

FRAGENKATALOG
ZUR BESTANDSAUFNAHME HINSICHTLICH DER WIRKUNGSWEISE DER RICHTLINIE
ÜBER DIE VORRATSSPEICHERUNG VON DATEN, DIE BEI DER BEREITSTELLUNG ÖFFENTLICH ZU-
GÄNGLICHER ELEKTRONISCHER KOMMUNIKATIONSDIENSTE ODER ÖFFENTLICHER KOMMUNIKA-
TIONSNETZE ERZEUGT ODER VERARBEITET WERDEN, UND ZUR ÄNDERUNG DER RICHTLINIE
2002/58/EG

30.09.2009

EINLEITUNG

- Umfang des Fragenkatalogs

Mit diesem Fragenkatalog sollen Informationen über alle maßgeblichen Aspekte der Wirkungsweise der Richtlinie über die Vorratsdatenspeicherung eingeholt werden, damit die Kommission sich einen möglichst umfassenden Überblick über ihre praktische Anwendung verschaffen kann. Die Kommission wird insbesondere auf dieser Grundlage die in Artikel 14 der Richtlinie erwähnte Bewertung vornehmen, die am 15. September 2010 vorzulegen ist.

Der Fragenkatalog ist an die vier Gruppen gerichtet, die als Akteure an der Anwendung der Richtlinie über die Vorratsdatenspeicherung (im Folgenden als Richtlinie bezeichnet) beteiligt sind, d. h. an die Mitgliedstaaten, den privaten Sektor, Datenschutzbehörden und das Europäische Parlament, und er beinhaltet für diese Akteure jeweils ein Kapitel (Näheres dazu im Folgenden unter „beteiligte Akteure“).

Darüber hinaus möchte die Kommission Kapitel 1 des Fragenkatalogs als Leitfaden für die Gespräche verwenden, die sie mit den Mitgliedstaaten und den EWR-Ländern, die nicht EU-Mitgliedstaaten sind, jeweils einzeln zwischen Ende September und Ende November nach einem bei dem Treffen am 10. September 2009 abzustimmenden Zeitplan zu führen beabsichtigt.

Die **erste Gruppe** von Fragen stellt darauf ab, der Europäischen Kommission die nötigen Rückmeldungen zu verschaffen, damit sie die Bewertung der Richtlinie nach Artikel 14 vornehmen kann.

Artikel 14 der Richtlinie lautet:

1. Die Kommission legt dem Europäischen Parlament und dem Rat spätestens am 15. September 2010 eine Bewertung der Anwendung dieser Richtlinie sowie ihrer Auswirkungen auf die Wirtschaftsbeteiligten und die Verbraucher vor, um festzustellen, ob die Bestimmungen dieser Richtlinie, insbesondere die Liste von Daten in Artikel 5 und die in Artikel 6 vorgesehenen Speicherungsfristen, gegebenenfalls geändert werden müssen; hierbei berücksichtigt sie die Weiterentwicklung der Technologie der elektronischen Kommunikation und die ihr gemäß Artikel 10 zur Verfügung gestellte Statistik. Die Ergebnisse dieser Bewertung werden öffentlich gemacht.

2. Die Kommission prüft zu diesem Zweck sämtliche Kommentare, die ihr von den Mitgliedstaaten oder der gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzten Datenschutzgruppe übermittelt werden.

Die Mitgliedstaaten sind nach Artikel 10 der Richtlinie verpflichtet, der Kommission jährlich eine Statistik über die Vorratsspeicherung von Daten zu übermitteln. Die Datenerfassungsmaske wurde von der Expertengruppe für Vorratsdatenspeicherung entwickelt und den Mitgliedstaaten bei ihrem Treffen am 22. Januar 2009 in Brüssel vorgestellt.

Die **für die Vornahme der Bewertung nötigen Angaben** stammen aus einer Vielzahl von Quellen, nämlich den nach Artikel 10 der Richtlinie übermittelten Statistiken, der Beurteilung des technischen Fortschritts und der Marktfolgen, aber auch aus strafverfolgungsspezifischen Informationen; so soll festgestellt werden, ob die in Artikel 5 enthaltene Liste von Daten und die in Artikel 6 bestimmten Speicherungsfristen angemessen und ausreichend sind.

Mit der **zweiten Gruppe** von Fragen sollen Rückmeldungen eingeholt werden, damit die Untersuchung vorgenommen werden kann, um die der JI-Rat bei seinem Treffen am 27. und 28. November 2008 ersucht hat. In seinen Schlussfolgerungen (**siehe Anlage**) hat der Rat die Kommission gebeten, die Wirksamkeit bestehender legislativer, nicht-legislativer oder technischer Maßnahmen zur Sicherstellung der Rückverfolgbarkeit der Nutzer von Kommunikationsdiensten, insbesondere von Mobiltelefonen mit vorausbezahlter SIM-Karte, zu bewerten. Die Mitgliedstaaten haben sich verpflichtet, „auf Ersuchen der Europäischen Kommission alle zweckdienlichen Informationen über die legislativen, nicht-legislativen oder technischen Lösungen, die ergriffen werden, um die Nutzer der elektronischen Kommunikation zu identifizieren, sowie über den Grad der operativen Wirksamkeit dieser Lösungen zu übermitteln“. Dieser Fragenkatalog enthält die konkreten Ersuchen der Kommission um Übermittlung dieser zweckdienlichen Informationen.

Die Bewertung wird sich somit auf zwei Bereiche erstrecken, nämlich darauf zu beurteilen,

- inwieweit die Richtlinie über die Vorratsdatenspeicherung ihren Zweck erfüllt, d.h. inwieweit mit der Harmonisierung der Pflichten für Informationsdiensteanbieter (im Folgenden als ISPs bezeichnet) gewährleistet werden kann, dass Daten zum Zweck der Ermittlung, Feststellung und Verfolgung von schweren Straftaten zur Verfügung stehen, und
- inwieweit sich nationale Maßnahmen zur rückverfolgenden Identifizierung von Nutzern bei der Bekämpfung der kriminellen Zwecken dienenden Nutzung der elektronischen Kommunikation und ihrer Anonymität als wirksam erwiesen haben.

- Beteiligte Akteure

Die zu diesen beiden Fragenkonstellationen zu beteiligenden Akteure sind:

1. EU-Mitgliedstaaten und EWR-Staaten und insbesondere (a) Strafverfolgungsbehörden (Ministerien des Innern und der Justiz) und (b) Telekommunikationsbehörden (Ministerium für Telekommunikation, nationale Regulierungsbehörden) (zu Kapitel 1 des Fragenkatalogs),
2. das Europäische Parlament und die Zivilgesellschaft (zu Kapitel 2 des Fragenkatalogs),
3. nationale Datenschutzbehörden und der Europäische Datenschutzbeauftragte (EDSB) (zu Kapitel 3 des Fragenkatalogs),
4. der private Sektor (Kommunikationsdiensteanbieter, darunter Internetdiensteanbieter, Festnetz- und Mobilfunkanbieter, Netz- und Kabelbetreiber usw.) (zu Kapitel 4 des Fragenkatalogs).

- Erarbeitung des Fragenkatalogs

Der Fragenkatalog wurde von der GD Justiz, Freiheit und Sicherheit und der GD Informationsgesellschaft und Medien insbesondere auf der Grundlage der Vorgaben aus der Konferenz „Wege zur Bewertung der Richtlinie über die Vorratsdatenspeicherung“ vom 14. Mai 2009 erarbeitet. Er wurde von der Arbeitsgruppe „Bewertung“ der Expertengruppe für Vorratsdatenspeicherung am 9. September 2009 erstmals beraten und den Vertretern der Mitgliedstaaten am 10. September 2009 in einer Sitzung in der Sicherheitszone der DG Justiz, Freiheit und Sicherheit in Brüssel vorgestellt. Die Kommission bat die Vertreter, die an dieser Sitzung teilgenommen hatten, um Stellungnahme bis zum 17. September 2009 und erarbeitete anschließend den endgültigen Fragenkatalog.

In der aktuellen Fassung sind die Stellungnahmen folgender Staaten (in der alphabetischer Reihenfolge) berücksichtigt: Deutschland, Estland, Finnland, Frankreich, Griechenland, Lettland, Österreich, Rumänien, Schweden, Spanien, Tschechische Republik, Ungarn, Vereinigtes Königreich.

In der Arbeitsgruppe „Bewertung“ sind dieselben Gruppen von Akteuren vertreten wie in der Expertengruppe für Vorratsdatenspeicherung. Sie besteht aus jeweils 2 - 3 Vertretern aus den Mitgliedstaaten, der Industrie, den Datenschutzbehörden und dem Europäischen Parlament.

Der Fragenkatalog wird das zentrale Element in dem Bewertungsprozess sein.

- Inhalt des Fragenkatalogs

Der Fragenkatalog besteht aus zwei Arten von Fragen: *Qualitativen Fragen*, bei denen es um die Modalitäten und Bedingungen der Durchführung der Richtlinie geht, und *quantitativen Fragen* zur Messung von Datenmengen, finanziellen, technischen und rechtlichen Auswirkungen sowie Verhältniszahlen zwischen verschiedenen Teilbereichen.

Die Arbeitsgruppe „Bewertung“ war der Auffassung, dass die Beantwortung der qualitativen Fragen weniger Zeit beanspruchen werde als die Bereitstellung der quantitativen Daten.

Im Fragenkatalog sind alle quantitativ zu beantwortenden Fragen wie folgt gekennzeichnet: „[Quantitative Antwort]“. Alle übrigen nicht so gekennzeichneten Fragen sind qualitative Fragen.

- Zeitplan für die Beantwortung der Fragen

Diese Fassung des Fragenkatalogs wurde während des Treffens am 10. September 2009 an die Mitgliedstaaten verteilt. Die Kommission bat die Mitgliedstaaten im Hinblick auf die spätere Erstellung eines endgültigen Fragenkatalogs um Stellungnahme zu Inhalt und Form der Fragen bis zum 17. September.

Nach Auffassung der Arbeitsgruppe „Bewertung“ ist für die Beantwortung der qualitativen Fragen ein Zeitraum von acht Wochen und für die Zusammenstellung der zur Beantwortung der quantitativen Fragen erforderlichen Daten ein Zeitraum von zwölf Wochen angemessen.

