XXIII.GP.-NR
626 /AB
30. Mai 2007
zu 591 /J

REPUBLIK ÖSTERREICH
WERNER FAYMANN
BUNDESMINISTER
Bundesministerium
für Verkehr, Innovation und Technologie

GZ. BMVIT-12.000/0005-I/PR3/2007 DVR:0000175

An die
Präsidentin des Nationalrates
Mag. Barbara Prammer
Parlament
1017 Wien

Wien, am 30. Mai 2007

Sehr geehrte Frau Präsidentin!

Die schriftliche parlamentarische Anfrage Nr. 591/J-NR/2007 betreffend Umsetzung der Richtlinie zur verdachtsunabhängigen Vorratsdatenspeicherung, die die Abgeordneten Alexander Zach und GenossInnen am 29. März 2007 an mich gerichtet haben, beehre ich mich wie folgt zu beantworten:

Frage 1:
Für wann planen Sie die Umsetzung der Richtlinie - auch im Hinblick auf das laufende Verfahren vor dem EuGH?
a) für Daten, die bei der Nutzung von Handys oder Festnetztelefonen anfallen?
b) für Daten, die bei der Nutzung von Internet-E-Mail und Internet-Telefonie anfallen?
c) Wie schätzen Sie die Erfolgsaussichten der EuGH-Klagen von Irland und der Slowakei gegen die Richtlinie ein?

Antwort:
Die Richtlinie 2006/24 EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsdatenspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58 EG (Abl L105 vom 13.4.2006 S 54) trat mit dem Tag der Veröffentlichung im Amtsblatt in Kraft. Gemäß Art 15 Abs. 1 sind die Mitgliedstaaten verpflichtet die erforderlichen Rechts- und Verwaltungsvorschriften bis spätestens 15. September 2007 in Kraft zu setzen.

Die Richtlinie wurde auf EU- Ebene im Rat der Justiz und Innenminister verhandelt. Zur Koordinierung der dort vertretenen Haltung hat das Bundesministerium für Justiz laufend Konsultationssitzungen abgehalten, in die das BKA-VD (Abt. V 3), das BMVIT und das BMI eingebunden waren. In grundsätzlichen Fragen wurde daher im Rat der Justiz und Innenminister stets eine abgestimmte Position vertreten. Dabei wurde auch einvernehmlich klargestellt, dass die nationale Umsetzung der Richtlinie im TKG 2003 und daher unter Federführung meines Ressorts zu erfolgen hat. In der Vorbereitungsphase wurde natürlich

über grundsätzliche Fragen des Entwurfs Einvernehmen mit dem Bundesministerium für Justiz hergestellt, weil der enge Zusammenhang mit der Regelung der Überwachung einer Telekommunikation in der StPO zu beachten ist.

Die Vorarbeiten für die Umsetzung in Österreich haben bereits begonnen, das Begutachtungsverfahren hat stattgefunden. Über 90 Stellungnahmen liegen vor, diese werden von meinem Ressort in Zusammenarbeit mit dem BMJ hinsichtlich der vertretenen Meinungen geprüft. Nach eingehender Prüfung und wenn notwendig, weiterer Konsultation werde ich die weiteren Schritte entsprechend veranlassen.

Art. 15 Abs. 3 der Richtlinie gibt den Mitgliedstaaten die Möglichkeit eines Aufschubs bezüglich der Anwendung der Richtlinie auf die Speicherung von Kommunikationsdaten betreffend Internetzugang, Internet - Telefonie und Internet- E-Mail bis zum 15. März 2009. Österreich hat eine diesbezügliche Erklärung abgegeben - weshalb eine weitere Novelle, welche die meisten Daten betreffend Internetzugang, Internet E-Mail und Internet-Telefonie betrifft, für ein in Kraft treten 18 Monate später am 15. März 2009 vorbereitet wird.

Die von Irland gegen den Rat der Europäische Union zu C 301/06 beim Europäischen Gerichtshof anhängige Klage zielt auf die Nichtigerklärung der Richtlinie ab, wobei freilich nicht den Inhalt der Richtlinie betreffende Argumente vorgebracht werden, sondern bloß die Auffassung vertreten wird, dass die richtige Rechtsform ein Rahmenbeschluss im Rahmen der 3. Säule der Europäischen Union gewesen wäre.

