwortet werden können.“ Wird beispielsweise zum Zugriff auf die Vorratsdaten technisch ein Mehr-Augen-Prinzip erzwungen, so ist dies natürlich positiv für den Schutz der Vorratsdaten vor unberechtigtem Zugriff. Auf der anderen Seite erfordert es im Falle eines Auskunftsersuchens aber auch, dass die notwendigen Personen verfügbar sind, um die Anfrage zu beantworten. Es ergibt sich also im Allgemein ein negativer Einfluss auf die unverzügliche Beantwortbarkeit von Anfragen.

Ein anderer negativer Einfluss auf den Schutz der Vorratsdaten ergibt sich aus den Regelungen zur Aufwandsentschädigung. Da Vorratsdatenspeicherung nicht zum Kerngeschäft eines Telekommunikationsanbieters gehört, ist klar, dass er nur ein absolutes Mindestmaß an Investitionen tätigen wird bzw. höchstens soviel investiert, wie ihm gemäß Entschädigungsregelung an Entschädigung zusteht. Betrachtet man beispielsweise die aktuellen anfragebezogenen Entschädigungen, so ist klar, dass sich nicht mehrere Mitarbeiter eines Telekommunikationsunternehmens mit der Bearbeitung einer einzelnen Anfrage beschäftigen können. Insofern scheidet eine konsequente Umsetzung eines Mehr-Augen-Prinzips von vornherein aus.

Zu den Technik inhärenten Problemen ist anzumerken, dass zwar in der Theorie viele Verfahren bekannt sind, die eine sichere Speicherung der Vorratsdaten ermöglichen, so dass sich die Anforderungen nach §113a TKG Absatz 10 umsetzen ließen – jedoch handelt es sich bei dem IT-System zur Speicherung und Beauskunftung um ein komplexes System und die Erfahrungen haben ebenso gezeigt, dass es nicht möglich ist, ein solches System fehlerfrei zu realisieren. Als Beispiel sei die große Zahl von regelmäßig veröffentlichten Sicherheitsupdates aus dem Betriebssystembereich genannt. Diese Sicherheitsupdates reagieren dabei keineswegs auf bis dahin nicht bekannte neue Bedrohungen – sie reparieren vielmehr Fehler, die sich bei der Implementierung ergeben haben. Dabei ist zusätzlich zu berücksichtigen, dass die prinzipiellen Fehlerursachen seit Jahren bekannt und wohluntersucht sind. Obwohl also bekannt ist, vorauf bei einer sicheren Umsetzung im Betriebssystembereich besonders zu achten ist und obwohl große IT-Unternehmen große Anstrengungen bezüglich der Sicherheit unternehmen, ist es ihnen trotzdem nicht möglich, die erwähnten Fehler zu vermeiden. Geht man nun im Falle der Vorratsdatenspeicherung von einer eher geringen Investitionsbereitschaft aus, so ist klar, dass eine auch nur annähernd fehlerfreie Umsetzung der theoretischen Konzepte nicht erfolgen wird. Dabei kommt erschwerend hinzu, dass – ebenfalls aus Kostengründen – die Telekommunikationsanbieter keine jeweils unabhängig entwickelten Lösungen verwenden werden, sondern eine Entwicklung eines Drittanbieters einkaufen werden, wobei nicht davon auszugehen ist, dass es sehr viele unterschiedliche derartige Anbieter geben wird. Insofern werden auch hier die bekannten IT-Sicherheitsprobleme eintreten, die sich aus Monokulturen ergeben. Diese liegen unter anderem darin, dass es für einen Angreifer lohnend ist, Schwachstellen in dem angebotenen System zur Vorratsdatenspeicherung zu suchen, da er dann die Systeme vieler Telekommunikationsanbieter kompromittieren kann.

Nach der Schilderung der generelle Probleme, die eine wirklich sichere Speicherung der Vorratsdaten verhindern, sollen einige der möglichen aus der Theorie bekannten Verfahren zum Schutz der Vorratsdaten zumindest kurz erwähnt werden. Notwendig ist dabei zunächst in jedem Falle eine Verschlüsselung der auf Vorrat zu speichernden Daten – und zwar spätestens unmittelbar vor der ersten Aufzeichnung auf Datenträgern. Darüber hinaus ist mit geeigneten Verfahren wie beispielsweise Hashwerten bzw. digitalen Signaturen sicher zu stellen, dass Manipulationen an den auf Vorrat gespeicherten Daten erkannt werden. Die verwendeten kryptographischen Schlüssel sind sicher zu speichern. Dies bedeutet, dass sie nur zum Zeitpunkt einer Auskunftserteilung durch ein IT-System zugreifbar sein dürfen und andernfalls an einem auch physisch gesicherten Ort aufzubewahren sind. Der Zugriff auf die Schlüssel