Ausgehend von dieser Einschätzung möchte die Kommission die ersten Antworten von den einzelnen Gruppen der Akteure im Rahmen des sie jeweils betreffenden Kapitels (siehe „Beteiligte Akteure“) auf die Fragen des erstgenannten Typs bis spätestens 15. November 2009 und auf die Fragen des zweitgenannten Typs (quantitativ) bis spätestens 15. Dezember 2009 erhalten.

Verarbeitung vertraulicher oder geheimhaltungsbedürftiger Informationen

Nach den Transparenzvorschriften kann es sein, dass die Kommission Informationen auf Anfrage verbreiten muss, wenn Akteure nicht in Bezug auf alle oder einige (ausdrücklich bezeichnete) Antworten zu dem Fragenkatalog angeben, dass sie unter die in Artikel 4 Absatz 1 bzw. 2 der Verordnung 1049/2001/EG genannten Ausnahmen fallen. Die Kommission beabsichtigt, die Antworten ausschließlich zum Zweck der Bewertung zu verwenden. Zusammengefasste oder anonymisierte Ergebnisse können, ohne dass sie einzelnen Akteuren zugeordnet werden können, in den Bericht einfließen, um z. B. bestimmte in der Bewertung enthaltene Positionen und Aussagen zu veranschaulichen.

Mit den Antworten auf bestimmte Fragen könnten vertrauliche oder geheimhaltungsbedürftige Informationen offengelegt werden.

Die Befragten werden gebeten, **in ihren Antworten zu dem Fragenkatalog anzugeben**, ob Antworten als vertraulich oder geheimhaltungsbedürftig (EU VERTRAULICH oder EU GEHEIM) zu behandeln sind, und **diese Antworten** nach dem entsprechenden Verfahren **gesondert zu übersenden**.

Die Kommission wird sicherstellen, dass den bei ihr eingehenden Informationen innerhalb ihrer Organisation ein Schutzniveau zuteil wird, das dem Schutzniveau entspricht, das durch Maßnahmen gewährleistet wird, die der betreffende Akteur für diese Informationen getroffen hat. Die Akteure werden gebeten, solche Maßnahmen zu benennen und die Informationen dementsprechend zu übermitteln. So gekennzeichnete Informationen verbleiben in der Sicherheitszone und sind nur Personen zugänglich, die entsprechend ermächtigt sind.

Anmerkungen zu den Datenkategorien

Die Richtlinie über die Vorratsdatenspeicherung hat drei Arten von Betriebsdaten zum Gegenstand: 1. Daten betreffend das Telefonfestnetz; 2. Daten betreffend den Mobilfunk und 3. Daten betreffend Internetzugang, Internet-E-Mail und Internet-Telefonie.

Nach Auffassung der Arbeitsgruppe „Bewertung“ der Expertengruppe für Vorratsdatenspeicherung ist es, wenn genaue quantitative Daten (noch) nicht zur Verfügung gestellt werden können, einfacher, Verhältniszahlen zwischen den verschiedenen Kategorien von Daten anzugeben, zumal sich die Verhältniszahlen zwischen Internetdaten im Vergleich zu Telefoniedaten zugunsten der Internetdaten verschieben.

Anmerkung zur technischen Entwicklung

Nach Artikel 14 der Richtlinie ist bei der Bewertung „die Weiterentwicklung der Technologie der elektronischen Kommunikation“ zu berücksichtigen.

Der konvergente Markt hat die Technologie der Jahre 2004/2005, in denen die Richtlinie verfasst wurde, bereits hinter sich gelassen.

Neue mit 3G-GSM angebotene Breitbanddienste und WiFi-fähige Mobiltelefone z. B. haben Auswirkungen auf die Möglichkeit, in Netzen erzeugte Netzereignisse zu vergleichen. Alle Akteure werden gebeten, die Auswirkungen dieser und anderer Entwicklungen auf die Anwendung der Richtlinie zu berücksichtigen.

Definition des Begriffs „Anfrage“

Die Arbeitsgruppe „Bewertung“ hat darauf hingewiesen, dass eine einzelne „Anfrage“ (vgl. die Artikel 8 und 10 Abs. 1 der Richtlinie sowie 1.A.1 unten) mehrere (viele) „Daten“ betref-

fen kann. Die Zahl der Anfragen kann deshalb wesentlich kleiner sein als die Zahl der Daten, die übermittelt werden. In der Antwort sollte in Abhängigkeit vom Kontext jeweils die Gesamtzahl der Anfragen oder der übermittelten Daten angegeben werden.

Neben quantitativen Angaben, die aufschlussreiche Erkenntnisse z. B. in Bezug auf die Menge der verarbeiteten Daten oder die Auswirkungen der Richtlinie auf die Marktakteure ermöglichen, bedarf es einer qualitativen Bewertung, um u. a. festzustellen, ob die in Artikel 5 der Richtlinie enthaltene Liste von Daten oder die in Artikel 6 bestimmten Speicherungsfristen sachgerecht und wirksam sind, um das Ziel der Richtlinie, nämlich Ermittlung, Feststellung und Verfolgung von schweren Straftaten, zu verwirklichen. Zur Unterstützung der Untersuchungen in dieser Frage werden die Mitgliedstaaten insbesondere gebeten, Fallbeispiele für Strafverfolgungen zu übermitteln, bei denen sich auf Vorrat gespeicherte Daten in den Ermittlungs- und Strafverfahren als hilfreich erwiesen haben.

In der gesamten ersten Gruppe von Fragen (über die Bewertung der Richtlinie) wird der Ausdruck „Land“ verwendet, um der Tatsache Rechnung zu tragen, dass der Fragenkatalog nicht nur an die EU-Mitgliedstaaten gerichtet ist, sondern auch an EWR-Ländern, die nicht EU-Mitgliedstaaten sind.

Vorbemerkung

Gegen die innerstaatliche Umsetzung der Vorgaben der Richtlinie 2006/24/EG sind zahlreiche Verfassungsbeschwerden beim Bundesverfassungsgericht anhängig.

Das Bundesverfassungsgericht hat durch mehrere einstweilige Anordnungen die vom Gesetzgeber vorgesehenen Verwendungsmöglichkeiten für die auf Vorrat gespeicherten Daten im repressiven und präventiven Bereich bis zur Entscheidung in der Hauptsache eingeschränkt. Die Verpflichtung der Telekommunikations-Unternehmen zur Speicherung der Daten bleibt durch die einstweiligen Anordnungen jedoch unberührt. Am 15. Dezember 2009 hat das Bundesverfassungsgericht die Verfassungsbeschwerden mündlich verhandelt. Eine abschließende Entscheidung über die Verfassungsbeschwerden kann möglicherweise im 1. Quartal 2010 erwartet werden.

Am 27. September 2009 wurde der 17. Deutsche Bundestag gewählt. Diese Wahl änderte die Mehrheitsverhältnisse im Deutschen Bundestag. Mit der Wahl der Bundeskanzlerin und der Ernennung der Kabinettsmitglieder hat am 28. Oktober 2009 eine neue Bundesregierung ihre Arbeit aufgenommen. Der Koalitionsvertrag der die neue Bundesregierung stellenden Parteien CDU, CSU und FDP verweist zum Thema „Vorratsdatenspeicherung“ auf die noch ausstehende Entscheidung des Bundesverfassungsgerichts. Die Bewertung der Vorratsspeicherung von Daten durch die neue Bundesregierung kann daher noch nicht als abgeschlossen gelten.

Vor diesem Hintergrund erfolgt die nachstehende Beantwortung des Fragenkatalogs auf Grundlage einer rechtlich wie politisch vorläufigen Bewertung der innerstaatlichen Umsetzung der Richtlinie 2006/24/EG und der innerstaatlichen Verwendungsregelungen für „auf Vorrat“ gespeicherte Verkehrsdaten.

Soweit der Fragenkatalog quantitative Angaben zur Anwendung der Richtlinie betrifft, die über die nach Artikel 10 der Richtlinie zu übermittelnden Angaben hinausgehen, ist eine Beantwortung regelmäßig nicht möglich, da die entsprechenden Angaben im Kalenderjahr 2008 in Deutschland nicht erhoben wurden.

1 FRAGEN AN MITGLIEDSTAATEN UND EWR-LÄNDER, DIE NICHT EU-MITGLIEDSTAATEN SIND

1.A Qualitative und quantitative Aspekte der Anwendung der Richtlinie 2006/24/EG, unter Berücksichtigung der Weiterentwicklung der Technologie der elektronischen Kommunikation und der gemäß Artikel 10 zur Verfügung gestellten Statistik.

1.A.1 Fragen betreffend die Strafverfolgung

1.A.1.a *Gesamtzahl der pro Jahr gestellten Anfragen nach Daten, die nach der Richtlinie auf Vorrat gespeichert sind. [quantitative Antwort]*

Antwort: Im Kalenderjahr 2008 wurden im Bereich der Strafverfolgung 13.904 Anordnungen zur Erhebung von Verkehrsdaten nach § 100g Strafprozessordnung (StPO) erlassen (13.426 Erst- und 478 Verlängerungsanordnungen). Davon waren 9.363 Anordnungen auf Verkehrsdaten gerichtet, deren Alter bis zu drei Monate betrug, und 2.336 Anordnungen auf Verkehrsdaten gerichtet, deren Alter bis zu sechs Monaten betrug. 985 Anordnungen betrafen Daten mit einem Alter von mehr als sechs Monaten, die z. B. von den Diensteanbietern noch zu Abrechnungszwe-

cken gespeichert waren. 664 Anordnungen betrafen nur künftig anfallende Verkehrsdaten. Für 556 Anordnungen kann nicht angegeben werden, ob diese auf Vorrat zu speichernde Daten betrafen. In 931 Fällen blieb die Maßnahme erfolglos, weil die abgefragten Daten ganz oder teilweise nicht verfügbar waren (siehe **Anhang 1**). Anhang 1 stellt die deutsche Statistik nach Artikel 10 der Richtlinie dar.

1.A.1.b *Anzahl/Prozentsatz dieser Anfragen, aufgeschlüsselt nach der Art der ersuchenden Behörde: 1. Polizei-, 2. Justiz- und 3. andere Behörden (bitte entsprechend angeben). [quantitative Antwort]*

Antwort: Zu 2.: 100%

Anordnungen zur Erhebung von Verkehrsdaten im repressiven Bereich sind nach § 100g Absatz 2 Satz 1 in Verbindung mit (i. V. m.) § 100b Absatz 1 Strafprozessordnung auf Antrag der Staatsanwaltschaften nur auf Grund gerichtlicher Anordnung zulässig. Lediglich bei Gefahr im Verzug kann die Anordnung auch durch die Staatsanwaltschaft selbst getroffen werden. Wenn diese jedoch nicht binnen drei Tagen von dem Gericht bestätigt wird, tritt sie außer Kraft.

