REPUBLIK ÖSTERREICH
DATENSCHUTZRAT

A-1010 Wien, Ballhausplatz 2
Tel. ++43-1-531 15/2527
Fax: ++43-1-531 15/2702
e-mail: dsrpost@bka.gv.at
DVR: 0000019

GZ BKA-817.304/0003-DSR/2007

An das
Bundesministerium für Verkehr, Innovation und Technologie

Per Mail: marcin.kotlowski@bmvit.gv.at
jd@bmvit.gv.at
christian.singer@bmvit.gv.at

Betrifft: TKG- Novelle zur Umsetzung der Richtlinie über Vorratsdatenspeicherung

Der Datenschutzrat hat in seiner 175. Sitzung am 16. Mai 2007 beschlossen, zu der im Betreff genannten Thematik folgende Stellungnahme abzugeben:

- In Einklang mit seinen vorangegangenen Beschlüssen und Stellungnahmen (Beschluss vom 4. September 2002, Stellungnahme vom 8. Juli 2004 und Stellungnahme vom 20. Oktober 2005) bekräftigt der Datenschutzrat neuerlich seine Bedenken zur flächendeckenden Speicherung von Vorratsdaten für Zwecke der Strafverfolgung. Der Datenschutzrat nimmt zur Kenntnis, dass die Richtlinie 2006/24/EG über die Vorratsspeicherung 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 (im Folgenden: die Richtlinie) am 15. März 2006 vom Europäischen Parlament und vom Rat angenommen wurde, bis 15. September 2007 von den Mitgliedstaaten umzusetzen ist. Der Datenschutzrat weist jedoch darauf hin, dass die anlasslose, verdachtsunabhängige undifferenzierte Speicherung des Telekommunikationsverhaltens der Gesamtbevölkerung, unabhängig von der Speicherdauer, Fragen der Verhältnismäßigkeit und der Vereinbarkeit solcher Maßnahmen mit Art. 8 EMRK und § 1 Abs. 2 DSG 2000 aufwirft.

- Der Datenschutzrat hebt hervor, dass im Rahmen der innerstaatlichen Umsetzung der ursprüngliche Zweck und Anlass für die Erlassung der Richtlinie zu beachten ist, nämlich die Bekämpfung von Terrorismus und organisierter Kriminalität (vgl. Erwägungsgründe 7, 8, 9, 10 der RL 2006/24/EG). Innerhalb des durch die verbindlichen Regelungen des Gemeinschaftsrechts vorgegebenen Rahmens kommt dem nationalen Gesetzgeber ein rechtspolitischer Gestaltungsspielraum zu, um die konkreten Maßnahmen zur Umsetzung der Richtlinie zu setzen. Der Datenschutzrat ruft dazu auf, bei der Ausübung dieses Gestaltungsspielraumes insbesondere den datenschutzrechtlichen Grundsätzen der Zweckbindung sowie der Verhältnismäßigkeit Rechnung zu tragen.

- Der Datenschutzrat erwartet mit Interesse die Einsetzung der Expertengruppe auf der Grundlage des Erwägungsgrundes 14 der Richtlinie, insbesondere im Hinblick auf offen gebliebene Fragen, wie jene des Kostenersatzes für Anbieter oder der Anwendung der Richtlinie im Bereich der Internetdaten, und setzt sich dafür ein, dass ehebaldigst eine Abschätzung der Auswirkungen der Richtlinie vorgenommen werden sollte.

Vor diesem Hintergrund nimmt der Datenschutzrat zum Entwurf der Novelle des TKG 2003, der am 17. April 2007 vom Bundesminister für Verkehr, Innovation und Technologie vorgelegt wurde, im Einzelnen wie folgt Stellung:

§ 92 Abs. 3 Z.3 lit.a:
Die Interpretation, nach der dynamische IP-Adressen zu den Stammdaten gezählt werden, ist dem zitierten OGH-Urteil nach ho. Auffassung nicht zu entnehmen. Bei einer Definition der dynamischen IP-Adressen als „Vorratsdaten“ sollte vielmehr berücksichtigt werden, dass diese dem Kommunikationsgeheimnis gemäß § 93 TKG unterliegen, da sie (in Übereinstimmung mit der Auffassung der Datenschutzkommission, Geschäftszahl K213.000/0005-DSK/2006 vom 29.9.2006) als Verkehrsdaten zu qualifizieren sind. Dieselbe Auffassung ergibt sich auch aus den Materialien der Regierungsvorlage zum TKG 2003, 128 der Beilagen XXII. GP, Seite 19 zu § 99 Abs. 3, sowie aus dem Erwägungsgrund 15 iVm Artikel 2 lit. b) der Richtlinie 2002/58/EG.

