

Anfrage + Antwort + Kommentar

Vorratsdatenspeicherung

des Abgeordneten Alexander Zach

und weiterer Abgeordneter

an die Bundesministerin für Justiz

betreffend Umsetzung der Richtlinie zur verdachtsunabhängigen Vorratsdatenspeicherung

Die Europäische Konvention zum Schutz der Menschenrechte und die Österreichische Verfassung mit dem Brief- und Fernmeldegeheimnis schützen die Privatsphäre jedes einzelnen Menschen. Art. 10a des Staatsgrundgesetzes (StGG) garantiert das Recht auf unbeobachtete elektronische Kommunikation (Kommunikationsgeheimnis), das auch das Recht umfasst, unbeobachtet seinen Kommunikationspartner auswählen zu dürfen. Der im Verfassungsrang stehende Artikel 1 des DSGVO definiert ein Grundrecht auf Datenschutz: „Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten [...]“

Eingriffe in diese Grundrechte durch staatliche Behörden sind nur nach den Bestimmungen des Art. 8 Abs. 2 der EMRK zulässig – und auch in diesen zulässigen Fällen darf der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden.

Aufgrund der Terroranschläge in Madrid und London gelang es unter britischer Ratspräsidentschaft den höchst umstrittenen und zuvor vom europäischen Parlament einstimmig abgelehnten Vorstoß zur Vorratsspeicherung der Telekommunikationsverbindungsdaten durchzubringen. Nach einem Gespräch der EU-Parlamentarier mit dem britischen Innenminister Charles Clarke beschloß das EU-Parlament in der Plenarsitzung vom 14.12.2005 die permanente und verdachtsunabhängige Überwachung der gesamten Bevölkerung der Europäischen Union.

Am 21.2.2006 segneten die Justiz- und Innenminister der EU-Länder die Richtlinie ohne weitere Aussprache ab. Irland und die Slowakei stimmten gegen die Richtlinie, weil sie das Richtlinienverfahren formal anzweifeln (es reichte aber eine qualifizierte Mehrheit der Stimmen der Ratsmitglieder). Eine Klage der beiden Länder beim Europäischen Gerichtshof ist bereits anhängig.

Im Hinblick auf eine allfällige Umsetzung der Richtlinie 2006/24/EG, den damit verbundenen Einschränkungen der Grundrechte und einer immensen Kostenbelastung für Konsumenten und Telekommunikationsunternehmen richten die unterfertigten Abgeordneten an die Bundesministerin für Justiz folgende

Anfrage:

- 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?

Zu 1:

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 von Irland gegen den Rat der Europäischen Union zu C 301/06 beim Europäischen Gerichtshof eingebrachte Klage zielt auf die Nichtigkeitserklärung der Richtlinie ab, wobei hier kein inhaltlicher sondern ein formeller Standpunkt vertreten wird, nämlich dass die richtige Rechtsform ein Rahmenbeschluss im Rahmen der 3. Säule der Europäischen Union gewesen wäre.

Mangels aufschiebender Wirkung einer solchen Klage haben die - ungeachtet des beim EuGH anhängigen Verfahrens - den Verpflichtungen aus dieser Richtlinie nachzukommen.

Da die Umsetzung der Richtlinie durch eine Änderung des TKG 2003 zu erfolgen haben wird, für deren Vorbereitung das Bundesministerium für Verkehr, Innovation und Technologie zuständig ist, muss ich mich in der Beantwortung der Anfrage auf die justiziellen Aspekte beschränken.

Art. 15 Abs. 3 der Richtlinie erlaubt den Mitgliedstaaten, die Anwendung der Richtlinie in Bezug auf die Speicherung von Kommunikationsdaten zu Internetzugang, Internet - Telefonie und Internet- E-Mail bis zum 15. März 2009 aufzuschieben. Österreich nimmt von dieser Möglichkeit Gebrauch, weshalb ich davon ausgehe, dass die Richtlinie zunächst bloß für den Bereich der klassischen Sprachtelefonie umgesetzt werden wird.

Als Justizministerin halte ich es gegenüber nationalen und supranationalen Gerichten stets so, dass ich eine präjudizierende Einschätzung des möglichen Verfahrensausganges vermeide. Grundsätzlich möchte ich aber darauf verweisen, dass der Rat im Verfahren eine Gegenschrift eingebracht hat, an deren Schlüssigkeit ich keinen Grund zu zweifeln sehe, zumal während den Verhandlungen weder der Rechtsdienst des Rates der Europäischen Union noch der Rechtsdienst der Europäischen Kommission Zweifel an der gewählten Rechtsgrundlage geäußert hat. Mit einer voreilenden Beurteilung der Erfolgsaussichten würde ich auch die Haltung Österreichs konterkarieren, das sich im Sinn einer Äquidistanz entschieden hat, weder Irland noch dem Rat als Streithelfer beizutreten.