1.A.1.c *Zeitspanne zwischen dem Zeitpunkt der Vorratsdatenspeicherung und dem Zeitpunkt der Anfrage, mit der die zuständige Behörde um Übermittlung der Daten gebeten hat, oder, wenn diese Informationen nicht verfügbar sind, das durchschnittliche Alter der angefragten Daten. Die Antwort auf diese Frage wurde möglicherweise bereits im Zusammenhang mit der Statistik nach Artikel 10 der Richtlinie zur Vorratsdatenspeicherung gegeben. [quantitative Antwort]*

Antwort: Die Zahl der im Kalenderjahr 2008 erlassenen Anordnungen zur Erhebung von Verkehrsdaten nach § 100g Strafprozessordnung aufgeschlüsselt nach dem maximalen Alter der abgefragten Daten ist aus **Anhang 1** ersichtlich.

Aus dieser Statistik kann ein Mittelwert von 2,5 Monaten für das maximale Alter der abgefragten Verkehrsdaten innerhalb der gesetzlich vorgeschriebenen Speicherfrist von sechs Monaten abgeleitet werden.

1.A.1.d *Welche Kommunikationswege werden zum Austausch von Informationen zwischen Strafverfolgungsbehörden und Diensteanbietern genutzt (E-Mail, Fax, sicheres Netz oder sonstige Kommunikationswege)? Wenn bestimmte Kommunikationswege vorgeschrieben sind, machen Sie bitte Angaben zu den zu nutzenden Kommunikationswegen.*

Antwort: 1) Für Anordnungen:

- a) derzeit noch FAX und elektronische Übermittlung über Telekommunikationsverbindungen (IP-VPN), die Wahl der derzeitigen Übermittlungsverfahren beruht auf geübter Praxis, Rechtsvorschriften bestehen nicht;
- b) künftig ist nur noch elektronische Übermittlung vorgesehen.

2) Für Auskünfte:

- a) derzeit existiert für die Übermittlung der Auskünfte keine ausdrückliche Regelung (in der Regel werden Auskunftersuchen derzeit unter Nutzung des Übermittlungswegs beantwortet, auf dem das Ersuchen vorgelegt wurde, aber auch Ausdrucke wären nicht zu beanstanden);

- b) künftig: elektronisch über Telekommunikationsverbindungen (IP-VPN) und für kleine Betreiber bzw. Diensteanbieter, deren Teilnehmerzahl bzw. Zahl sonstiger Nutzungsberechtigter unterhalb einer Marginalgrenze liegt, Übermittlung auf Datenträger.

Bei der Nutzung von Telekommunikationsverbindungen ist technisch sicherzustellen, dass sowohl die Anordnung als auch die Auskünfte auf dem Übertragungsweg gegen unbefugte Kenntnisnahme durch Dritte geschützt sind.

Die Rechtsvorschriften zu 1b) und 2b) sollen in Form einer Ergänzung der bestehenden Telekommunikations-Überwachungsverordnung eingeführt werden, sie befinden sich derzeit im Entwurfsstadium, ein Inkrafttreten wird für Ende 2010 / Anfang 2011 angestrebt.

1.A.1.e Arten von Straftaten

1.A.1.e.1 Bei welchen Arten von Straftaten dürfen nach innerstaatlichem Recht auf Vorrat gespeicherte Daten erlangt und verwendet werden? Bitte übermitteln Sie eine Liste dieser Straftaten.

Antwort: Hinsichtlich der Verwendung von Verkehrsdaten wird in Deutschland unterschieden zwischen

- a. dem Fall der Übermittlung von Verkehrsdaten an die zuständigen Stellen und
- b. dem Fall, bei dem Verkehrsdaten betriebsintern von Diensteanbietern verwendet werden, um eine Auskunft über Bestandsdaten an die zuständigen Stellen erteilen zu können.

Zu a.

Übermittlung von Verkehrsdaten an die zuständigen Stellen:

Mit dem Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, das am 1. Januar 2008 in Kraft getreten ist, hat der Gesetzgeber vorgegeben, dass die auf Vorrat gespeicherten Daten zur Verfolgung von

- Straftaten von im Einzelfall erheblicher Bedeutung und
- Straftaten, die mittels Telekommunikation begangen wurden,

erhoben werden dürfen, soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich ist (§ 100g Absatz 1 Strafprozessordnung). Straftaten von im Einzelfall erheblicher Bedeutung sind solche, die mindestens dem mittleren Kriminalitätsbereich zuzuordnen sind, die den Rechtsfrieden erheblich stören und die geeignet sind, das Gefühl der Rechtssicherheit der Bevölkerung erheblich zu beeinträchtigen. Daher wird in der Regel bei Verbrechen (Mindeststrafe 1 Jahr) die erhebliche Bedeutung zu bejahen sein. Bei Vergehen wird vorauszusetzen sein, dass die Strafrahmengrenze über zwei Jahren liegt. Bagatelldelikte scheiden aus. Maßnahmen nach § 100g Strafprozessordnung dürfen grundsätzlich nur auf Antrag der Staatsanwaltschaften durch das Gericht angeordnet werden (§ 100g Absatz 2 i. V. m. § 100b Absatz 1 Strafprozessordnung).

Diese vom Gesetzgeber vorgesehenen Verwendungsmöglichkeiten wurden durch das Bundesverfassungsgericht durch einstweilige Anordnungen auf Grund von Verfassungsbeschwerden eingengt.

Mit einstweiliger Anordnung vom 11. März 2008 entschied das Gericht, dass bis zur Entscheidung in der Hauptsache die Diensteanbieter die allein auf Grund der Umsetzung der Richtlinie gespeicherten Daten nur dann an Strafverfolgungsbehörden übermitteln dürfen, wenn es sich um

- schwere Straftaten im Sinne des § 100a Absatz 1 und 2 Strafprozessordnung handelt (siehe **Anhang 2**) und
- die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre.

Schwere Straftaten sind Straftaten, die grundsätzlich mit einer Mindesthöchststrafe von 5 Jahren bewehrt sind und bei denen nach deutschem Recht auch das Abhören und Aufzeichnen des Inhalts der Telekommunikation zulässig ist.

Liegt keine solche Straftat vor, dürfen die angefragten Daten einstweilen nicht an die Strafverfolgungsbehörden übermittelt werden. Die Daten müssen in diesen Fällen vielmehr durch die Diensteanbieter bis zur Entscheidung in der Hauptsache aufbewahrt werden, auch über die Mindestspeicherungsfrist hinaus.

Mit der Wahl der Bundeskanzlerin und der Ernennung der neuen Kabinettsmitglieder hat am 28. Oktober 2009 eine neue Bundesregierung ihre Arbeit aufgenommen. Die Regierungsparteien (CDU, CSU, FDP) haben im Koalitionsvertrag vereinbart:

„Wir werden den Zugriff der Bundesbehörden auf die gespeicherten Vorratsdaten der Telekommunikationsunternehmen bis zur Entscheidung des Bundesverfassungsgerichts über die Verfassungsmäßigkeit der Vorratsdatenspeicherung aussetzen und bis dahin auf Zugriffe zur Abwehr einer konkreten Gefahr für Leib, Leben und Freiheit beschränken.“

An der Umsetzung dieser Vereinbarung wird derzeit gearbeitet.

Zu b.)

Betriebsinterne Verwendung von Verkehrsdaten durch den Diensteanbieter zur Auskunftserteilung über Bestandsdaten nach § 113 des Telekommunikationsgesetzes (siehe **Anhang 3**):

Diensteanbieter dürfen auf Vorrat gespeicherte Daten betriebsintern zum Zwecke einer Auskunftserteilung über Bestandsdaten gemäß § 113 des Telekommunikationsgesetzes verwenden.

Auskünfte über Bestandsdaten, d. h. über solche Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden (z. B. Name, Adresse, Rufnummer), richten sich nach den §§ 161, 163 Strafprozessordnung i. V. m. § 113 Telekommunikationsgesetz. Ein Fall der richterlichen Anordnung nach § 100 g der Strafprozessordnung liegt dann nicht vor.

Die allgemeine Eingriffsermächtigung nach §§ 161, 163 Strafprozessordnung ist von den Voraussetzungen her nicht auf bestimmte Straftaten beschränkt, unterliegt jedoch – wie alle strafprozessualen Eingriffsmaßnahmen – dem Grundsatz der Verhältnismäßigkeit (Übermaßverbot).

1.A.1.e.2

Wie ist das durchschnittliche Alter der angefragten Daten, aufgeschlüsselt nach den unter Punkt 1.A.1.e.1 genannten Arten von Straftaten? [quantitative Antwort]

Antwort: Hierzu liegen keine statistischen Erhebungen vor.

1.A.1.e.3 *Gestattet oder verbietet das innerstaatliche Recht, Daten von Kommunikationsanbietern, die der Richtlinie und/oder damit in Beziehung stehenden Instrumenten unterliegen, für andere Zwecke als zur Ermittlung, Feststellung und Verfolgung schwerer Straftaten zu erlangen (z. B. bei Urheberrechtsverletzungen)? Wenn ja, machen Sie bitte nähere Angaben zu dem alternativen Zweck/den alternativen Zwecken bzw. zu den Rechtsvorschriften, die die Erlangung von Daten zu diesem Zweck/diesen Zwecken verbieten.*

Antwort: Gespeicherte Verkehrsdaten dürfen außer für Zwecke der Verfolgung von Straftaten grundsätzlich auch

- zur Abwehr erheblicher Gefahren für die öffentliche Sicherheit sowie
- zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes und des Militärischen Abschirmdienstes

an die zuständigen Stellen übermittelt werden, soweit dies in den jeweiligen gesetzlichen Bestimmungen unter Bezugnahme auf § 113a des Telekommunikationsgesetzes vorgesehen und die Übermittlung im Einzelfall angeordnet ist (§ 113b Telekommunikationsgesetz).