§ 102 a Abs. 1:
Es wird gebeten, in Abs. 1 zu ergänzen, dass die Daten „[…] für einen Zeitraum von sechs Monaten ab dem Zeitpunkt der Beendigung des Kommunikationsvorganges ausschließlich zum Zweck der Ermittlung, Feststellung und Verfolgung“ schwerer Straftaten zu speichern sind.

Zur Einschränkung des Anwendungsbereichs auf **schwere Straftaten** ist folgendes auszuführen:

Vorausgeschickt werden darf, dass der Anwendungsbereich der Richtlinie auf den Zugang zu Vorratsdaten zum Zweck der Ermittlung, Feststellung und Verfolgung **schwerer Straftaten,** wie sie **von jedem Mitgliedstaat in seinem nationalen Recht bestimmt werden**, beschränkt ist (Artikel 1 der RL 2006/24/EG).

Der nach EG-Recht vorgegebene Rahmen sieht daher eine Beschränkung auf „schwere Straftaten“ vor. Dies ist mit dem Hintergrund und Anlass für die Erlassung der Richtlinie in Zusammenhang zu sehen, nämlich jenem, die Vorratsdaten-speicherung als Werkzeug zur Bekämpfung von Terrorismus und organisierter Kriminalität einzusetzen (vgl. Erwägungsgründe 7, 8, 9, 10 der RL 2006/24/EG).

Innerhalb dieses gemeinschaftsrechtlich vorgegebenen Rahmens liegt es in der Verantwortung des nationalen Gesetzgebers, die in Frage stehenden Tatbestände zu konkretisieren. Diese Umsetzung unterliegt wiederum den Vorgaben des nationalen Rechts, und damit unter anderem den datenschutzrechtlichen Grundsätzen der Zweckbindung sowie der Verhältnismäßigkeit (vgl. auch Erwägungsgrund 9 und 17 der RL 2006/24/EG).

Hinzuzufügen ist in diesem Zusammenhang, dass in der RL 2002/58/EG („Datenschutzrichtlinie für elektronische Kommunikation“) der Rechtsgrundsatz verankert ist, dass Verkehrsdaten gelöscht werden müssen, sobald eine Speicherung nicht mehr für Zwecke erforderlich ist, die mit der Kommunikation selbst zusammenhängen (einschließlich Abrechnungszwecken). Ziel der RL 2002/58 ist die Achtung der Grundrechte, insb. Art 7 und 8 der EU-Grundrechtecharta und der Anspruch, Nutzern öffentlich zugänglicher Kommunikationsdienste unabhängig von der zugrunde liegenden Technologie den gleichen Grad des Schutzes personenbezogener Daten und der Privatsphäre zu gewährleisten (vgl. insb. Erwägungsgründe 2, 3 und 4). Die Vorratsspeicherung zum Zwecke der Strafverfolgung wurde, wie auch den Erwägungsgründen 3, 4 und 9 der RL 2006/24/EG zu entnehmen ist, als Ausnahme dieser Rechtsgrundsätze konzipiert

und muss zu besonderen Zwecken der Aufrechterhaltung der öffentlichen Ordnung notwendig, angemessen und verhältnismäßig sein.

Ein Zugriff von Strafverfolgungsbehörden auf Verkehrs- und Standortdaten darf aus den genannten Gründen nur in Ausnahmefällen, unter klar und restriktiv formulierten Bedingungen und strengen Schutzmaßnahmen erfolgen. Die Umsetzungsmaßnahme hat demnach jedenfalls Zweck und Voraussetzungen eines Zugriffs unmissverständlich wiederzugeben.

Dies folgt aus dem datenschutzrechtlichen Grundsatz der Zweckbindung (§ 6 Abs. 1 Z 2 DSG 2000; Art. 5 lit. b DS-Konvention; Art. 6 Abs. 1 lit. b EG-DSRL; Art. 8 Abs. 2 GRC), nach dem personenbezogene Daten nur für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden dürfen. Auch im Falle zulässiger Beschränkungen des Grundrechts auf Datenschutz, darf der Eingriff gemäß der Verfassungsbestimmung des Artikels 1 Abs. 2 DSG 2000 jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden.