[LIF-Anmerkung: Wir fordern nicht Umsetzen bis das Eugh-Urteil vorliegt! Wäre ja nicht das erste Mal in Österreich ...](#)

- 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?

Zu 2:

Aus meiner Sicht sollte über eine Speicherfrist von sechs Monaten ab der Beendigung des Kommunikationsverkehrs nicht hinaus gegangen werden.

- 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?

Zu 3:

Beschränkungen des Grundrechtes auf Geheimhaltung von Daten (§ 1 DSGVO) sind zur Wahrung berechtigter Interessen oder auf Grund von Gesetzen zulässig, die aus den in Art 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 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.

LIF-Anmerkung: "geht davon aus, dass die Umsetzung Emrk-konform ist": Das ist alles andere als klar. Voraussichtlich wird es nach Umsetzung in den Nationalstaaten auch Klagen bzgl Emrk geben.

"Zugriffsbedingungen, die ausschliesslich auf Zwecke der Strafverfolgung abstellen" --> später steht in der Beantwortung, Provider sollen die Daten auch bei zivilrechtlichen Sachen an Musikindustrie herausgeben dürfen.

- 4) Wieviele Bürgerinnen und Bürger sind in Österreich nach der Umsetzung der Richtlinie von der verdachtsunabhängigen Speicherung ihres Telekommunikationsverhalten betroffen?

Zu 4:

Das lässt sich derzeit nicht abschätzen. Ich möchte aber darauf hinweisen, dass Betreiber öffentlicher Telekommunikationsdienste – 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).

- 5) Zur Bekämpfung welcher Straftaten bzw. Bedrohungen ist es Ihrer Einschätzung nach gerechtfertigt, einen derartigen Eingriff in die Grundrechte vorzunehmen?

Zu 5:

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. Der Rat forderte anlässlich seiner Annahme von Änderungsvorschlägen des Europäischen Parlaments zur vorliegenden Richtlinie am 21. Februar 2006, 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 §§ 149a ff. StPO erfolgen. Es werden daher die gleich strengen Regeln zur Anwendung kommen, wie für eine Überwachung des Inhalts von Nachrichten.

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

Zu 6:

Gemäß § 149a StPO ist ein Zugriff auf die Daten im Wege einer Überwachung der Telekommunikation zulässig, wenn

- zu erwarten ist, dass die Aufklärung einer vorsätzlich begangenen mit mehr als sechsmonatiger Freiheitsstrafe bedrohten strafbaren Handlung gefördert wird und der Inhaber des Anschlusses ausdrücklich zustimmt,
- Standortdaten oder Verkehrsdaten festgestellt werden, wenn zu erwarten ist, dass die Aufklärung einer vorsätzlich begangenen mit mehr als einjähriger Freiheitsstrafe bedrohten Handlung gefördert wird.

Die Erfahrungen aus der Strafrechtspflege haben gezeigt, dass die Gerichte mit dem Einsatz des Instruments im Sinne des Verhältnismäßigkeitsprinzips maßvoll umgehen. Aus diesem Grund soll die bisherige Praxis auf der Basis des § 149a StPO beibehalten werden.

- 7) 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 (zB gerichtliche Genehmigung, gewerbliche Urheberrechtsverletzung)?

Zu 7:

Wenn derjenige, der eine Urheberrechtsverletzung begeht, sich hierzu der Dienste eines Vermittlers bedient, dann hat der in seinem Urheberrecht Verletzte nach dem Urheberrechtsgesetz verschiedene zivilrechtliche Ansprüche; es sind dies insbesondere der Unterlassungsanspruch nach § 81 Abs. 1a UrhG und der Auskunftsanspruch nach § 87b Abs. 3 UrhG. Nach dieser Bestimmung hat der Vermittler dem Verletzten auf dessen schriftliches und ausreichend begründetes Verlangen Auskunft über die Identität des Verletzers bzw. die zur Feststellung des Verletzers erforderlichen Auskünfte zu geben. Wie jeder zivilrechtliche Anspruch ist dieses Auskunftsverlangen im Bestreitungsfall durch Klage geltend zu machen; das angerufene Gericht entscheidet mit Urteil über seine Berechtigung.