Seit dem 1. Januar 2009 darf z. B. das Bundeskriminalamt (BKA) zur Abwehr einer im Bundeskriminalamtgesetz (BKAG) definierten (terroristischen) Gefahr diese Verkehrsdaten erheben (§ 20m BKAG). Die Erhebung darf nur auf Antrag der zuständigen BKA-Abteilungsleitung oder deren Vertretung durch das Gericht angeordnet werden (§ 20m Absatz 3 i. V. m. § 20l Absatz 3 BKAG), bei Gefahr im Verzug auch durch die Abteilungsleitung oder deren Vertretung. Ferner haben inzwischen einige Länder Vorschriften erlassen, wonach unter bestimmten Voraussetzungen zum Zwecke der Gefahrenabwehr (Baden-Württemberg, Bayern, Schleswig-Holstein, Thüringen) oder des Verfassungsschutzes (Bayern, Niedersachsen, Mecklenburg-Vorpommern, Schleswig-Holstein) auf Verkehrsdaten zugegriffen werden darf.

Durch die einstweilige Anordnung vom 28. Oktober 2008 hat das Bundesverfassungsgericht die Voraussetzungen, unter denen die gespeicherten Daten für Zwecke der Gefahrenabwehr oder der Dienste herausgegeben werden dürfen, wie folgt konkretisiert:

Die Daten sind an eine Gefahrenabwehrbehörde nur dann zu übermitteln, wenn

- dies im Gesetz ausdrücklich vorgesehen ist,
- die jeweiligen gesetzlichen Voraussetzungen vorliegen und
- die Daten zur Abwehr einer dringenden Gefahr für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder zur Abwehr einer gemeinen Gefahr erforderlich sind.

Die Daten sind an die Dienste nur dann zu übermitteln, wenn

- dies im Gesetz ausdrücklich vorgesehen ist (bislang nur der Fall in wenigen Ländern),
- die jeweiligen gesetzlichen Voraussetzungen vorliegen und
- zudem auch die Voraussetzungen von § 1 Absatz 1, § 3 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-

Gesetz) gegeben sind. In Bezug genommen sind damit die Voraussetzungen, unter denen die Dienste Telekommunikationsüberwachungsmaßnahmen durchführen dürften, nämlich zur Abwehr von drohenden Gefahren für die freiheitliche demokratische Grundordnung oder den Bestand oder die Sicherheit des Bundes oder eines Landes einschließlich der Sicherheit der in der Bundesrepublik Deutschland stationierten NATO-Truppen, soweit tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand eine der in § 3 des Artikel 10-Gesetzes näher aufgezählten Katalogtaten begangen hat.

Liegen die jeweils zuletzt genannten Voraussetzungen im Einzelfall nicht vor, hat das Telekommunikations-Unternehmen die Daten zu sichern, bis das Hauptsacheverfahren beim Bundesverfassungsgericht entschieden ist.

Weitere Einschränkungen sind durch die Koalitionsvereinbarung veranlasst (vgl. die Hinweise in der Antwort zu 1.A.1.e.1 unter zu Punkt a.).

Für allein zivilrechtliche Zwecke, z. B. Auskunftsanspruch bei Verletzung des Urheberrechtes, dürfen auf Vorrat gespeicherte Daten von den Telekommunikations-Unternehmen nicht herausgegeben werden.

1.A.1.e.4 *Beurteilung der auf Vorrat zu speichernden Daten*

1.A.1.e.5 *Verlangt das innerstaatliche Gesetz zur Umsetzung der Richtlinie zur Vorratsdatenspeicherung oder ein damit in Beziehung stehendes Instrument, dass zusätzlich zu den in Artikel 5 der Richtlinie genannten Daten noch andere Datenkategorien auf Vorrat gespeichert werden? Wenn ja, machen Sie bitte nähere Angaben zu den zusätzlichen Daten und zu dem Instrument, in dem diese Verpflichtung verankert ist.*

Antwort: Nein.

Es wird aber auf Folgendes hingewiesen:

§ 113a Absatz 6 des Telekommunikationsgesetzes verpflichtet denjenigen, der Telekommunikations-Dienste erbringt und hierbei auf Vorrat zu speichernden Angaben verändert, zur Speicherung der ursprünglichen und der neuen Angabe sowie des Zeitpunktes der Umschreibung dieser Angaben nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone.

Unter diese Vorschrift fallen z. B. Anonymisierungsdienste, die eine Veränderung der Quell-Internetprotokoll-Adresse bei der Übermittlung von Daten im Internet vornehmen. Ohne eine Verpflichtung dieser Anbieter ist die Vorgabe der Richtlinie, die zur Rückverfolgung und Identifizierung der Quelle einer Nachricht und zur Identifizierung des Adressaten benötigte Daten sicherzustellen, nicht zu erfüllen.

1.A.1.e.6 *Angemessenheit der nach Artikel 5 der Richtlinie auf Vorrat gespeicherten Daten und ihre Relevanz für die Strafverfolgung*

1.A.1.e.7 *Bitte geben Sie an, ob die von den Diensteanbietern nach Artikel 5 der Richtlinie auf Vorrat zu speichernden Daten im Hinblick auf die Strafverfolgung relevant und ausreichend sind, und geben Sie ferner an, welche Daten als redundant aus der Liste des Artikels 5 gestrichen werden sollten oder welche Daten, die relevant sind und noch nicht auf Vorrat gespeichert werden, hinzugefügt werden sollten.*

Die Mitgliedstaaten sind aufgefordert, ihre Antwort zu begründen und Beispiele zu nennen, die die Redundanz bzw. die Anforderungen der Strafverfolgung veranschaulichen.

Antwort: Aus dem Katalog des Artikels 5 der Richtlinie ist aus Sicht der Praxis nichts zu streichen.

1.A.1.f Zum Inhalt der Anfragen im Einzelnen

1.A.1.f.1 Die Art der Informationen, die von den Diensteanbietern abgerufen werden sollen; bitte machen Sie Angaben zu den typischen Suchparametern (Auswahlkriterien für die Informationen), die in Anfragen nach Vorratsdaten enthalten sind, z. B. eine Auflistung der Kommunikationsvorgänge, die von einer bestimmten Telefonnummer ausgingen, an eine bestimmte Telefonnummer gingen oder an einem bestimmten Datum oder zu einer bestimmten Uhrzeit erfolgten, oder eine Auflistung aller Anrufe, die von einem bestimmten Standort aus getätigt wurden, oder aller Telefonnummern, die von einem identifizierten Nutzer gewählt wurden.

Antwort: Anordnungen zur Erhebung von Verkehrsdaten nach § 100g Strafprozessordnung betreffen typischerweise Abfragen:

- zu einer Kennung,
- zu Verbindungen, die zu einer bestimmten Zieladresse hergestellt wurden,
- für eine benannte Funkzelle,
- für mehr als eine benannte Funkzelle,
- für einen bestimmten, durch eine Adresse bezeichneten Standort (in Fällen, in denen lediglich Ort und Zeitraum der Kommunikation bekannt sind),
- für eine bestimmte geografische Fläche,
- für eine bestimmte Wegstrecke,
- für künftig anfallende Verkehrsdaten in Echtzeit,
- über den letzten dem Netz bekannten Standort eines Mobiltelefons (Standortabfrage),
- über die Struktur von Funkzellen (z. B. Hauptstrahlrichtungen).

Von besonderer Relevanz als Suchparameter sind nach Rückmeldungen der Praxis insbesondere Funkzelle oder ein-/ausgehende Verbindungen. Zur Klarstellung: Eine Anfrage anhand von Suchparametern mit nahezu grenzenloser Streubreite ist schon ermittlungstaktisch nicht geboten, sondern die Parameter sind z. B. anhand des Zeitfensters so klein wie möglich zu halten.

1.A.1.f.2 Hat Ihr Land das Format für die Erlangung und Offenlegung von Kommunikationsdaten zwischen öffentlichen Stellen und Kommunikationsdiensteanbietern vereinheitlicht oder wird eine solche Vereinheitlichung angestrebt (z. B. in Dienstleistungsvereinbarungen oder durch Bezugnahme auf die entsprechenden ETSI-Standards)? Wenn ja, machen Sie bitte Angaben zu dem entsprechenden Standard (Formular oder Format) für Anfragen, dem Nachrichtenformat, den technischen Modalitäten und/oder der Schnittstelle.

Antwort: Deutschland vertritt seit Einführung der Standardisierungen im Lawful Interception-Bereich die Auffassung, dass die nationalen technischen Vorgaben so weit wie möglich den internationalen Standards entsprechen müssen. Abweichungen davon sind zu begründen.

Die gleiche Politik verfolgt Deutschland auch für den Bereich der Speicherung von Verkehrsdaten und der Auskunftserteilung, wobei es allerdings entsprechend den nationalen Gesetzen keine Vorgaben für die Datenspeicherung geben wird, sondern nur für die Auskunftserteilung.

Die technischen Festlegungen dazu werden in der „Technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation und zum Auskunftersuchen für Verkehrsdaten“ (TR TKÜV) getroffen, Ausgabe 6.0, Teil B und C, womit die Empfehlungen ETSI ES 201 671 / TS 101 671 und TS 102 232-01, TS 102 657 als national verbindlich festgelegt werden sollen. Der Entwurf für diese Ausgabe der TR TKÜV ist KOM am 28.07.2009 zur Notifizierung vorgelegt worden. Die Notifizierung ist mittlerweile abgeschlossen.

Im Vorfeld dazu nutzen bereits einige Bundesländer, z. B. Bayern und Nordrhein-Westfalen, und große Netzbetreiber eine sog. Elektronische Schnittstellen für Behörden (ESB), die unabhängig von der Richtlinie 2006/24/EG auf freiwilliger Basis von Telekommunikations-Unternehmen und Strafverfolgungsbehörden entwickelt wurde.

1.A.1.g *Inhalt der Antworten auf die unter Punkt I.A.1.f genannten Anfragen im Einzelnen*

Antwort: Typischerweise umfasst die Antwort eine den Suchparametern entsprechende Auswahl der nach der innerstaatlichen Umsetzung der Richtlinie auf Vorrat zu speichernden Daten oder es wird mitgeteilt, dass keine Daten vorliegen.