Diese - gemeinschafts- und verfassungsrechtlichen - Vorgaben müssen in einer möglichst restriktiven Definition „schwerer Straftaten“, die sich am ursprünglichen Ziel und Zweck der Richtlinie (der Bekämpfung organisierter Kriminalität und des Terrorismus) orientiert, sowie in einer klaren Abgrenzung der zugriffsberechtigten Behörden zum Ausdruck kommen. Begleitend sind datenschutzrechtliche Sicherheitsmaßnahmen und Protokollierungspflichten vorzusehen, die eine angemessene Kontrolle und Überprüfbarkeit der Datenverwendungen ermöglichen.

Die Erklärung des Rates JI zum Begriff „Schwere Straftat“ (Ratsdokument 5777/06 ADD 1 REV 1 vom 17.02.2006, http://register.consilium.europa.eu/pdf/de/06/st05/st05777-ad01re01.de06.pdf.) kann in diesem Zusammenhang zum Zweck der Definition schwerer Straftaten beispielhaft herangezogen werden. Diese Erklärung kann jedoch nicht als Umsetzungsrahmen bzw. zur Begründung der Verfassungsmäßigkeit einer nationalen Umsetzungsmaßnahme dienen, da sie als einseitige Erklärung des Rates verbindliches Gemeinschaftsrecht selbstverständlich nicht abändern kann.

Vor dem Hintergrund des verfassungsrechtlichen Gebots einer restriktiven Definition des Zugriffsbereichs und unter Berücksichtigung des gemeinschaftsrechtlichen Rahmens schlägt der Datenschutzrat vor, etwa jene Straftaten heranzuziehen, die explizit zur Umsetzung internationaler Übereinkommen bzw. europäischer Rahmen-

beschlüsse zur Bekämpfung organisierter Kriminalität bzw. des Terrorismus in das StGB eingeführt wurden (d.h. §§ 278 sowie 278 a – d StGB). Darüber hinaus wäre denkbar, Verbrechen im Sinne des § 17 Abs. 1 StGB in die Definition aufzunehmen, um Straftaten im oberen Kriminalitätsbereich einzubeziehen. Eingeschränkt könnten allenfalls zur Berücksichtigung der Erklärung zur Richtlinie auch Delikte einbezogen werden, die ausschließlich im Wege der Telekommunikation begangen werden, wie beispielsweise § 207a StGB. Eine generelle Einbeziehung von Vergehen in diese Definition ist hingegen als unverhältnismäßig iSd Artikels 1 Abs. 2 DSG 2000 (sowie auch des Artikel 8 EMRK) abzulehnen und entspricht zudem nicht den Vorgaben des Gemeinschaftsrechts.

§ 102 a Abs. 2:

Es kann jedoch nicht alleine darauf ankommen, dass Daten ausschließlich zum Zweck der Bekämpfung genannter Straftaten gespeichert werden. Vielmehr liegt ein Eingriff in das Grundrecht auf Datenschutz auch in der Übermittlung der Daten an die gemäß § 149 b Abs. 1 StPO zuständigen Behörden (Eine derartige Übermittlungsbestimmung muss dann jedenfalls eine Präzisierung der Straftaten enthalten, zu deren Verfolgung die Daten verwendet werden dürfen). Wie bereits angesprochen, ist der Zugang von Strafverfolgungsbehörden als Ausnahme von dem Grundsatz der RL 2002/58/EG zu werten, nach dem Vorratsdaten gelöscht werden müssen, sobald deren Speicherung nicht mehr für mit der Kommunikation in Zusammenhang stehende Zwecke erforderlich ist. Die Pflicht zur Vorratsspeicherung von Daten führt zu umfangreichen Datenbanken, einschließlich der Daten unbescholtener Benutzer, und birgt für den Einzelnen besondere Risiken des Datenmissbrauchs. Die in der Speicherungsverpflichtung gemäß §102a Abs. 1 vorgeschlagene Einschränkung muss sich daher auch in den entsprechenden, nationalen Bestimmungen zur Datenübermittlung wieder finden.