Nach § 87b Abs. 3 UrhG ist es unerheblich, woher der Vermittler die für die Erteilung der Auskunft notwendigen Kenntnisse hat; dass Daten, über die nach dieser Bestimmung Auskunft zu erteilen ist, mit Daten identisch sind, die künftig im Rahmen der Vorratsdatenspeicherung erfasst werden müssen, ist natürlich nicht ausgeschlossen.

[LIF-Anmerkung](#): Ministerin beantwortet nicht die Frage, ob der Provider selbst auf die Vorratsdaten zugreifen darf, um sie weiter zu geben....

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

Zu 8:

Ich gehe 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.

- 9) 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 berufmäßigen Parteienvertretern (Rechtsanwälte, Steuerberater) telefonisch oder per E-Mail kommuniziert?
 - c) mit welchem Arzt telefonisch oder per E-Mail kommuniziert?
- 10) 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?
- 11) 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?
- 12) Sind von der Vorratsdatenspeicherung Telefonate und der E-Mail-Verkehr von Sicherheits- und Militärbehörden betroffen?
- 13) 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?

Zu 9 bis 13:

Aus meiner Sicht soll der Betreiber gar nicht die Möglichkeit erhalten, die Vorratsdaten nach bestimmten Kriterien zu ordnen. Es sollen daher die Stamm- und Verkehrsdaten aller anrufenden und angerufenen Anschlüsse für Festnetz und Mobiltelefonie, sowie im Mobiltelefonienetz die Standortkennung bei Beginn der Verbindung gespeichert werden, ohne dass diese zum Zeitpunkt der Speicherung nach einem weiteren Kriterium untersucht werden.

Zu den jeweiligen Fragen bezüglich der Emaildaten darf ich neuerlich auf die von Österreich angestrebte Umsetzung bis 15. März 2009 und die noch zu führende interministerielle Konsultation verweisen.

Der Schutz von Amtsgeheimnissen oder Berufsgeheimnissen unterliegt ausschließlich den Zugriffsbedingungen gemäß der StPO. Hier wäre auf den besonderen Schutz (§ 149a Abs. 3 StPO) von Anschlüssen von Medienunternehmen und Parteienvertretern und Angehörigen von Berufen der psychosozialen Betreuung hinzuweisen. Der Zugriff auf Vorratsdaten von Anschlüssen eines Medienunternehmens ist nur dann zulässig, wenn die zugrunde liegende Straftat mit einer lebenslänglichen Freiheitsstrafe oder mit einer Freiheitsstrafe, deren Untergrenze nicht weniger als fünf Jahre und deren Obergrenze mehr als zehn Jahre beträgt. Daten von Anschlüssen von Parteienvertretern oder Angehörigen von Berufen der psychosozialen Betreuung dürfen nur abverlangt werden, wenn die Person als Anschlussinhaber selbst der Tat dringend verdächtigt wird.

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.

- 14) 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 zB bei offenen (privaten) WLANs, Trojanern, Adware, etc anfallen können?

Zu 14:

Neben der Informationspflicht gemäß § 96 Abs. 3 TKG finden 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).

- 15) 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?
 - c) Wie sollen allfällige Nutzungsverbote kontrolliert und durchgesetzt werden?
- 16) 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?

Zu 15 und 16:

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).

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.

Die Regelungen zur Verwendung von Daten für Streitigkeiten zwischen dem Betreiber und Kunden über Entgelte nach den §§ 97 und 99 TKG werden beibehalten, so dass 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, weil diese Daten im Streitfall der Schlichtungsstelle nach § 71 Abs 2 TKG zur Verfügung zu stellen sind.

Die Übermittlung von Daten an Dritte wurde ebenso wie das Auskunftsrecht von Nutzern bereits dargestellt.

Die unbefugte Nutzung von Daten wird durch § 108 TKG erfasst. Danach ist ein Betreiber oder eine Person, die an der Tätigkeit des Betreibers mitwirkt auch dann mit einer Freiheitsstrafe von bis zu drei Monaten oder mit einer Geldstrafe bis zu 180 Tagesätzen zu bestrafen, wenn er oder sie unbefugt über die Tatsache oder den Inhalt des Telekommunikationsverkehrs bestimmter Personen einem Unberufenen Mitteilung macht oder ihm Gelegenheit gibt, Tatsachen, auf die sich die Pflicht zur Geheimhaltung erstreckt, selbst wahrzunehmen.

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

- 17) Halten Sie die Vorratsdatenspeicherung für geeignet um Terrorismus oder organisiertes Verbrechen zu verhindern?