1.A.1.h *Gestatten die innerstaatlichen Rechtsvorschriften über die Erlangung von Kommunikationsdaten der öffentlichen Stelle, die Frist zu benennen, innerhalb deren die Daten offenzulegen sind, worauf in der Richtlinie mit der Formulierung „unverzüglich“ Bezug genommen wird?*

Antwort: Nach den in Deutschland geltenden Rechtsvorschriften (z. B. § 100b Absatz 3 Satz 3 i. V. m. § 100g Absatz 2 Strafprozessordnung) sind die erforderlichen Auskünfte unverzüglich zu erteilen. Ob und in welchem Umfang hierfür Vorkehrungen zu treffen sind, bestimmt sich nach dem Telekommunikationsgesetz (TKG) und der Telekommunikations-Überwachungsverordnung (TKÜV).

Ein konkreter Zeitrahmen für die Beantwortung von Auskunftersuchen ist hingegen nicht vorgeschrieben. Im Entwurf für die Ergänzung der TKÜV sind jedoch Obergrenzen für die organisatorischen und technischen Reaktionszeiten vorgesehen. Die von den Telekommunikations-Unternehmen zu treffenden Vorkehrungen müssen so gestaltet sein, dass diese Vorgaben im Regelfall eingehalten werden.

Wenn ja:

1.A.1.h.1 *Bitte nennen Sie Beispiele für Fristen, die auf Grundlage der innerstaatlichen Gesetzgebung oder im Wege von Dienstleistungsvereinbarungen zwischen den zuständigen Behörden und Kommunikationsanbieter durchsetzbar sind.*

Antwort: Überlegungen zu den unter 1.A.h.1 erwähnten Fristenvorgaben gehen dahin, dass unterschieden wird zwischen Fristen für die organisatorische Umsetzung einer Anordnung (Entgegennahme und Prüfung) und Fristen für deren betriebliche Umsetzung. Die Unternehmen sollen verpflichtet werden, organisatorische Vorkehrungen dergestalt zu treffen, dass sie Anordnungen zur Erteilung von Auskünften über Verkehrsdaten innerhalb ihrer üblichen Geschäftszeit jederzeit entgegennehmen können und außerhalb der Geschäftszeiten spätestens innerhalb von sechs Stunden. Für die betriebliche Umsetzung sollen höchstens zulässige Umsetzungsfristen in Abhängigkeit von der Art der jeweiligen Telekommunikationsanlage festgelegt werden. Es wird erwartet, dass die betriebliche Umsetzung im Regelfall innerhalb weniger Stunden möglich ist. Für einzelne, besonders dringliche Ermittlungen sollen im Bedarfsfall kürzere Reaktionszeiten möglich sein. Voraussetzung für eine Auskunftserteilung ist aber in allen Fällen, dass dem Verpflichteten die Daten bereits vorliegen. In Fällen von internationalem Roaming oder speziellen Konfigurationen der Telekommunikationsanlage kann es allerdings vorkommen, dass bestimmte Verkehrsdaten erst nach einigen Tagen oder später vollständig vorliegen.

1.A.1.h.2 *Welche Maßnahmen werden von den zuständigen Behörden ergriffen, um die Einhaltung der Frist für die Beantwortung der Anfrage zu gewährleisten?*

Antwort: Die Bundesnetzagentur ist für die Durchsetzung der Vorschriften des Telekommunikationsgesetzes und der Telekommunikations-Überwachungsverordnung und damit auch für die Einhaltung der Speicherungspflichten zuständig. § 115 Telekommunikationsgesetz sieht insoweit u. a. den Erlass von Anordnungen, die Festsetzung von Zwangsgeldern und ggf. sogar die Untersagung des Telekommunikations-Betriebs vor. Daneben können Verstöße der Telekommunikations-Unternehmen gegen die Speicherungs- bzw. sonstigen Vorkehrungspflichten nach Maßgabe des § 149 Telekommunikationsgesetz als Ordnungswidrigkeit mit Bußgeld in beträchtlicher Höhe geahndet werden.

Nach § 95 Absatz 2 i. V. m. § 100b Absatz 3 Satz 3 und § 100g Absatz 2 Strafprozessordnung haben die Strafverfolgungsbehörden für den Fall, dass ein Telekommunikations-Unternehmen sich weigert, unverzüglich Auskunft zu erteilen, die Möglichkeit, die in § 70 Strafprozessordnung bestimmten Ordnungs- und Zwangsmittel (Ordnungsgeld, Ordnungshaft) zu ergreifen.

1.A.1.h.3 *Unterscheiden die zuständigen Behörden gegebenenfalls bei Fristen, innerhalb deren sie die Offenlegung von Daten verlangen, nach den Kommunikationsanbietern und der Art der Anfrage oder der Art der von ihnen benötigten Daten? Wenn ja, nennen Sie bitte Beispiele für diese Unterscheidung.*

Antwort: Eine Unterscheidung erfolgt nur im Einzelfall. In Eilfällen wird die Eilbedürftigkeit z. B. im Anfragefax explizit vermerkt oder auch direkt telefonisch Kontakt mit dem Diensteanbieter aufgenommen. Dies kann im Einzelfall zu einer Beschleunigung der Auskunftserteilung führen.

1.A.1.i *Kostenerstattung*

1.A.1.i.1 *Erstattet Ihr Land Investitionskosten (CAPEX¹) und/oder Betriebskosten (OPEX²), die den Diensteanbietern entstehen? Wenn ja, machen Sie bitte Angaben zu den Kostenarten, die erstattet werden, sowie zu den Modalitäten und der Höhe oder Quote der Erstattung.*

Antwort: Die Kosten, die den Telekommunikations-Unternehmen bei der Speicherung von Daten auf Vorrat entstehen, werden nicht entschädigt.

Die Frage, ob insoweit die entschädigungslose Inanspruchnahme von Telekommunikations-Unternehmen verfassungsrechtlich zulässig ist, ist Gegenstand von Verfahren vor dem Bundesverfassungsgericht.

Eine Entschädigung der Telekommunikations-Unternehmen erfolgt jedoch für die Erteilung von Auskünften über Verkehrsdaten im Einzelfall. Die Erteilung von Auskünften wird nach dem Justizvergütungs- und -entschädigungsgesetz (JVEG) (vgl. **Anhang 4**) z. B. wie folgt entschädigt:

Für Auskünfte über gespeicherte Verkehrsdaten werden für jede Kennung, die der Auskunftserteilung zugrunde liegt, 30,00 € gezahlt. Für Auskünfte zu Verbindungen, die zu einer bestimmten Zieladresse hergestellt wurden, durch Suche in allen Datensätzen der abgehenden Verbindungen eines Betreibers (Zielwahlsuche) werden je abgefragte Zieladresse 90,00 € gezahlt. Bei der Abfrage von Verkehrsdaten bestimmter Funkzellen beträgt die Entschädigung 30,00 € für eine Funkzelle und 4,00 € für jede weitere Funkzelle. Bei Funkzellen für bestimmte Adressen, nach Flächen oder Strecken erfolgt die Pauschalierung der Entschädigung nach der kalkulierten Anzahl von Funkzellen in Blöcken (60,00 €, 110,00 €, 190,00 €, 490,00 €, 930,00 €).

Bei der Kalkulation der Pauschalen sind nur die durch die einzelne Datenabfrage entstehenden Kosten, nicht aber Investitionskosten berücksichtigt.

1.A.1.i.2 *Macht Ihr Land die Kostenerstattung von der Einhaltung bestimmter Bedingungen abhängig, z. B. von der Garantie einer bestimmten Dienstgüte (Anfrageprofile, Menge der zu bearbeitenden Anfragen, Abfragegeschwindigkeit)? Wenn ja, machen Sie bitte Angaben zu den Bedingungen, die die Diensteanbieter erfüllen müssen, und dazu, wie diese mit dem Erstattungssystem zusammenhängen.*

Antwort: Nur in Bezug auf die Art der Datenabfrage im Einzelfall, siehe Antwort zu 1.A.1.i.1

1.A.1.j *Wirksamkeit – wie ist die Erfolgsquote der Verwendung von Vorratsdaten?*

Antwort: Statistiken zu Erfolgsquoten werden nicht geführt. Aus den vorläufigen Ergebnissen einer Sondererhebung können jedoch Erkenntnisse abgeleitet werden, in welchem Maß die Aufklärung von Straftaten vereitelt bzw. erschwert wurde, weil Auskunftersuchen über Verkehrsdaten erfolglos blieben.

¹ CAPEX (CAPital EXpenditure) sind Ausgaben, die zukünftige Nutzeffekte schaffen. Konkret handelt es sich um die Kosten der Entwicklung und Bereitstellung nicht-verbrauchbarer Bestandteile des Produkts oder Systems, die auch Personalkosten und Ausgaben für Anlagen wie Miete/Pacht und Versorgungsdienstleistungen einschließen können.

² OPEX (OPerational EXpenditure) sind **Betriebskosten** oder fortlaufende Ausgaben, die mit dem Betrieb eines Unternehmens oder einer Vorrichtung, eines Bauteils, eines Ausrüstungsgegenstands oder einer Anlage zusammenhängen.

Die Sondererhebung wurde auf Grund von einstweiligen Anordnungen des Bundesverfassungsgerichts durchgeführt und umfasst den Zeitraum vom 1. Mai 2008 bis einschließlich 31. August 2009. Sie betrifft die Fälle, in denen im repressiven Bereich Anordnungen zur Erhebung von Verkehrsdaten erlassen wurden, d.h. Anordnungen nach § 100g Strafprozessordnung.

In dem 16-Monats-Zeitraum ergingen in 10.359 Ermittlungsverfahren insgesamt 20.524 Anordnungen zur Erhebung von Verkehrsdaten. Bei 423 Anordnungen blieb das Auskunftersuchen (ganz oder teilweise) erfolglos, weil die Verpflichtung zur Speicherung von Daten auf Vorrat von den Telekommunikations-Unternehmen (ganz oder teilweise) noch nicht erfüllt wurde bzw. erfüllt werden musste. In 449 Verfahren musste das Auskunftersuchen (ganz oder teilweise) erfolglos bleiben, weil es sich nicht um schwere Straftaten nach § 100a Absatz 1 und 2 Strafprozessordnung handelte und die Verkehrsdaten in diesen Fällen auf Grund von einstweiligen Anordnungen des Bundesverfassungsgerichts bis zur Entscheidung in der Hauptsache nicht beauskunftet werden dürfen.

Die Erfolglosigkeit des Auskunftersuchens hat die Aufklärung von Straftaten in 300 Ermittlungsverfahren vereitelt und in 116 Ermittlungsverfahren erschwert. In 57 Ermittlungsverfahren hatte bzw. wird die Erfolglosigkeit des Auskunftersuchens keine nachteiligen Auswirkungen auf das Ermittlungsverfahren haben. Damit liegen zu 473 Verfahren (300 + 116 + 57) Aussagen zu den Auswirkungen der Erfolglosigkeit des Auskunftersuchens vor.