Dementsprechend wären die entsprechenden Bestimmungen in §§149 a ff. StPO dahingehend abzuändern, dass eine gerichtliche Anordnung gemäß § 149 b Abs. 1 StPO zur Weiterleitung von gemäß § 102a Abs. 1 gespeicherten Daten ausschließlich zum Zweck der Ermittlung, Feststellung und Verfolgung von Verbrechen im Sinne des § 17 Abs. 1 StGB, einschließlich der Tatbestände der §§ 278 und 278 a – d StGB und § 207a StGB erfolgen darf. In § 102a Abs. 2 ist ein entsprechender Verweis auf die neu gefasste Bestimmung der StPO aufzunehmen: „Eine Weiterleitung der Daten an die für die Durchführung einer Überwachung einer Telekommunikation zuständigen Behörde darf nur auf Grund einer gerichtlichen Anordnung gemäß § 149b […] StPO erfolgen."

Es wird weiters um Erläuterung gebeten, worauf sich die Formulierung „und alle sonstigen damit zusammenhängenden Informationen“ in Abs. 2 des Referentenentwurfes bezieht. Nach ho. Auffassung sollten keine anderen Daten weitergegeben werden, als jene, die für den Zweck der Anfrage erforderlich sind.

Sollte seitens des BMJ keine StPO-Novellierung ins Auge gefasst werden, so wäre in der gegenständlichen TKG-Novelle zu regeln, **zur Verfolgung welcher Straftaten auf richterliche Anordnung eine Datenübermittlung an die Strafverfolgungsbehörden** zulässig ist.

§ 102 a Abs. 3:
Es wird gebeten, § 102a Abs. 3 dahingehend zu ergänzen, dass sicherzustellen ist, „[…] dass der Zugang zu den Daten ausschließlich besonders ermächtigten Mitarbeitern der Anbieter und Betreiber öffentlicher Kommunikationsnetze vorbehalten ist, die sich zur Einhaltung des Datengeheimnisses vertraglich verpflichtet haben.“ Allenfalls könnte auch in den Erläuterungen auf die Geltung des Datengeheimnisses nach § 15 DSG 2000 verwiesen werden.

§ 102 b (Auskunftspflichten):
Zunächst stellt sich die Frage, welche Auskünfte der BM für Justiz „für den Vollzug des § 102a“ benötigt, zumal sich § 102a an die Betreiber richtet und diesen bestimmte Verpflichtungen auferlegt.

Weiters werden folgende Präzisierungen zur Formulierung dieser Bestimmung vorgeschlagen:
„[…] Dies sind insbesondere Auskünfte darüber
1. in welchen Fällen gemäß §102a Abs. 2 Daten weitergegeben wurden;
2. wie viel Zeit zwischen dem Zeitpunkt der Vorratsspeicherung der Daten und dem Zeitpunkt, zu dem sie gerichtlich angefordert wurden, vergangen ist.
3. in welchen Fällen die Anfragen nach Daten erfolglos geblieben sind.“

§ 102 c (Sanktionsbestimmung):
Gemäß Artikel 13 Abs. 2 der Richtlinie haben die Mitgliedstaaten Maßnahmen zu ergreifen, um sicherzustellen, dass der vorsätzliche, unrechtmäßige Zugang bzw. die Übermittlung von Vorratsdaten mit wirksamen, verhältnismäßigen und abschreckenden Sanktionen belegt wird. Es wird angeregt, in § 102 c eine entsprechende Ergänzung vorzunehmen, die diese Sanktionsbestimmung der Richtlinie umsetzt, da mit den in §§ 51f DSG 2000 genannten Straftatbeständen nicht das Auslangen gefunden werden kann. Ob derzeit bestehende gerichtlich strafbare Tatbestände

(etwa die §§ 118a oder 119a StGB) greifen würden, scheint zweifelhaft, da diese Tatbestände etwa insbesondere auf die Zuwendung eines Vermögensvorteils oder die Zufügung eines Nachteils abstellen, indem spezifische Sicherheitssysteme verletzt werden.

Zu § 114a:
In den Erläuterungen ist die Einschränkung auf Abs. 3 des § 102a zu streichen. Die Datenschutzkommission ist umfassend zur Kontrolle der Weitergabe von Daten gemäß § 102a TKG zuständig.