Zu 17:

Die Diskussionen im Rahmen der Verhandlungen zur Richtlinie haben gezeigt, dass ein an das moderne Kommunikationsverhalten der Gesellschaft angepasstes Ermittlungswerkzeug für die Strafverfolgungsbehörden bei der Aufklärung von Straftaten und auch im Kampf gegen den Terrorismus von großer Bedeutung ist. Erste und schnelle Ermittlungserfolge brachte die Auswertung von Vorratsdaten nach den Terroranschlägen in Madrid am 11. März 2004 und in London am 7. Juli 2005. Die spanischen Behörden wurden auf Grund von Daten eines Mobiltelefons auf die Spur der Hintermänner geführt, die Behörden Großbritanniens konnten einen Mittäter auf Grund von Vorratsdaten und unter grenzüberschreitender europäischer Zusammenarbeit rasch ausforschen und verhaften. Diese Fakten lassen erkennen, dass die Speicherung von Vorratsdaten ein geeignetes Werkzeug für Aufklärungserfolge darstellt.

Daneben möchte ich auch auf die einstimmig angenommene Entschließung des Nationalrates zur Bekämpfung der Internetkriminalität vom 7. März 2007, 11/E (XXIII. GP) hinweisen, die ohne entsprechende Ermittlungsmethoden nicht erfolgreich verlaufen kann. Dasselbe gilt für Stalking und andere Missbräuche moderner Kommunikationsmittel.

LIF-Anmerkung: Antwort und Praxis haben gezeigt, dass die aktuelle Regelung vollkommen ausreichend ist (kurze Speicherdauer, soweit für Abrechnung notwendig). Datenzugriff erfolgte bei den Terroranschlägen binnen Stunden bzw. wenige Tage nach dem Verbrechen!

- 18) Werden Vertreter der ISPA (Internet Service Providers Austria) im Zuge der Umsetzung konsultiert?
- 19) Werden Vertreter der ArgeDaten und/oder von VIBE (Verein der Internet-Benutzer Österreichs) im Zuge der Umsetzung konsultiert?

Zu 18 und 19:

Schon während der Verhandlungen der vorliegenden Richtlinie im Rat der Europäischen Union in Brüssel waren die beteiligten Ressorts (insbesondere auch das BKA-

VD), Vertreter der Telekomindustrie und Vertreter der ISPA in den interministeriellen Koordinationsprozess eingebunden; eine solche breite Konsultation rege ich auch für die Umsetzung an.

- 20) 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 (zB Nutzung von Chatrooms)?
- 22) 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?
- 26) 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?

Zu 20, 22 und 26:

Da Österreich bezüglich der Internetdaten die Umsetzungsfrist bis 15. März 2009 nützen wird, konzentrieren sich die derzeitigen Arbeiten auf die Umsetzung hinsichtlich der Telefondaten. Was die zu speichernden Internetdaten betrifft, verweise ich auf die künftigen Konsultationen unter der führenden Zuständigkeit des Bundesministers für Verkehr, Innovation und Technologie.

21) Wer soll die Kosten für Vorratsdatenspeicherung übernehmen?

Zu 21:

Auf der Basis der Überwachungskostenverordnung, BGBl II Nr. 322/2004, werden den Betreibern die Kosten für die Mitwirkung an einer Überwachung einer Telekommunikation abgegolten. Nach Maßgabe des Erkenntnisses des Verfassungsgerichtshofs (VfGH) vom 27.2.2002 ist bei der Kostentragung für Investitionen für die Telekommunikationsüberwachung nach dem Verhältnismäßigkeitsgrundsatz eine Abwägung der Höhe der den Betreibern entstehenden Kosten einerseits und konkreter Kriterien, die eine besondere rechtliche und wirtschaftliche Beziehung begründen, andererseits vorzunehmen.

Konkrete Zahlen zu den zusätzlichen Kosten, die den Betreibern auf Grund der Speicherverpflichtung nach der vorliegenden Richtlinie entstehen werden, konnten bisher nicht einmal von den Anbietern annähernd beziffert werden. Erst nach Kenntnis dieser wird es möglich sein, im Sinne der Entscheidung des VfGH eine Kostenregelung zu finden.

[LIF-Anmerkung:](#) keine Aussage, wer Kosten übernehmen soll. im Endeffekt zahlen auf jeden fall die Bürger: entweder als Konsumenten oder als Steuerzahler.

23) 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?

Zu 23:

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 Benutzer anonymen Wertkartenhandys letztlich ausgeforscht werden.