Im Erhebungszeitraum führten erfolglose Auskunftersuchen zu Verkehrsdaten in 63% der betroffenen Verfahren dazu, dass die Aufklärung der Straftat vereitelt wurde, in 25% der betroffenen Verfahren erschwert wurde und in 12% der betroffenen Verfahren zu keinen nachteiligen Auswirkungen auf das Ermittlungsverfahren.

1.A.1.j.1 War die Verwendung von Vorratsdaten bei der gerichtlichen Feststellung und/oder Verfolgung von Straftaten hilfreich, die sonst gescheitert wäre? Wenn ja, nennen Sie bitte Beispiele. [erfordert möglicherweise quantitative Angaben]

Antwort: Die Erhebung und Verwendung von Verkehrsdaten ist nach Berichten aus der Praxis ein hilfreiches Instrument zur Verfolgung von Straftaten.

Aus der Praxis sind hierzu Beispiele berichtet worden; eine Differenzierung zwischen Verkehrsdaten, die als Vorratsdaten gespeichert waren, und solchen, die die Telekommunikationsunternehmen ohnehin zu geschäftlichen Zwecken (insbesondere zu Abrechnungszwecken) gespeichert hatten, ist den Berichten aus der Praxis nicht stets zu entnehmen. Vor diesem Hintergrund sind beispielhaft folgende Fälle aus der Praxis zu nennen:

- Ein Fall der Staatsanwaltschaft Traunstein hatte einen Mord (§ 211 des Strafgesetzbuches (StGB)) zum Gegenstand. Die im Wege der Rechtshilfe eingeholten Verbindungsdaten des Mobiltelefons des Getöteten befähigten die Ermittler zur genauen zeitlichen und örtlichen Rekonstruktion der von diesem mit den beiden Verdächtigen zurückgelegten Fahrstrecke. Dies trug wesentlich zur Überführung der Täter bei.
- Im Verfahren der Bundesanwaltschaft zur „Sauerlandgruppe“, der die Planung von Bombenanschlägen auf US-Einrichtungen vorgeworfen wird, konnten durch die Erhebung und Auswertung von Verkehrsdaten Erkenntnisse zu den Kommunikationsvorgängen erhoben werden, die der Vorbereitung der beabsichtigten Anschläge dienten. Ohne die Erhebung und Auswertung von Verkehrsdaten hätten diese Erkenntnisse nicht oder nur mit zeitlichem Verzug erlangt werden können.

1.A.1.j.2 *Was kostet die Verwendung von Vorratsdaten, was den Personaleinsatz und die Beschaffung und Wartung der speziell für diesen Zweck bestimmten Ausrüstung betrifft? Was sind die typischen Kostentreiber? [quantitative Antwort]*

Antwort: Hierzu sind keine belastbaren Angaben möglich.

1.A.1.j.3 *Wie kann die Kostenwirksamkeit der Erlangung und Verwendung von Vorratsdaten erhöht werden? [erfordert quantitative Angaben]*

Antwort: Da keine belastbaren Angaben zu den Kosten bei der Verwendung von Vorratsdaten möglich sind (vgl. Frage 1.A.1.j.2), sind auch Aussagen zu Erhöhung der Kostenwirksamkeit nicht möglich.

1.A.2 Nationale und transnationale Anfragen und Antworten

1.A.2.a *In diesem Fragenkatalog bedeutet „transnationale Anfrage“ eine grenzüberschreitende Anfrage zur Erlangung von Kommunikationsdaten zwischen EU-Mitgliedstaaten bzw. EWR-Ländern, die nicht EU-Mitgliedstaaten sind, wobei entweder*

1.A.2.a.1 *Sie von Strafverfolgungsbehörden aus einem anderen Land um Übermittlung von Daten ersucht werden, die von Diensteanbietern in Ihrem Land auf Vorrat gespeichert werden („eingehende Anfragen“), oder*

1.A.2.a.2 *Ihre zuständigen Behörden Anfragen veranlassen, mit denen sie um die Übermittlung von Daten ersuchen, die sich im Hoheitsgebiet eines anderen Landes befinden („ausgehende Anfragen“).*

Im Hinblick auf die Gesamtzahl der unter Punkte 1.A.1.a genannten Anfragen:

1.A.2.a.3 *Wie viele (a) eingehende und (b) ausgehende Anfragen werden von Ihrem Land pro Jahr bearbeitet? Wenn möglich, unterscheiden Sie bitte zwischen justizieller und nicht-justizieller Zusammenarbeit. [quantitative Antworten]*

Antwort: Es liegen keine Erkenntnisse hierüber vor.

Artikel 10 der Richtlinie 2006/24/EG sieht eine derartige Erhebung nicht vor.

1.A.2.a.4 *Wie ist das Verhältnis zwischen nationalen und transnationalen Anfragen (Gesamtzahl der transnationalen Anfragen)? [quantitative Antwort]*

Antwort: Es liegen keine Erkenntnisse hierüber vor.

1.A.2.b *Wie lange dauert im Durchschnitt*

1.A.2.b.1 *die Beantwortung einer ausgehenden Anfrage, vom Zeitpunkt der Stellung der Anfrage bis zum Erhalt der Antwort (siehe auch 1.A.2.f)? Welche Kriterien (z. B. Art des Verfahrens) bestimmen die Dauer des Verfahrens? [quantitative Angaben]*

Antwort: Im internationalen Bereich werden ausländische Diensteanbieter nicht unmittelbar, sondern entweder im Rahmen eines Rechtshilfeersuchens oder über polizeiliche Partnerdienststellen angefragt. Ein durchschnittliches Zeit-Antwort-Verhalten kann nicht angegeben werden.

1.A.2.b.2 *die Beantwortung einer eingehenden Anfrage, vom Zeitpunkt des Erhalts der Anfrage bis zur Absendung der Antwort? Welche Kriterien (z. B. Art des Verfahrens) bestimmen die Dauer des Verfahrens? [quantitative Angaben]*

Antwort: Entsprechende Anfragen werden je nach Diensteanbieter innerhalb von zwei bis drei Wochen beantwortet. Bei eiligen Anfragen wird zusätzlich auf die Dringlichkeit hingewiesen, was überwiegend zu einer tagesaktuellen Beantwortung führt. Gegebenenfalls erforderliche Übersetzungen bedingen einen zusätzlichen Zeitbedarf von ca. zwei Werktagen.

1.A.2.b.3 *Welche Strategien könnten angewendet werden, um die Dauer der Beantwortung einer eingehenden Anfrage zu verringern?*

Antwort: Konsequente Einhaltung des unmittelbaren Geschäftsweges; Nutzung des I-24/7 Netzwerkes zur Datensicherung; eventuell analog diversen Rahmenbeschlüssen Entwicklung eines Formblattes oder Musters, dem zu entnehmen ist, welche Angaben erforderlich sind und ausreichen müssen.

1.A.2.c *Welche Behörde entscheidet in Ihrem Land über die Stellung einer transnationalen Anfrage? Sind alle Strafverfolgungsbehörden berechtigt, eine transnationale Anfrage zu stellen oder eine solche Anfrage zu veranlassen?*

Antwort: In Deutschland sind im Rahmen des Rechtshilfeverkehrs mit Mitgliedstaaten der EU die örtlichen Staatsanwaltschaften befugt, ausgehende Anfragen zu stellen und eingehende Ersuchen zu erledigen.

1.A.2.d *Gibt es in Ihrem Land eine zentrale Stelle, die ausgehende Anfragen stellt oder eingehende Anfragen entgegennimmt? Wenn ja, machen Sie bitte nähere Angaben zu diesen zentralen Stellen.*

Antwort: Nein.

Vorratsdaten, die bei ausländischen Diensteanbietern gespeichert sind, sind grundsätzlich nur über ein justizielles Rechtshilfeersuchen zu erlangen. Hierbei ist jedoch auch zwischen Bestands- und Verkehrsdaten zu unterscheiden. Während die Erlangung von Bestandsdaten bei einigen ausländischen Anbietern (z. B. Google) ohne richterlichen Beschluss möglich ist, sind bei Verkehrsdaten justizielle Rechtshilfeersuchen notwendig. Im Rahmen des Rechtshilfeverkehrs mit Mitgliedstaaten der EU sind die örtlichen Staatsanwaltschaften befugt, ausgehende Ersuchen zu stellen und eingehende Ersuchen zu erledigen (vgl. 1.A.2.c).

Um jedoch sicherzustellen, dass bei Eintreffen des Ersuchens in dem jeweiligen Land die Daten bei dem Anbieter noch vorhanden sind und nicht vorher gelöscht wurden, wird in solchen Fällen um Vorabsicherung dieser Daten (Preservation Order) über den jeweiligen nationalen G8-Kontaktpunkt ersucht.

1.A.2.e *Kosten*

1.A.2.e.1 *Wenn Ihr Land Betriebskosten erstattet (siehe 1.A.1.i), erstatten Sie innerstaatlichen Diensteanbietern in gleicher Weise die Kosten für die Beantwortung transnationaler Anfragen? Bitten Sie andere Mitgliedstaaten um Kostenteilung oder beabsichtigen Sie, dies zu tun?*

Antwort: Werden die Diensteanbieter im Rahmen der internationalen Rechtshilfe in Anspruch genommen, werden sie in gleicher Weise entschädigt wie bei einer innerstaatlichen Inanspruchnahme.

Im Rahmen der Rechtshilfe anfallende Auslagen für Entschädigungszahlungen sind grundsätzlich nach § 5 Absatz 2 der Justizverwaltungskostenordnung anzusetzen. Dies gilt jedoch dann nicht, wenn nach § 75 des Gesetzes über die internationale Rechtshilfe in Strafsachen oder nach § 71 des Gesetzes über die Zusammenarbeit mit dem Internationalen Strafgerichtshof darauf verzichtet worden ist oder soweit Rahmenbeschlüsse des Rates der Europäischen Union oder völkerrechtliche Übereinkommen einen gegenseitigen Verzicht auf Kostenerstattung vorsehen.