Es wird darauf hingewiesen, dass der gegenständlichen Stellungnahme in der Anlage ein Votum Separatum des Vertreters der Grünen im Datenschutzrat angeschlossen ist.

Anlage: Votum Separatum

18. Mai 2007
Für den Datenschutzrat
Der Vorsitzende:
WÖGERBAUER

Elektronisch gefertigt

Stellungnahme zur Änderung des Telekommunikationsgesetz 2003 – TKG 2003 ("Vorratsdatenspeicherung")

Abgegeben durch Hans G. Zeger, Mitglied des Datenschutzrates
Votum Separatum im Sinne §44 Abs. 3 des DSG 2000

Der vorliegende Entwurf wird als grundrechtswidriger und in Hinblick auf die in der EG-Richtlinie 2006/24/EG geschaffenen Vorgaben, als weit überschießender Versuch der umfassenden Aushöhlung der Persönlichkeitsrechte der Bürger, abgelehnt.

Weit über die EG-Richtlinie hinausgehender Entwurf

Neben den prinzipiellen Bedenken gegenüber dem Vorhaben der Vorratsdatenspeicherung richtet sich die Kritik an die Art der österreichischen Umsetzung. Manches am vorliegenden Entwurf ist unklar und schlecht geregelt. Die Umsetzung geht - wie zu zeigen sein wird - über das von der EU geforderte Niveau weit hinaus. Der vorliegende Entwurf ist somit - entgegen seinen eigenen Erläuterungen - nicht bloß die verpflichtende Umsetzung der Richtlinie 2006/24/EG sondern bildet vielmehr eine eigenständige Grundlage für eine bislang in einem Rechtsstaat nicht dagewesene Form der präventiven Überwachung der eigenen Bürger durch die staatlichen Organe.

Es soll ein eigenständiges Gesetz geschaffen werden, für das die EG-Richtlinie nur mehr Vorwand, nicht jedoch Grundlage darstellt.

Das ursprünglich angeblich angestrebte Ziel der verbesserten Terrorismusbekämpfung ist mit diesem Entwurf nicht erreichbar und wird gänzlich zugunsten der Verfolgung von Allerwelts- und Bassenaverdächtigungen, wie dem derzeit so modischen Stalking, aufgegeben.

Gerade das Beispiel Staking (§107a StGB) zeigt überdeutlich die Unverhältnismässigkeit und geradezu Obszönität des Entwurfes. Stalking, "beharrliche Verfolgung" ist ein sehr beliebtes Anzeigedelikt mit hunderten Fällen seit der Schaffung des Paragraphen, mit jedoch nur ganz wenigen entsprechenden Verurteilungen. Sicherheitspolitisch, insbesondere in Hinblick auf die Gesamtsicherheit der Bevölkerung ist das Delikt völlig bedeutungslos. Der Tatbestand dient vornehmlich in Rosenkriegen (Scheidungs- und Trennungsverfahren), Bassenastreitigkeiten, Mobbingfällen und gegenseitiger Bespitzelung als Rechtskeule zur gegenseitigen Kriminalisierung. Es zeigt von erschreckend geringer Sensibilität und geradezu Verantwortungslosigkeit der Autoren des Gesetzesentwurfes, dass sie für derartige Fälle eine flächendeckende Speicherung des Kommunikationsverhaltens aller Bürger vorsehen.

Im übrigen ist Stalking ein Delikt, dass nicht im Verborgenen geplant wird und dessen wesentliches Merkmal ("beharrlich") die Wiederholung eines unerwünschten Verhaltens ist. Einem durch Stalking Geschädigten stehen heute schon jede Menge rechtlicher Mittel offen (beginnend von der Überwachung seines eigenen Telefonanschlusses) um ganz gezielt gegen einen Stalker vorzugehen und eine zweckgerichtete Rechtverfolgung zu betreiben. Die flächendeckende Erfassung des Kommunikationsverhaltens, das jedenfalls einen Engriff in das durch Art. 10 EMRK garantierte Recht auf freier Meinungsäußerung darstellt, ist dazu nicht erforderlich.

Weitere Beispiele ließen sich ohne Zahl aufzählen. Auch Wilderei wäre durch diesen Entwurf erfasst. Auf Terrorismusjagd geht man angeblich, Wilderer erlegt man tatsächlich!