Mangels aufschiebender Wirkung einer solchen Klage, haben die Mitgliedstaaten und somit auch Österreich - ungeachtet des beim EuGH anhängigen Verfahrens - den Verpflichtungen aus dieser Richtlinie nachzukommen.

Die Erfolgsaussichten der EuGH Klagen von Irland und der Slowakei kann ich nicht beurteilen, dies obliegt seriöserweise ausschließlich dem EuGH selbst.

Frage 2:
Wie lange sollen diese verdachtsunabhängig gespeicherten Daten über das Kommunikationsverhalten der Bürgerinnen und Bürger aufbewahrt werden? Für welche Speicherfrist (gemäß Artikel 6 der Richtlinie) treten Sie ein?

Antwort:
Ich trete für die – nach den Vorgaben der Richtlinie - kürzestmögliche Speicherdauer von 6 Monaten ein.

Frage 3:
Ist für die Umsetzung der Richtlinie ein Eingriff in die verfassungsmäßig garantierten Grundrechte der Bürgerinnen und Bürger erforderlich?
a) Falls ja, welche Bestimmungen im Verfassungsrang müssen aufgehoben bzw. geändert werden?

Antwort:
Beschränkungen des Grundrechtes auf Geheimhaltung von Daten (§ 1 DSG) sind zur Wahrung berechtigter Interessen oder auf Grund von Gesetzen zulässig, die aus den in Artikel 8 Abs. 2 EMRK genannten Gründen notwendig sind. Ich gehe davon aus, dass sich die Umsetzungsgesetzgebung der Richtlinie in jenem Bereich bewegt, der gemäß Artikel 8

Abs. 2 EMRK Eingriffe in die Grundrechte auf private Lebensgestaltung und auf Schutz personenbezogener Daten zulässt. Dazu bedarf es natürlich einer besonderen Regelung der anzuwendenden Datensicherheits- und Datenschutzmaßnahmen wie auch einer verhältnismäßigen Regelung der Zugriffsbedingungen, die ja ausschließlich auf Zwecke der Strafverfolgung abstellen. Dadurch wird auch sichergestellt, dass gemäß Artikel 10a StGG Daten bloß auf Grund einer gerichtlichen Anordnung herausgegeben werden dürfen.

Frage 4:
Wie viele Bürgerinnen und Bürger sind in Österreich nach der Umsetzung der Richtlinie von der verdachtsunabhängigen Speicherung ihres Telekommunikationsverhaltens betroffen?

Antwort:
Da die Richtlinie keine Ausnahmen vorsieht, sind alle jene, die die in Frage kommenden Kommunikationsmittel benützen, von den Regelungen betroffen. Ich möchte aber darauf hinweisen, dass Betreiber öffentlicher Telekommunikationsdaten – jedenfalls soweit der Bereich der klassischen Sprachtelefonie betroffen ist - schon gegenwärtig Daten zu Verrechnungszwecken speichern dürfen (auf die auch im Wege einer Anordnung gemäß den §§ 149a StPO zugegriffen werden darf).

Fragen 5, 6 und 7:
Zur Bekämpfung welcher Straftaten bzw. Bedrohungen ist es Ihrer Einschätzung nach gerechtfertigt, einen derartigen Eingriff in die Grundrechte vorzunehmen?

Sollen auf die gespeicherten Kommunikationsdaten auch bei anderen, leichteren Straftaten zugegriffen werden dürfen?

Erhalten Rechteinhaber, Verwertungsgesellschaften oder in deren Auftrag tätige Organisationen, Firmen oder Personen im Zuge von behaupteten Urheberrechtsverletzungen Zugriff oder Auskünfte über Daten, die im Rahmen der Vorratsdatenspeicherung erfasst wurden?
a) Falls ja, unter welchen Auflagen und Bedingungen (z.B. gerichtliche Genehmigung, gewerbliche Urheberrechtsverletzung)?