[LIF-Anmerkung:](#) Antwort zeigt, dass Vorratsdatenspeicherung nicht notwendig ist. Bereits jetzt erfasste Daten sind ausreichend!

24) Ist Ihnen bekannt, dass bei Internet-Telefonie die Richtlinie einfach und von jedermann umgangen werden kann, indem der Konsument zB einen Diensteanbieter mit Sitz ausserhalb der EU wählt?

25) 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, das seinen Bürgerinnen und Bürger noch unbeobachtete Kommunikation gestattet?

Zu 24 und 25:

Dass die vorgesehene Vorratsdatenspeicherung keine lückenlose Überwachung mit sich bringt, ist mir bekannt. Eine solche ist auch gar nicht erwünscht.

27) Soll die anonyme Nutzung von Telefonzellen oder Internet-Cafés verboten werden?

Zu 27:

Es ist derzeit nicht vorgesehen, die Voraussetzungen für die Nutzung von öffentlichen Telefonzellen bzw. die Nutzung von Internet-Cafes zu ändern.

[LIF-Anmerkung:](#) Ministerin gibt zu, dass die Vorratsdatenspeicherung löchrig ist wie ein Schweizer Käse. Jeder mit etwas technischem Verständnis kann sie leicht umgehen; auch Kriminelle werden diese Möglichkeiten nutzen; somit bleibt: ausser Spesen nix gewesen!

28) 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?

Zu 28:

Es kommt in diesem Zusammenhang nicht darauf an, ob eine Person ein Telefon unter Angabe ihrer wahren Identität benutzt oder in Betrieb nimmt. Die Daten in einem konkreten Fall lassen die Ermittlungsbehörden Rückschlüsse ziehen, die der Strafverfolgung dienen. Die Ermittlungserfolge nach den Terroranschlägen in Madrid und in London zeigten, dass Vorratsdaten auch dann, wenn die wahre Identität des Nutzers im Verborgenen blieb, wichtige Informationen brachten, die zu der Ausforschung der Verantwortlichen der Anschläge geführt haben.

[LIF-Anmerkung:](#) Ermittlung in Strafsachen in der Regel auch ohne Kenntnis der Stammdaten (Name, Anschrift) hilfreich. --> also wozu kostenintensive Vorratsdatenspeicherung?

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

30) Halten Sie die Richtlinie für sinnvoll?

a) Falls ja, warum?

b) Falls nein, was werden Sie dagegen unternehmen?

Zu 29 und 30:

Wie die Europäische Kommission, das Europäische Parlament und die Mehrheit der Mitgliedstaaten der Europäischen Union meine ich, dass es einen großen Nutzen bringt, wenn in diesem Bereich eine Mindestharmonisierung vorgenommen wird und die zu speichernden Daten in allen Mitgliedstaaten für die Verfolgung von schweren Straftaten zur Verfügung stehen. Es besteht kein Grund von dieser Entscheidung abzugehen.

Bisher haben die Mitgliedstaaten die Speicherverpflichtung der Betreiber unterschiedlich gehandhabt. Mit der vorliegenden Richtlinie ist es gelungen, zumindest eine Harmonisierung bezüglich der Datenkategorien und der Dauer der Speicherung auf einem Minimalniveau zu schaffen. Damit geht auch einher, dass diese Daten im Rahmen der justiziellen strafrechtlichen Zusammenarbeit zur Verfügung stehen (abhängig jeweils von einer gerichtlichen Entscheidung).

31) Werden Sie – falls der EUGH die Richtlinie für ungültig erklärt – trotzdem für die Umsetzung in nationales Recht eintreten?

Zu 31:

Sollte der EUGH zum Schluss kommen, dass die Richtlinie für nichtig zu erklären ist, hat dies noch keine unmittelbaren Auswirkungen auf bereits verabschiedete nationale Umsetzungsakte. Es wird sodann abzuwarten sein, ob nicht ähnlich wie im Rahmen der sogenannten PNR- Daten rasch eine „Reparatur“ durch einen Rechtsakt im Rahmen der 3. Säule erfolgt, der sodann ebenfalls umzusetzen wäre.

[LIF-Anmerkung: Ministerin bestätigt: nationale Gesetzgebung bleibt bestehen, selbst wenn der Eugh die Richtlinie aufhebt.](#)

[CONCLUSIO: LIF wird bei Umsetzung der Vorratsdatenspeicherung in Österreich eine Klage vor dem Europäischen Gerichtshof für Menschenrechte prüfen! -> So könnte das österreichische Gesetz aufgehoben werden.](#)