FÜR ORGANISIERTE KRIMINALITÄT LEICHT UMGEHBARE BESTIMMUNGEN

Wer Terrorismus und organisierte Kriminalität betreibt, ist organisiert und professionell genug, um die Fallen, die ihm die Vorratsdatenspeicherung stellen möchte, zu vermeiden. Die "beträchtlichen, technischen Fortschritte", die die EG-Richtlinie erwähnt, machen das problemlos möglich. Welcher Terrorist oder einigermaßen professionelle Kriminelle wird, angesichts des großen Getöses, das die Vorratsdatenspeicherung verursacht, seine Kommunikation so führen, dass sie dann im Rahmen der Vorratsdatenspeicherung auch rückverfolgbar wird?

Ausweichmöglichkeiten gibt es genug: Diensteanbieter außerhalb der EU für Internettelefonie und e-mail; Anonymisierungsdienste; Wertkartenhandys; Roamingdienste; Telefonzellen; Internetcafes; etc... Das sind die Möglichkeiten, die schon dem Normalbürger spontan einfallen.

Wie die Herkunft von eMails zu verschleiern sind, zeigen uns die täglichen Phishingattacken. Mails werden nicht über offzielle und somit durch die Vorratsdatenspeicherung erfasste Mailserver verschickt, sondern heimlich über geknackte Privat-PCs, auf denen mittels Würmer entsprechende Serverprogramme installiert wurden.

Die Vorratsdatenspeicherung ist als massiver Eingriff, der sich nicht einmal ansatzweise bemüht, gesetzte Maßnahmen abzufedern und auf Einzelfälle zu konzentrieren und stattdessen die gesamte Bevölkerung unter Generalverdacht stellt, abzulehnen. Sie stellt einen ersten - aber beträchtlichen -Schritt weg vom Rechtstaat, der erst auf konkreten Verdacht hin tätig wird, hin zum Unrechtsstaat, der vorsorglich mal alle verdächtigt und präventiv auch ohne Ansatzpunkt tätig wird, dar.

UNZULÄSSIGER PAUSCHALVERDACHT UNBESCHOLTENER BÜRGER

Die Vorratsdatenspeicherung wird massenweise Datensammlungen mit sich bringen, allerdings nur geringen Erfolg. Der positive Effekt in der Terrorbekämpfung und bei der organisierten Kriminalität wird nicht wahrnehmbar sein. Der unbescholtene Einzelbürger, der durch Zufälligkeiten, falsche Verdächtigungen und Auswertungsfehlern ins Visier der "Sicherheitsorgane" gerät wird große Aufwändungen in der Beseitigung der Verdachtsmomente haben. In Einzelfällen wird ihm das nicht gelingen, in vielen Fällen wird er mit einer nachhaltigen Beänträchtigung und Schädigung seines Ansehens rechnen müssen, es wird ihm aber im Gegenzug dazu kaum der positiver Effekt - "erhöhte Sicherheit" - geboten werden.

GESETZESENTWURF BENUTZT TERRORISMUSBEKÄMPFUNG ALS VORWAND ZUR TOTALÜBERWACHUNG

Welche Straftaten die Mitgliedsländer als schwer genug betrachten, um eine Vorratsdatenspeicherung zu rechtfertigen, liegt bei ihnen selbst. Dem jeweiligen nationalen Gesetzgeber wird in der EG-Richtlinie ausdrücklich das Recht gegeben, diese gesetzlich zu bestimmen. Zu orientieren hat er sich dabei aber an den Erwägungsgründen der Richtlinie, welche diese erst interpretierbar machen.

Betrachtet man diese im konkreten Fall, dann wird klar: Die Richtlinie spricht in ihren Erwägungsgründen von "schweren Fällen" wie beispielsweise organisierter Kriminalität und Terrorismus. Ein Auftrag an den nationalen Gesetzgeber, generell bei Straftaten, die mit mehr als einem Jahr Freiheitsstrafe bedroht sind, massenweise Datenabfragen zu gestatten, lässt sich daraus keinesfalls

ableiten. Die Festlegung des österreichischen Gesetzgebers, die Verarbeitung auf sämtliche Straften nach § 17 SPG anzuwenden, ist daher willkürlich und durch die Vorgaben der EU nicht mehr gedeckt.