Antwort:
Art. 1 Abs. 1 der Richtlinie fordert, dass die zu speichernden Daten jedenfalls für Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten, wie sie von jedem Mitgliedstaat in seinem nationalen Recht bestimmt werden, zur Verfügung stehen. Anlässlich seiner Annahme der Änderungsvorschläge des Europäischen Parlaments zur gegenständlichen Richtlinie am 21. Februar 2006 forderte der Rat in einer Ratserklärung, dass die Mitgliedstaaten bei ihrer Definition von „schwerer Straftat" die in Art. 2 Abs. 2 des Rahmenbeschlusses über den Europäischen Haftbefehl genannten Straftaten sowie Straftaten unter Einsatz von Telekommunikationseinrichtungen angemessen zu berücksichtigen haben.

Der Zugang zu diesen Daten darf ausschließlich unter den Voraussetzungen und Bedingungen für eine Überwachung einer Telekommunikation gemäß den Bestimmungen der StPO erfolgen. Details wie auch die dem Zugriff zugrunde liegende Strafbedrohung sind

derzeit auf Basis der beim Begutachtungsverfahren eingelangten Stellungnahmen Gegenstand von Verhandlungen.

Frage 8:
Werden auch private oder nicht-professionelle/nicht-kommerzielle Anbieter von öffentlichen Internetzugängen (z. B. Privatperson mit offenem WLAN, Kaffeehaus mit offenem WLAN, kostenloser, öffentlicher Hotspot eines Vereins etc.) zur Speicherung der Standort- und Verkehrsdaten verpflichtet?

Antwort:
Der vorgeschlagene Entwurf geht davon aus, dass Anbieter und Betreiber öffentlicher Kommunikationsnetze zur Datenspeicherung verpflichtet werden. Die Definition des Begriffes eines Betreibers gemäß § 3 Z 1 TKG umfasst ein Unternehmen, das ein öffentliches Kommunikationsnetz oder eine zugehörige Einrichtung bereitstellt, oder zur Bereitstellung hiervon befugt ist. Der Begriff des Anbieters nach § 92 Abs. 3 Z 1 TKG umfasst einen Betreiber von öffentlichen Kommunikationsdiensten. Darunter sind gewerbliche Dienstleistungen zu verstehen, die ganz oder überwiegend in der Übertragung von Signalen über Kommunikationsnetze bestehen, ausgenommen davon sind jene Dienste, die eine inhaltliche Kontrolle bei der Übermittlung ausüben.

Dies wird bei den genannten Beispielen nicht der Fall sein.

Frage 9:
Gilt die Speicherpflicht auch für im Ausland betriebene Server österreichischer Provider bzw. in Österreich betriebene Server ausländischer Anbieter?
a) Im folgenden Fall: Der Mailserver eines österreichischen Internet-Providers, den seine Kunden via SMTP und POP3-Protokoll nutzen, befindet sich in einem Rechenzentrum in der Schweiz.
b) Im folgenden Fall: Ein US-amerikanisches Unternehmen (ohne eigenem Sitz in Österreich) betreibt in einem österreichischen Rechenzentrum einen Mailserver.

Antwort:
Diese Frage betrifft E-Mail-Daten. Ich darf deshalb auf die von Österreich angestrebte Umsetzung bis 15. März 2009 und die diesbezüglich noch zu führende interministerielle Konsultation verweisen.

Fragen 10 bis 13:
Wird im Zuge der Vorratsdatenspeicherung erfasst, wann, wie oft und von welchem Ort aus eine Bürgerin/ein Bürger
a) Dienste wie die Telefonseelsorge (142) oder Rat auf Draht (147) nutzt?
b) mit berufsmäßigen Parteienvertretern (Rechtsanwälte, Steuerberater) telefonisch oder per E-Mail kommuniziert?
c) mit welchem Arzt telefonisch oder per E-Mail kommuniziert?

Wird im Zuge der Vorratsdatenspeicherung erfasst, wann, wie oft und von welchem Ort aus ein Informant mit einem Vertreter der Presse telefonisch oder per E-Mail kommuniziert?

Sind von der Vorratsdatenspeicherung Telefonate und der E-Mail-Verkehr von Bundespräsident, den Mitgliedern der österreichischen Bundesregierung und den Mitgliedern von Nationalrat und Bundesrat betroffen?

Sind von der Vorratsdatenspeicherung Telefonate und der E-Mail-Verkehr von Sicherheits- und Militärbehörden betroffen?