1.A.2.f *Sprache*

1.A.2.f.1 *Legt Ihr Land sprachliche Bedingungen für eingehende Anfragen fest (z. B. Übersetzung in eine Landes- oder Verkehrssprache)? Wenn ja, machen Sie bitte nähere Angaben zu diesen Bedingungen.*

Antwort: Die Spracherfordernisse ergeben sich aus dem jeweils dem Ersuchen zu Grunde liegenden Vertrag. Zu Art. 16 des Europäischen Übereinkommens über die Rechtshilfe in Strafsachen (EU-RhÜbk) hat Deutschland bei der Hinterlegung der Ratifikationsurkunde am 2. Oktober 1976 erklärt:

„Where the request for mutual assistance and the annexed documents are not in the German language they must be accompanied by translations of the request and the supporting documents into the German language or into one of the official languages of the Council of Europe.“

1.A.2.f.2 *Welche Mittel setzt Ihr Land ein, um sprachliche Bedingungen, die andere Staaten für ausgehende Anfragen festgelegt haben, zu erfüllen? Verfügen Sie über eine zentrale Einrichtung zur sprachlichen Unterstützung?*

Antwort: In Deutschland gibt es keinen zentralen Übersetzungsdienst. Die Staatsanwaltschaften bedienen sich freier, regelmäßig vereidigter Übersetzer.

1.A.2.g *Datensicherheit*

Welche Maßnahmen (Regelungen, Verfahren, Prüfbestimmungen) werden ergriffen, um Daten gegen Missbrauch zu schützen?

Antwort: Alle Verkehrsdaten, auch die auf Vorrat gespeicherten, unterliegen dem Fernmeldegeheimnis. Die Unternehmen sind nach § 109 Absatz 1 Telekommunikationsgesetz verpflichtet, angemessene technische Vorkehrungen oder sonstige Maßnahmen zum Schutz dieser Daten zu treffen. Für Telekommunikationsanlagen, die dem Erbringen von Telekommunikationsdiensten für die Öffentlichkeit

dienen, ist ein Sicherheitskonzept zu erstellen, aus dem hervorgeht, welche technischen Vorkehrungen oder sonstigen Schutzmaßnahmen zur Erfüllung der Verpflichtung getroffen oder geplant sind. Das Sicherheitskonzept ist der Bundesnetzagentur mit einer Erklärung vorzulegen, dass die aufgezeigten technischen Vorkehrungen und sonstigen Schutzmaßnahmen umgesetzt sind oder unverzüglich umgesetzt werden (§ 109 Absatz 3 Telekommunikationsgesetz). Die Einhaltung der vorgesehenen Schutzvorkehrungen wird von der Bundesnetzagentur nach § 115 Telekommunikationsgesetz kontrolliert und ggf. mit Mitteln des Verwaltungszwangs durchgesetzt.

Die Kontrolle der Maßnahmen stellt sich wie folgt dar: Grundsätzlich unterliegen alle Verpflichteten hinsichtlich der Umsetzung der genannten Maßnahmen der Aufsicht der Bundesnetzagentur. Da der Kreis der Verpflichteten abstrakt generell ist und der Bundesnetzagentur nicht in jedem Fall jeder Verpflichtete bereits konkret bekannt ist, ergeben sich in der Praxis drei Fallgruppen:

- Soweit es sich bei den Verpflichteten um die Betreiber von Telekommunikationsanlagen für die Öffentlichkeit handelt, sind diese der Bundesnetzagentur bereits im Einzelnen bekannt (vgl. § 109 Absatz 3 Telekommunikationsgesetz, zurzeit ca. 500 Unternehmen). Die von diesen Unternehmen bei Inbetriebnahme bzw. Aktualisierung vorzulegenden Sicherheitskonzepte werden – auch im Hinblick auf die Vorkehrungen für Daten nach § 113a Telekommunikationsgesetz - kontrolliert. Zusätzlich finden jährlich bei ca. 50 Unternehmen stichprobenartig Vor-Ort-Kontrollen statt.
- Soweit es sich bei den Verpflichteten nicht um solche Telekommunikations-Anlagenbetreiber handelt, sie aber nach § 6 Telekommunikationsgesetz Meldungen abgegeben haben (ca. 1500 Unternehmen, die auch § 109 Absatz 1 Telekommunikationsgesetz unterliegen), erfolgen Kontrollmaßnahmen zum Sicherheitskonzept grundsätzlich anlassbezogen (bislang einige wenige pro Jahr) sowie einige Stichproben.
- Während die Prüfindensität von nach § 6 Telekommunikationsgesetz gemeldeten Unternehmen bei Bedarf auch erhöht werden könnte, können die sonstigen, namentlich nicht bekannten Unternehmen in jedem Fall nur anlassbezogen bei Kenntniserlangung überprüft werden.

Für die nach § 113a Telekommunikationsgesetz auf Vorrat gespeicherten Verkehrsdaten gilt darüber hinaus, dass das jeweilige Telekommunikationsunternehmen sicherzustellen hat, dass der Zugang zu diesen Daten ausschließlich hierzu von ihm ermächtigten Personen möglich ist (§ 113a Absatz 11 Telekommunikationsgesetz). Zur Kontrolle dieser Vorschrift ist vorgesehen, eine lückenlose Protokollierung jedes einzelnen Zugriffs auf gespeicherten Daten vorzuschreiben (im Rahmen der Ergänzung der Telekommunikations-Überwachungsverordnung (TKÜV) hinsichtlich der für Verkehrsdatenauskünfte zu treffenden Vorkehrungen, siehe auch Antwort zu Frage 1.A.1.d).

1.A.3 Telekommunikationsbehörden

1.A.3.a Aufgabenverteilung

- 1.A.3.a.1 Welchen innerstaatlichen Behörden werden Aufgaben übertragen, die sich aus der Richtlinie ergeben (z. B. mit den entsprechenden Diensteanbietern bezüglich des anwendbaren Rechts in Verbindung treten; den Inhalt der z. B. als CDRs auf Vorrat zu speichernden Daten im Einzelnen festsetzen; für eine gewisse Vereinheitlichung sorgen, z. B. auf Grundlage von ETSI-Standards; Erstattungssysteme verwalten; die wirtschaftlichen Auswirkungen der Umsetzung*

und Anwendung der Richtlinie beurteilen)? Welche Aufgaben werden welcher Behörde übertragen?

Antwort: Als zentrale Aufgabe, die sich aus der Richtlinie ergibt, ist deren Umsetzung in nationale Vorschriften anzusehen, also die Vorgabe der entsprechenden technischen und organisatorischen Eckpunkte sowie die Festlegung der nationalen technischen Parameter. Die technischen und organisatorischen Eckpunkte werden in der Telekommunikations-Überwachungsverordnung vom Bundesministerium für Wirtschaft und Technologie (BMWi) unter Beachtung der dafür vorgesehenen Beteiligungen vorgegeben. Die nationalen technischen Standards legt die Bundesnetzagentur unter Beachtung der dafür geltenden gesetzlichen Vorschriften fest. Die Bundesnetzagentur hat jedoch keine Aufgaben im Zusammenhang mit der Durchführung konkreter Auskunftersuchen zu gespeicherten Verkehrsdaten.

Für Auskunftersuchen sind die jeweiligen Strafverfolgungsbehörden zuständig, für die Auskunftserteilungen die jeweils betroffenen Unternehmen. In Deutschland gibt es für diese Maßnahmen keine zwischengeschalteten Behörden.

Die Entschädigung der Telekommunikationsunternehmen bei der Erteilung von Auskünften über Verkehrsdaten im Einzelfall (insoweit wird auf 1.A.1.i.1 verwiesen) erfolgt durch die Stelle, die den Diensteanbieter herangezogen hat (§§ 1 und 2 JVEG). Im Rahmen der Strafverfolgung sind dies das Gericht, die Staatsanwaltschaft, die Finanzbehörde in den Fällen, in denen diese das Ermittlungsverfahren selbstständig durchführt, und die Polizei, wenn die Heranziehung im Auftrag oder mit vorheriger Billigung der Staatsanwaltschaft oder einer anderen Strafverfolgungsbehörde erfolgt. Im Übrigen richtet sich die Entschädigung nach dem Recht der heranziehenden Stelle, bei den Landespolizeibehörden nach dem jeweiligen Landesrecht, das zum großen Teil auf das JVEG verweist.

Es besteht die Möglichkeit, zentrale Kontaktstellen für eine oder mehrere Behörden einzurichten und über diese Kontaktstellen Leistungen der Diensteanbieter anzufordern und abzurechnen. Bisher wird diese Möglichkeit nur vereinzelt (z. B. in Bayern und in Nordrhein-Westfalen) genutzt (siehe auch 1A.1.f.2).

1.A.3.a.2 Wann nahmen/nehmen die jeweiligen Behörden ihre Tätigkeiten in Bezug auf diese Aufgaben auf?

Antwort: Auf Antwort zu Frage 1.A.3.a.1 wird verwiesen. Die Bundesnetzagentur hat ihre Aufgabe nach Verabschiedung der Richtlinie und noch vor Beginn der entsprechenden ETSI-Arbeitsgruppen ab etwa Juni 2006 aufgenommen und zwischenzeitlich den Entwurf für eine Ergänzung der „Technischen Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation und zum Auskunftersuchen für Verkehrsdaten“ erarbeitet, der der KOM mit Schreiben vom 28.07.2009 zur Notifizierung vorgelegt wurde. Die Notifizierung ist mittlerweile abgeschlossen.

1.A.3.a.3 Bitte geben Sie für jede einzelne Behörde an, ob zusätzliche Fachkenntnisse erworben werden müssen/mussten, um die Aufgaben nach der Richtlinie erfüllen zu können? Welche? Wie wurde bzw. wird dies umgesetzt (z. B. neues Personal, Reorganisation, spezielle Schulungen)?

Antwort: Auf Antwort zu Frage 1.A.3.a.1, insbesondere Buchstabe b, wird verwiesen. Für die Erfüllung der Aufgaben, die der Bundesnetzagentur aus der Richtlinie zufallen (indirekte Aufgaben), hat diese zusätzliche Fachkenntnisse über die Speicherpraxis bei den Unternehmen erwerben müssen. Sie konnte dabei jedoch auf

langjährige Erfahrungen auf dem Gebiet der Telekommunikations-Überwachung zurückgreifen, das artverwandt ist. Die Aufgaben wurden im Wesentlichen einer zusätzlichen Fachkraft übertragen.