Nicht verzichtet werden soll hier darauf, einige Delikte beispielsweise zu nennen, bei denen künftig Abfragen zulässig sein soll, geht man vom vorliegenden Entwurf aus: Mitwirkung am Selbstmord (§78 StGB); Fahrlässige Tötung und besonders gefährlichen Verhältnissen (§81 StGB, umfaßt auch Verkehrsunfälle), Raufhandel (§91 StGB), Auskundschaftung eines Geschäfts- oder Betriebsgeheimnisses (§123 StGB), Schwere Sachbeschädigung (§126 StGB) sowie schwere Vermögensdelikte, wie etwa Diebstahl, Unterschlagung, Veruntreuung einschließlich schwere Eingriffe in fremdes Jagd- und Fischereirecht bei Schäden über EUR 50.000, betrügerische Krida (§156 StGB), Geldwucher, Begünstigung eines Gläubigers, Brandstiftung, Störung einer Religionsausübung (§189 StGB), Falsche Beweisaussagen vor Gerichten oder Verwaltungsbehörden (§§288 und 289).

KRITIK ZU §102A ABS. 1:

Wie bereits im Allgemeinen Teil der Stellungnahme erläutert wurde, entspricht die Einbeziehung sämtlicher Delikte nach § 17 SPG sowie der §§ 107 und 107 a StGB keineswegs den Intentionen der umzusetzenden Richtlinie. Das ergibt sich vor allem aus der Gesamtbetrachtung der Erwägungsgründe der Richtlinie.

In Art. 5 der Erwägungsgründe zur zugrundeliegenden Richtlinie wird ausgeführt, dass das Ziel eine weitgehende Vereinheitlichung der europäischen Bestimmungen zur Vorratsdatenspeicherung ist. In Art. 8 der Erwägungsgründe wird auf die Erklärung zum Kampf gegen den Terrorismus verwiesen.

In Art. 9 der Erwägungsgründe wird darauf verwiesen, dass Vorratsdatenspeicherung insbesondere in schweren Fällen wie organisierter Kriminalität oder Terrorismus notwendig und hilfreich sei.

Art. 1 Abs. 2 der Richtlinie hält zwar fest, dass sich diese auf "schwere Straftaten, wie von jedem Mitgliedsstaat in seinem Recht bestimmt werden" bezieht. Diese Bestimmung ist aber keineswegs so zu interpretieren, dass die Vorratsdatenspeicherung jedenfalls bei allen Delikten greifen soll, welche nationale Rechtsordnungen als "schwer" bezeichnen. Das wäre schon insoferne sinnlos, als die jeweiligen, nationalen Rechtsordnungen hier sehr unterschiedlich sind.

Während eine Rechtsordnung Delikte mit einer Androhung einer mehr als sechsmonatigen Freiheitsstrafe schon als schwerwiegend beurteilen mag, erfassen andere Rechtsordnungen – wie die österreichische- erst Delikte ab einer Strafdrohung von mehr als einem Jahr Freiheitsstrafe als schwerwiegend. Weiters ist fragwürdig, ob überhaupt alle Rechtsordnungen von EU- Mitgliedsstaaten den Begriff von „schweren Straftaten“ oder einen ähnlichen kennen.

Hinzu kommen natürlich noch die sehr unterschiedlichen Strafdrohungen bei den jeweiligen einzelnen Delikten. Eine solche Interpretation des Art. 1 Abs 2 der Richtlinie würde somit jedenfalls den Zweck, eine einheitliche europäische Basis zu schaffen, völlig unterlaufen.

Sinngemäß kann der Art. 1 Abs. 2 der Richtlinie somit jedenfalls nur dahingehend interpretiert werden, dass dem nationalen Gesetzgeber die Möglichkeit eingeräumt wird, die jeweiligen Delikte zu bezeichnen, für welche die Vorratsdatenspeicherung gilt, dies aber nicht nach Gutdünken sondern im Geiste der Richtlinie. Eine Erstreckung der Vorratsdatenspeicherung auf alle Delikte mit einer Strafdrohung von mehr als einem Jahr Freiheitsstrafe ist somit eine mehr als unnötige Fleißaufgabe des österreichischen Gesetzgebers, der damit weit über die ihm aus der Richtlinie erwachsenden Verpflichtungen hinausgeht.