Sind Ausnahmen von der allgemeinen Speicherpflicht für besondere Behörden, Institutionen, Firmen, Personen, Angehörige bestimmter Berufsgruppen oder sonstige Ausnahmen geplant?
a) Falls die zur Vorratsdatenspeicherung verpflichteten Betriebe ausnahmslos von allen Kunden Kommunikationsdaten speichern müssen, sind Verwertungsverbote von über bestimmte Behörden, Institutionen, Personen, Angehörige bestimmter Berufsgruppen gespeicherte Daten vorgesehen?

Antwort:
Es werden alle von der Richtlinie verlangten Daten gespeichert. Ausnahmen für bestimmte Benutzer bestehen nach der Richtlinie nicht. Es ist jedoch darauf hinzuweisen, dass dem Betreiber eine Selektion der Daten nach bestimmten Kriterien bereits nach datenschutzrechtlichen Bestimmungen untersagt ist.

Der Schutz von Amts- oder Berufsgeheimnissen unterliegt jedoch den Zugriffsbedingungen gemäß der StPO, deren § 149a Abs. 3 Anschlüsse von Medienunternehmen und Parteienvertretern und Angehörigen von Berufen der psychosozialen Betreuung einem besonderen Schutz unterstellt. Die Daten von Anschlüssen von Geistlichen, Parteienvertretern oder Angehörigen von Berufen der psychosozialen Betreuung und Medienunternehmen dürfen bei sonstiger Nichtigkeit nicht verwertet werden, wenn dadurch ein Entschlagungsrecht (§§ 151 Abs. 2, 152 Abs. 3 und § 31 Abs. 2 Mediengesetz) umgangen würde.

Frage 15:
Sollen Betroffene das Recht erhalten, die über Sie erhobenen Daten einzusehen? Sollen sie ein Recht auf Löschung oder Korrektur fehlerhafter oder nicht durch Sie verursachte Daten haben, wie diese z.B. bei offenen (privaten) WLANs, Trojanern, Adware etc. anfallen können?

Antwort:
Für die Daten gelten die allgemeinen Bestimmungen des Datenschutzrechtes, die solche Rechte vorsehen. Neben der Informationspflicht gemäß § 96 Abs. 3 TKG finden nämlich die §§ 26 und 27 DSG in Bezug auf das Auskunftsrecht und das Recht auf Richtigstellung und Löschung Anwendung. Zum einen hat der Anbieter spätestens bei Beginn des Rechtsverhältnisses den Teilnehmer oder Benutzer darüber zu informieren, welche Daten auf welcher Rechtsgrundlage gespeichert werden. Zum anderen hat der Betroffene im konkreten Fall das Recht auf Auskunft über die zu seiner Person verarbeiteten Daten. Das Recht auf Auskunft unterliegt gemäß § 26 Abs. 2 DSG einer Beschränkung sofern ein überwiegendes öffentliches Interesse (Vorbeugung, Verhinderung oder Verfolgung von Straftaten) betroffen ist. Über die Zulässigkeit der Auskunftsverweigerung hat die Datenschutzkommission gemäß § 30 Abs. 3 DSG die Kontrolle. Das Recht auf

Richtigstellung und Löschung ergibt sich aus § 27 DSG. In den Fällen, in denen eine Auskunftsverweigerung gerechtfertigt wäre (§ 26 Abs. 2 Z 1 bis 5) ist dem Betroffenen eine Mitteilung zu machen, dass die Datenbestände einer Überprüfung unterzogen wurden. Bei einem berechtigten Begehren des Betroffenen ist eine Richtigstellung oder Löschung jedenfalls vorzunehmen. Die Vorgangsweise unterliegt wiederum der Kontrolle der Datenschutzkommission (§ 30 Abs. 3 DSG).

Frage 16:
Derzeit ist es Telekommunikationsanbietern untersagt, Daten zu erheben, die nicht für die Abrechnung erforderlich sind. Die für die Abrechnung gespeicherten Daten dürfen nicht für andere Zwecke verwendet werden und müssen danach gelöscht werden. Dürfen die nach Umsetzung der Richtlinie zur umfangreichen Datenspeicherung verpflichteten Telekommunikationsunternehmen diese Daten

a) zu eigenen Zwecken (Kundenprofile, Marketing) verwenden?
b) anderen Unternehmen oder Personen zugänglich machen? Falls ja, unter welchen Bedingungen?
c) in zivilrechtlichen Streitigkeiten zwischen Telko-Anbieter und Kunde verwendet werden? Falls ja, unter welchen Bedingungen?
d) in zivilrechtlichen Angelegenheiten zwischen Kunden und Dritten verwendet werden? Falls ja, unter welchen Bedingungen?
e) Wie sollen allfällige Nutzungsverbote kontrolliert und durchgesetzt werden?