1.A.3.a.4 *Sammelt eine der in diesem Abschnitt genannten Behörden Daten über die wirtschaftlichen Auswirkungen von Maßnahmen, die nach dieser Richtlinie erforderlich sind, z. B. darüber, wie es sich auswirkt, wenn gerichtlichen Anordnungen der Übermittlung von Vorratsdaten Folge geleistet wird, die von Zivilgerichten in Klageverfahren gegen illegales Downloaden und File-Sharing urheberrechtlich geschützter Materialien auf Antrag der klagenden Urheberrechtsinhaber erlassen wurden? Wenn diese Frage bejaht wird, machen Sie bitte nähere Angaben zu der betreffenden Behörde und zu den gesammelten Daten. [erfordert möglicherweise quantitative Angaben]*

Antwort: Nein.

1.A.3.a.5 *Betreibt eine der in diesem Abschnitt genannten Behörden grenzüberschreitende Zusammenarbeit im Zusammenhang mit der Richtlinie? Wenn ja, machen Sie bitte nähere Angaben zu 1. den betreffenden Behörden, 2. der Art der Maßnahmen oder Tätigkeiten, die diese Behörden in diesem Zusammenhang durchführen. [erfordert möglicherweise quantitative Angaben]*

Antwort: Die Bundesnetzagentur und Vertreter einiger Strafverfolgungsbehörden sind in der ETSI-Arbeitsgruppe (TC LI) tätig, die Fragen der technischen Standardisierung bearbeitet, die sich aus der Richtlinie ergeben.

1.A.3.a.6 *Sammeln die in diesem Abschnitt genannten Behörden Daten über die Auswirkungen der erforderlichen Maßnahmen auf den Wettbewerb, z. B. auf den Markteintritt neuer Betreiber oder auf die Vorteile für größere Unternehmen? Bitte machen Sie nähere Angaben zu der Art der gesammelten Daten! [letzter Abschnitt erfordert möglicherweise quantitative Angaben]*

Antwort: Nein.

1.A.3.a.7 *Zentrale Datenspeicherung durch Diensteanbieter*

Hat Ihr Land Schwierigkeiten mit der Erlangung von Vorratsdaten, die von Diensteanbietern außerhalb Ihres Landes gespeichert werden (z. B. Schwierigkeiten in Bezug auf die Dauer der Beantwortung oder die Qualität der Antwort)? Bitte machen Sie gegebenenfalls nähere Angaben zu diesen Schwierigkeiten und den zur Lösung ergriffenen Maßnahmen. [erfordert möglicherweise quantitative Angaben]

Antwort: Bislang sind keine Probleme oder Schwierigkeiten bekannt geworden.

1.B Bewertung der Wirksamkeit bestehender (nicht-)legislativer Maßnahmen oder technischer Lösungen zur Sicherstellung der Rückverfolgbarkeit von Nutzern von Kommunikationsdiensten, insbesondere Mobiltelefonanschlüssen, die mit vorausbezahlten SIM-Karten eingerichtet wurden (cf. Schlussfolgerungen des Rates in Anlage)

1.B.1 Fragen betreffend die Strafverfolgung

1.B.1.a Welche Mittel (technische, operative Mittel) oder Maßnahmen (administrative, gesetzliche Maßnahmen) setzt Ihr Land zur Verbesserung der Rückverfolgbarkeit von Nutzern von Telekommunikationsdiensten ein, um die Strafverfolgungsbehörden bei der Zuordnung von Endgeräten zu den entsprechenden Nutzern zu unterstützen? Berücksichtigen die genannten Maßnahmen neben den Daten, die derzeit bei Kommunikationsanbietern vorliegen, wie Kundendienstaufzeichnungen, Zahlungsverhalten, Versicherungsverträge, IMEI-History, auch Supermarkt-Kundenbindungskarten hinsichtlich des Verlaufs der Auflade-Aktivität, der Nutzung von elektronischen Aufladefunktionen („e-top-up“) in Zusammenhang mit Guthaben- oder Kreditkarten, Informationen, die bei Kreditauskunfteien vorliegen, sowie als Kontakte angegebene Mobilgeräten und die forensische Untersuchung von Mobilgeräten? Bitte beschreiben Sie diese Maßnahmen.

Antwort: Die Erhebung von Kundendaten durch die Dienstanbieter ist seit dem 26. Juni 2004 durch § 111 Absatz 1 Satz 1 des Telekommunikationsgesetzes – auch für Prepaid-Kunden – vorgeschrieben.

1.B.1.b Inwieweit tragen diese Mittel oder Maßnahmen zur Verbesserung der Rückverfolgbarkeit von Nutzern bei? Bitte machen Sie nähere Angaben zur juristischen Rechtfertigung bzw. verwaltungsmäßigen Begründung dieser Instrumente sowie über ihren Anwendungsbereich, d.h. ob sie auf die Unterstützung der Verhütung, Feststellung, Ermittlung oder Verfolgung von Straftaten gerichtet sind. Auf welche Straftaten beziehen sich die von Ihrem Land eingesetzten Mittel und Maßnahmen typischerweise?

Antwort: Siehe Antwort zu Frage 1.b.1.a.

1.B.1.c Effizienz

1.B.1.c.1 Wird mit den Maßnahmen die Zielsetzung, mit der sie von Ihrem Land ergriffen wurden, effizient verwirklicht? Bitte machen Sie nähere Angaben über die durch den Einsatz der entsprechenden Mittel oder Maßnahmen erzielten Ergebnisse. [erfordert möglicherweise quantitative Angaben]

Antwort: Hierzu liegen keine über die Ausführungen zu Frage 1.A.1.j hinausgehenden Erkenntnisse vor.

1.B.1.c.2 Hat Ihr Land eine Beurteilung der Wirksamkeit der Maßnahmen vorgenommen? Wenn ja, machen Sie bitte nähere Angaben zu dieser Beurteilung.

Antwort: Nein.

1.B.1.c.3 Welche Effizienzgewinne sind - über die Ergebnisse hinaus, die mit den nach Artikel 5 Absatz 1 Buchstabe e Nummer 2 der Richtlinie, insbesondere Ziffer vi, erlangten Daten erzielt wurden - durch die von Ihrem Mitgliedstaat ergriffenen Maßnahmen erreicht worden, was die Verbesserung Ihrer Fähigkeiten zur Feststellung, Ermittlung oder Verfolgung von Terrorismus und anderer schwerer Formen der Kriminalität betrifft? [erfordert möglicherweise quantitative Angaben]

Antwort: Hierzu liegt kein belastbares Zahlenmaterial vor.

1.B.1.c.4 Welche Kosten entstehen dem privaten Sektor durch diese Maßnahmen? [erfordert möglicherweise quantitative Angaben]

Antwort: Hierzu liegen keine Erkenntnisse vor.

1.B.1.d Sollten Maßnahmen auf europäischer Ebene ergriffen werden, um die Rückverfolgbarkeit von Nutzern von Kommunikationsgeräten zu verbessern? Wenn ja, welche Maßnahmen sollten auf europäischer Ebene ergriffen werden? Wie würden diese Maßnahmen die Effizienz der Mittel und Maßnahmen, die Sie auf innerstaatlicher Ebene einsetzen, verbessern?

Antwort: Solche Maßnahmen erscheinen derzeit nicht veranlasst.

1.B.1.e Welche Schulungs- oder Qualifizierungsprogramme bietet Ihr Mitgliedstaat den Strafverfolgungsbehörden an, um ihre Fähigkeiten zu schulen, Endgeräte (z. B. Mobiltelefone) Daten zuzuordnen (mit Daten in Verbindung zu bringen), die bei Kommunikationsanbietern vorliegen, um so Endnutzer identifizieren zu können?

Antwort: In Deutschland gibt es auf Ebene des Bundes und auf der Ebene der Länder eine Vielzahl von Maßnahmen, die der Schulung und Qualifizierung der bei den Strafverfolgungsbehörden tätigen Personen dienen (z. B. Lehrgänge, Fortbildungen, Seminare). Dazu, inwieweit hierbei die in der Frage angesprochenen Fähigkeiten speziell geschult werden, liegen keine detaillierten Erkenntnisse vor.

1.B.2 Telekommunikationsbehörden

1.B.2.a Welche Auswirkungen haben die in Abschnitt 1.B.1 genannten Mittel oder Maßnahmen auf den Markt?

Antwort: Die Kosten für die Unternehmen steigen leicht. Es ist daher möglich, dass die Endverbraucherpreise ein etwas höheres Niveau aufweisen, als es ohne die Speicherverpflichtung denkbar wäre. Ein Preisanstieg war im Zuge der Einführung der Vorratsdatenspeicherung allerdings nicht zu verzeichnen.

1.B.2.b Überwacht die unter Punkt 1.A.3.a. genannte Behörde die innerstaatlichen Maßnahmen und setzt sie bei den Anbietern oder sonstigen Akteuren durch?

Antwort: Ja, die Bundesnetzagentur ist für Durchsetzung der Vorschriften des Telekommunikationsgesetzes zuständig.

1.B.2.b.1 *Hat die in der vorangegangenen Frage genannte Behörde bereits Fälle untersucht, in denen die innerstaatlichen Instrumente oder Maßnahmen nicht beachtet wurden? Bitte machen Sie gegebenenfalls nähere Angaben. [erfordert möglicherweise quantitative Angaben]*

Antwort: Bisher wurden entsprechende Fälle nicht untersucht.

1.B.2.b.2 *Falls das innerstaatliche Recht Maßnahmen vorsieht, um die Identifizierung von Nutzern vorausbezahlter SIM-Karten zu gewährleisten: Wie werden Karten behandelt, die bereits vor Inkrafttreten der betreffenden Rechtsvorschriften erworben wurden? Werden diese Karten nach einer bestimmten Nutzungsdauer gesperrt?*

Antwort: Seit Inkrafttreten des Telekommunikationsgesetzes vom 22. Juni 2004 (BGBl. I S. 1190), mithin seit dem 26. Juni 2004, ist rechtverbindlich geregelt, dass auch Kundendaten von Erwerbern von Prepaid-Karten zu erheben und zu speichern sind (§ 111 Absatz 1 Satz 1 und 2 Telekommunikationsgesetz). Kundendaten zu „alten“ Prepaid-Verträgen müssen nicht nachträglich erhoben werden, dies ergibt sich aus § 111 Absatz 1 Satz 4 Telekommunikationsgesetz. Prepaid-Karten, zu denen keine Kundendaten vorliegen, werden aus diesem Grunde nicht gesperrt.