Vorgeschlagen wird somit, dass der Gesetzgeber ersatzweise einen Katalog von Delikten erstellt, für welche die Vorratsdatenspeicherung gelten soll und diesen auf jene Delikte beschränkt, die tatsächlich im Hintergrund von Terrorismus und organisierter Kriminalität stehen. Beispiele dafür sind die §§ 278 ff. StGB.

KRITIK ZU §102A ABS. 2:

Diese Bestimmung macht die umfangreiche Datenaufzählung in § 92 Abs. 4 a des Entwurfs insoferne sinnlos, als hier eine Übermittlung "sonstiger Informationen" vorgesehen wird. Die Erläuternden Bemerkungen sehen zu dieser Bestimmung keinerlei Bechränkung vor. Bei Formulierungen dieser Art ist jedenfalls zu befürchten, dass dies Anlass zur Übermittlung weiterer, nicht ausdrücklich genannter personenbezogener Daten bieten könnte, sofern diese als "notwendige Information" eingestuft werden. Vorgeschlagen wird daher, diesen Teil ersatzlos zu streichen.

Weiters ist darauf zu verweisen, dass der vorliegende Entwurf bei der Datenübermittlung an zuständige Behörden keine Rücksicht auf den Schutz besonderer Berufsgruppen nimmt.

Eine Überwachung eines Teilnehmeranschlusses ist im Sinne von § 149 a Abs. 3 StPO für den Fall, dass dessen Inhaber ein Medienunternehmen ist, nur dann zulässig, wenn zu erwarten ist, dass dadurch die Aufklärung einer strafbaren Handlung gefördert werden kann, die mit lebenslanger Freiheitsstrafe oder mit einer zeitlichen Freiheitsstrafe bedroht ist, deren Untergrenze nicht weniger als fünf Jahre und deren Obergrenze mehr als zehn Jahre beträgt.

Verteidiger, Rechtsanwälte, Notare und Wirtschaftstreuhänder, Psychiater, Psychotherapeuten, Psychologen, Bewährungshelfer sowie eingetragene Mediatoren dürfen nur überwacht werden, wenn diese Personen selbst einer Tat dringend verdächtig sind.

Durch den vorliegenden Entwurf wird dieser Schutz besonderer Berufsgruppen insoferne zahnlos, als die Überwachung auf den Telekombetreiber ausgelagert werden kann und es für die Speicherung und Übermittlung von Vorratsdaten keine Beschränkung wie in §149 a Abs. 3 StPO gibt. Der bestehende Schutz für besondere Berufsgruppen sollte durch die Vorratsdatenspeicherung jedenfalls nicht unterlaufen werden und es wird daher vorgeschlagen, die Verkehrsdaten dieser Gruppen von der Vorratsspeicherung jednefalls auszunehmen.

KRITIK ZU §102A ABS. 3:

Vorgeschlagen wird, zusätzlich zur "besonderen Ermächtigung" der jeweiligen Personen, welche Zugang zu den Daten haben auch auf deren Pflichtenseite abzustellen, insbesondere deren Verpflichtung zur Geheimhaltung und zum Datenschutz.

KRITIK ZU §102B:

Die Verpflichtung zur Auskunft „sämtlicher Informationen, die für den Vollzug von §102 a TKG nötig sind“ ist zu weitgehend formuliert. Die Aufzählung der zu erteilenden Auskünfte sollte nicht- wie hier im Entwurf- nur deklarativ sondern abschließend erfolgen, um sicherzustellen, dass mit dem vorliegenden Entwurf nicht über die Übermittlung der in §92 Abs 3 Z 4 a TKG aufgezählten Daten hinausgegangen wird.

Im Zusammenhalt mit der neu eingeführten Strafbestimmung des §109 Abs. 3 Z 17 b TKG besteht die Gefahr, dass auf Telekombetreiber massiver druck ausgeübt wird, alle gewünschten Informationen zu erteilen.

BISHER UNZUREICHENDE STELLUNGNAHME DES DATENSCHUTZRATES

Der Autor anerkennt die Bemühungen des Datenschuzrates eine Vorratsdatenspeicherung im möglichst geringen Umfang zu verlangen, weist aber ausdrücklich darauf hin, dass die Grundrechtsverletzung des geplanten Vorhabens in den bisherigen Stellungnahmen nicht ausreichend gewürdigt wurde. Die bisherigen DSR-Stellungnahmen blieben daher unzureichend und können vom Autor nicht mitverantwortet werden.