Antwort:
a) Wie schon bisher dürfen Anbieter Stammdaten, Verkehrsdaten, Standortdaten und Inhaltsdaten für Marketingzwecke nur verwenden, wenn der Teilnehmer oder Nutzer dazu seine jederzeit widerrufbare Einwilligung erteilt hat (§ 96 Abs. 2 und § 99 Abs. 4 TKG).

b) Das Überlassen und Übermitteln von Daten an Dritte ist nur soweit zulässig, als es für die Erbringung eines Telekommunikationsdienstes, für den diese Daten ermittelt und verarbeitet wurden, erforderlich ist (§ 96 Abs. 2 TKG). Daher dürfen Daten, die im Sinne der Vorratsdatenspeicherung zu speichern sind, nicht an Dritte weitergegeben werden.

c) Die Regelungen zur Verwendung von Daten für Streitigkeiten zwischen dem Betreiber und Kunden über Entgelte nach den §§ 97 und 99 TGK werden beibehalten, sodass Stammdaten und Verkehrsdaten so lange zu speichern sind, als dies für die Zwecke der Verrechnung von Entgelten erforderlich ist, und zwar bis zum Ablauf jener Frist, innerhalb derer die Rechnung rechtlich angefochten werden kann, da diese Daten im Streitfall der Schlichtungsstelle nach § 71 Abs. 2 TKG zur Verfügung zu stellen sind.

d) Die Übermittlung von Daten an Dritte wurde ebenso wie das Auskunftsrecht von Nutzern bereits dargestellt. Es braucht daher nicht näher auf die Frage der Datenverwendung in zivilrechtlichten Streitigkeiten zwischen einem Kunden eines Anbieters und einem Dritten eingegangen werden.

e) Die unbefugte Nutzung von Daten wird durch § 108 TKG erfasst. Danach wäre eine unbefugte Weitergabe oder unbefugte Gewährung von Einsicht durch einen Betreiber oder durch eine Person, die an der Tätigkeit des Betreibers mitwirkt, von Tatsachen oder Inhalten

des Telekommunikationsverkehrs mit einer Freiheitsstrafe von bis zu drei Monaten oder mit einer Geldstrafe bis zu 180 Tagesätzen zu bestrafen.

Frage 17:
Können Sie ausschließen, dass die erhobenen Überwachungsdaten - wie bei der illegalen Weitergabe von über 100 Millionen europäischen Bank-Überweisungsdaten an den US-Geheimdienst CIA passiert (Fall SWIFT) - ausländischen Geheimdiensten oder Behörden ohne jegliche Kontrollierbarkeit zugänglich gemacht werden? Welche Maßnahmen sind geplant, um derartigen Missbrauch zu verhindern?

Antwort:
Zu dieser Frage darf ich neuerlich auf die Strafbestimmung des § 108 TKG verweisen, die die unbefugte Weitergabe oder unbefugte Gewährung von Einsicht von Tatsachen oder Inhalten einer Telekommunikation unter Strafe stellt.

Zur Datensicherheit werden die Betreiber darüber hinaus verpflichtet auch geeignete technische und organisatorische Vorkehrungen zu treffen, damit Daten unter anderem auch vor der unberechtigten oder unrechtsmäßigen Speicherung, Verarbeitung, Zugängigmachung und Verbreitung geschützt werden.

Frage 18:
Halten Sie die Vorratsdatenspeicherung für geeignet um Terrorismus oder organisiertes Verbrechen zu verhindern?

Antwort:
Durch die auf EU-Ebene stattgefundene Diskussion in Folge folgenschwerer terroristischer Übergriffe sehe ich die damit zusammenhängende Debatte und damit verbundene Maßnahmen als nicht vollkommen unberechtigt; bei Fragen der Kriminalitätsbekämpfung bleibt der Hintergrund der eingeschränkten nationalen Ausprägung des Problems und damit verbundener Fragen der Machbarkeit und des Datenschutzes immer bestehen. Die Umsetzung der EU-Richtlinie ist darüber hinaus unabhängig von meiner persönlichen Meinung vorzubereiten.