ist durch geeignete Authentisierungsverfahren zu schützen – hierzu sollte mindestens die Eingabe eines Geheimnisses (PIN) notwendig sein. Empfehlenswert wäre natürlich die Umsetzung eines Mehr-Augen-Prinzips, das heißt, dass der Zugriff auf die geheimen Schlüssel durch mehrere Personen autorisiert werden muss bzw. dass ein Entschlüsseln der Vorratsdaten nur durch die Verwendung mehrerer unterschiedlicher geheimer Schlüssel möglich ist. Zusätzlich sollten als Medien für den Schlüsselspeicher Geräte verwendet werden, die auch im Falle eines Diebstahls einen gewissen Schutz der Schlüsseldaten bieten (sogenannte „tamper resistant" Geräte). Smartcards bieten beispielsweise diesen minimalen Schutz – wohingegen eine gewöhnliche Festplatte oder ein USB-Stick als nicht ausreichend angesehen werden kann. Darüber hinaus sollte dieses Gerät die Möglichkeit haben, Kenntnis über die aktuelle Zeit zu erlagen. Somit kann das Gerät den Zugriff auf die Schlüssel (und in der Konsequenz letztlich die Entschlüsselung von gespeicherten Daten) verweigern, wenn diese Daten älter als 6 Monate sind. Insofern handelt es sich um eine technische Unterstützung der Forderung aus §113a Absatz 11.

In jedem Fall hat der Zugriff auf die Schlüssel und somit letztlich die Beauskunftung unter Benutzung eines besonders geschützten IT-Systems zu erfolgen. Dies bedeutet im Minimum, dass keinerlei Verbindung zu irgendeinem Rechnernetz bestehen darf. Generell sind alle Zugriffe auf die Vorratsdaten und die benutzten kryptographischen Schlüssel revisionssicher zu protokollieren. Dabei ist sicher zu stellen, dass diejenigen, die Zugriff auf die Vorratsdaten und die zugehörigen Schlüssel haben, keinen Zugriff auf die protokollierten Audit-Daten haben.

Abschließend ist festzustellen, dass jegliche IT-Systeme, die zur Umsetzung der Vorratsdatenspeicherung und zum Schutz der gespeicherten Daten eingesetzt werden ebenso wie die damit verbundenen organisatorischen Prozesse auf eine ständige Überprüfung angewiesen sind. Der Sicherheitsexperte Bruce Schneier formulierte dazu treffend: „Sicherheit ist ein Prozess – kein Zustand." Inwieweit Telekommunikationsanbieter tatsächlich gesetzlich zu einer fortlaufenden Überprüfung und Aktualisierung verpflichtet sind und inwieweit tatsächlich eine Überprüfung einer derartigen Verpflichtung erfolgt, ist unklar. Im TKG ist (beispielsweise in § 109) im Wesentlichen eine einmalige Abnahme durch die Bundesnetzagentur geregelt. Zwar finden sich Formulierungen wie: „Sofern sich die dem Sicherheitskonzept zu Grunde liegenden Gegebenheiten ändern, hat der Betreiber das Konzept anzupassen und der Bundesnetzagentur unter Hinweis auf die Änderungen erneut vorzulegen." Daraus lässt sich aber sicher nicht die Verpflichtung zu einer regelmäßigen Überprüfung ableiten. Zwar kann die Bundesnetzagentur gemäß §115 TKG prinzipiell zu jeder Zeit eine Überprüfung der Einhaltung der Vorschriften vornehmen, jedoch ist sie dazu nicht verpflichtet und insofern ist unklar, inwieweit eine Überprüfung durch die Bundesnetzagentur in Praxis tatsächlich erfolgt.

Zur Ausgestaltung der Nutzung:

13. Welche Instrumente (z. B. Kennzeichnungs-, Löschungs- und Auskunftspflichten, Richtervorbehalte, Benachrichtigungspflichten, die eine ergänzende nachträgliche Gerichtskontrolle gewährleisten, oder – eventuell auch immaterielle – Scha-

denersatzansprüche bei rechtswidrigem Datenzugriff) werden zur Einhegung und rechtstaatlichen Kontrolle der Nutzung der nach § 113a TKG zu speichernden Daten diskutiert? Worin liegen ihre Vor- und Nachteile?

Hierzu ist uns nichts bekannt. Der Gesetzgeber erlaubt sich diesbezüglich vollständige Ignoranz, insbesondere was technische Sicherheitsprobleme beim Schutz großer Datensammlungen, die im kurzfristigen Zugriff für Berechtigte sein sollen, gegen unberechtigten Zugriff (etwa organisierte Kriminalität oder fremde, insbesondere auch feindliche Geheimdienste) angeht.