Fragen 19 bis 21:
Werden Vertreter der ISPA (Internet Service Providers Austria) im Zuge der Umsetzung konsultiert?

Werden Vertreter der ArgeDaten und/oder von VIBE (Verein der Internet-Benutzer Österreichs) im Zuge der Umsetzung konsultiert?

Werden Vertreter der betroffenen Telekommunikationsunternehmen (WKÖ Fachverband Telekommunikation) bzw. diese selbst im Zuge der Umsetzung konsultiert?

Antwort:
Die bereits in den Vorbereitungen des Entwurfs eingebundenen Stellen werden auch im Begutachtungsverfahren direkt angesprochen. Der Begutachtungsentwurf ist jedoch überdies auf der Homepage des Bundesministeriums für Verkehr, Innovation und Technologie veröffentlicht. Jedermann ist eingeladen, dazu eine Stellungnahme abzugeben.

Wie bereits ausgeführt wird seitens des BMVIT angestrebt bezüglich der Internetdaten die Umsetzungsfrist bis 15. März 2009 ausnutzen, sodass sich die derzeitigen Arbeiten auf die Umsetzung hinsichtlich der Telefondaten konzentrieren.

Frage 22:
Sollen neben Fest- und Mobilfunktelefonaten, SMS, EMS und MMS, Internet-E-Mail und Internet-Telefonie von weiteren elektronischen Kommunikationsmöglichkeiten die entsprechenden Standort- und Verkehrsdaten gespeichert werden (z.B. Nutzung von Chatrooms)?

Antwort:
Die Richtlinie und demzufolge der Gesetzesentwurf sehen derartiges nicht vor.

Frage 23:
In welcher Form ist eine Regelung geplant, um durch die Richtlinie keine Überschneidungen mit den geltenden Bestimmungen zur Überwachung der Telekommunikation (§ 94 TKG i.V.m. § 149 ff StPO) zu schaffen (unterschiedliche Verhältnismäßigkeitsgrundsätze und Anspruchsgrundlagen bei Zugriff auf vorzuhaltende Daten)

Antwort:
Die Umsetzung der Richtlinie wird so in das Telekommunikationsgesetz 2003 integriert werden, dass für alle Tatbestände die gleichen Grundsätze zur Anwendung kommen.

Frage 24:
Inwieweit ist eine nationale Definition der (in technischer Hinsicht zu ungenau definierten) zu speichernden Datenarten geplant (teilweise technisch nicht möglich, teilweise mit enormen Kosten (ohne Nutzen für die Verbrechensbekämpfung) verbunden?

Antwort:
Die Datenarten werden orientiert an der Richtlinie taxativ aufgezählt werden.

Frage 25:
Erfolgt in Bezug auf Frage 24. eine Kosten-/Nutzen-Analyse?

Antwort:
Soweit entsprechende Ungleichgewichte bestehen, werden diese jetzt auf Basis der vorliegenden Stellungnahmen evaluiert werden.

Frage 26:
Beispiel Art 2 Abs. 2 lit. c) der RL: Telefondienst "Datenabrufungen" - da keine Inhalte gespeichert werden können und dürfen, ist nur die Datenmenge (meist auch keine Dauer bedingt durch eine always-on Funktion bei GPRS und UMTS/HSDPA) ohne sonstige verwertbare Information zu speichern?

Antwort:
Der vorliegende Entwurf sieht - da er sich nicht auf Internet-Daten bezieht - dies nicht vor.

Frage 27:
Sind aus Ihrer Sicht Daten erfolgloser Anrufversuche ebenfalls zu speichern (Art 3 Abs. 2 der RL sieht (auf Grund technischer Gegebenheiten) keine Speicherpflicht vor)?

Antwort:
Dieser Punkt wird im Zuge des Begutachtungsverfahren nochmals evaluiert.

Frage 28:
Wen betrifft die nicht genau definierte Speicherpflicht abgerufener und gesicherter Daten und für welchen Zeitraum sind diese zu speichern (vgl. Art. 7 d) der RL)?

Antwort:
Die Pflicht zur Löschung umfasst alle Daten, die beim Anbieter oder Betreiber vorliegen. Die abgerufenen und gesicherten Daten sind jene, die auf der Grundlage eines richterlichen Befehls übermittelt wurden und beim Empfänger aufliegen.

Frage 29:
Wer soll die Kosten für Vorratsdatenspeicherung übernehmen?

Antwort:
Die Kosten der Mitwirkung werden durch die Überwachungskostenverordnung, BGBl II Nr. 322/2004 geregelt. Die Kosten der Investitionen werden vor dem Hintergrund eingelangter Stellungnahmen noch gesonderter Betrachtung bedürfen, § 94 TKG bezieht sich derzeit nur auf solche Investitionen, die Betreibern auf Grund der Überwachungsverordnung, BGBl II NR 418/2001, vorgeschrieben sind. Die Speicherung von Vorratsdaten ist davon nicht umfasst.

Frage 30:
Gibt es bereits einen Entwurf für die Umsetzung der Richtlinie in nationales Gesetz?
a) Falls ja, wie lautet dieser?
b) Falls nein, für wann ist die Fertigstellung eines Entwurfes geplant?

Antwort:
Der Begutachtungsentwurf liegt dem Nationalrat vor.

Frage 31:
Ist Ihnen bekannt, dass sogenannte Wertkartenhandys auch anonym genutzt werden können und bei häufigem Wechseln von Handy und SIM-Karte (immer andere IMSI und IMEI) die Vorratsdatenspeicherung ins Leere läuft?

Antwort:
Bei sogenannten Wertkartenhandys, die anonym benutzt werden können, sind die zu speichernden Daten insbesondere in Kombination mit den Erkenntnissen einer konkreten Ermittlung von Bedeutung (Rückverfolgung im Wege der IMEI oder IMSI- Nummer in

Zusammenhang mit einer Observation). Daher können schon derzeit viele Benützer anonymer Wertkartenhandys letztlich ausgeforscht werden.

Fragen 32 und 33:
Ist Ihnen bekannt, dass bei Internet-Telefonie die Richtlinie einfach und von jedermann umgangen werden kann, indem der Konsument z.B. einen Diensteanbieter mit Sitz außerhalb der EU wählt?

Ist Ihnen bekannt, dass die Erfassung von Standort- und Verkehrsdaten im Zuge des E-Mail-Versands auf einfachstem Wege umgangen werden kann, indem man einen Anbieter aus einem Land wählt, dass seinen Bürgerinnen und Bürger noch unbeobachtete Kommunikation gestattet?

Antwort:
Ja.

Fragen 34 und 35:
Soll die Nutzung von Anonymisierungsdiensten (z.B. Java Anon Proxys (JAP) oder TOR-Netzwerk) verboten werden oder die Provider verpflichtet werden, deren Nutzung durch technische Maßnahmen zu verhindern?

Soll die anonyme Nutzung von Telefonzellen oder Internet-Cafes verboten werden?

Antwort:
Der Begutachtungsentwurf sieht derartige Maßnahmen nicht vor.

Fragen 36, 37 und 38:
Glauben Sie, dass Terroristen oder Mitglieder krimineller Vereinigungen unter Rücksicht auf die Vorratsdatenspeicherung ihre Handys (mit korrekten Daten) anmelden oder stets E-Mail-Dienstleister wählen, die der Datenspeicherpflicht unterliegen?

Halten Sie die Richtlinie für geeignet, die in Artikel 1 Absatz 1 der Richtlinie genannten Ziele zu erreichen?

Halten Sie die Richtlinie für sinnvoll?
a) Falls ja, warum?
b) Falls nein, was werden Sie dagegen unternehmen?

Antwort:
In diesem Zusammenhang darf ich auf meine Ausführungen zu den Fragen 9 und 18 verweisen.

Frage 39:
Werden Sie - falls der EuGH die Richtlinie für ungültig erklärt - trotzdem für die Umsetzung in nationales Recht eintreten?

Antwort:
Die nationalen Umsetzungsaspekte sind aus meiner Sicht in Entsprechung zum EU-Recht umzusetzen, aber auch neuerlich zu überdenken, wenn der EUGH die Richtlinie für nichtig erklären würde.

Mit freundlichen Grüßen

Werner Faymann