An die
Parlamentsdirektion
Begutachtungsverfahren

1010 Wien

Wien, 21. Mai 2007

Betreff: Stellungnahme der ARGE DATEN zu
Bundesgesetz, mit dem das Telekommunikationsgesetz 2003 – TKG 2003 geändert wird - "Vorratsdatenspeicherung"
Zeichen: 61/ME (XXIII. GP) / BMVIT-630.333/0001-III/PT2/2007

In der Anlage finden Sie die Stellungnahme der
ARGE DATEN - Österreichische Gesellschaft für Datenschutz
mit dem dringenden Ersuchen um Kenntnisnahme und Berücksichtigung.

Für allfällige Fragen stehen wir gerne zur Verfügung.

Mit vorzüglicher Hochachtung

Mag. Dr. Hans Gerhard ZEGER, Vertretung ARGE DATEN als Obmann
CN = Mag. Dr. Hans Gerhard ZEGER, Vertretung ARGE DATEN als Obmann, C = AT, L = Wien, S = Wien, O = ARGE DATEN - Oesterreichische Gesellschaft fuer Datenschutz
2007.05.21 12:27:18 +02'00'

Dr. Hans G. Zeger (Obmann)

Charlotte Schönherr (Schriftführerin)

Stellungnahme elektronisch übermittelt

Alle Stellungnahmen werden unter ftp://ftp.freenet.at/privacy/gesetze veröffentlicht.

Stellungnahme der ARGE DATEN vom 21. Mai 2007 zu:

BUNDESGESETZ, MIT DEM DAS TELEKOMMUNIKATIONSGESETZ 2003 – TKG 2003 GEÄNDERT WIRD - "VORRATSDATENSPEICHERUNG

Allgemeiner Teil

1. Einleitung

Das Bundesministerium für Verkehr, Innovation und Technologie hat den Entwurf einer Novelle des Telekommunikationsgesetzes 2003 ausgearbeitet und das Begutachtungsverfahren eingeleitet.

Ziel und einziger Schwerpunkt des vorliegenden Entwurfes ist - ausgehend von den Erläuterungen zum Entwurf- die Umsetzung der Richtlinie 2006/24/EG in das österreichische Recht, somit die Schaffung einer österreichischen Gesetzesgrundlage für die viel diskutierte "Vorratsdatenspeicherung".

Kritik und Bedenken sollen aus unserer Sicht in diesem Zusammenhang auf verschiedenen Ebenen ansetzen. Einerseits sind starke grundsätzliche Bedenken gegen das Vorhaben der Vorratsdatenspeicherung, wie es die eingangs zitierte Richtlinie vorsieht, anzumelden. Seitens der österreichischen Verantwortungsträger wurde im Rahmen der Präsentation des vorliegenden Gesetzesentwurfs in den vergangenen Tagen und Wochen stets schon fast entschuldigend angemerkt, man sei eben an die Vorgaben der EU gebunden und habe "ohnedies nur die Minimalstandards" umgesetzt.

Ein derartiges Vorgehen ist aus unserer Sicht unzulässig und typisch für den Umgang der österreichischen Politik bei der Umsetzung von Europarecht. Üblicherweise werden durch den österreichischen Gesetzgeber zahlreiche europarechtliche Standards, die eigentlich verpflichtend wären, nur zögerlich und schleppend umgesetzt, insbesondere dann, wenn die korrekte Umsetzung mit einem Zuwachs an persönlichen Rechten des Einzelnen verbunden wäre. Zu verweisen ist dabei etwa auf die mangelhafte Umsetzung der EU-Datenschutzrichtlinie und anhängige Beschwerden bei der EU-Kommission in dieser Frage.

Umgekehrt präsentiert sich der österreichische Gesetzgeber im Falle der "Vorratsdatenspeicherung", die gravierende Einschränkungen der persönlichen Rechte des einzelnen Bürgers mit sich bringt, als EU-Musterschüler. Auf inhaltliche Kritik wird im Rahmen notwendiger Diskussion dabei in der Regel nicht eingegangen, sondern die Verantwortung nach Brüssel delegiert, um sich den lästigen Diskurs mit den eigenen Bürgern über die Einschränkung ihrer Rechte zu sparen. Dabei ist aber darauf zu verweisen, dass die Republik Österreich im Rahmen der Vorarbeiten zur Entstehung der zugrundeliegenden Richtlinie kaum Kritik an der EU-Entscheidung gezeigt hat, die Rechte ihrer Bürger im Rahmen des Gesetzwerdungsprozesses zu schützen. Zu erinnern ist daran, dass Slowakei und Irland ein Verfahren vor dem Europäischen Gerichtshof angestrengt haben. Die österreichischen Verantwortungsträger haben offensichtlich nicht daran gedacht, sich für die Grundrechte ihrer Bürger einzusetzen. Weder wurde fristgerecht eine Beschwerde beim EuGH eingebracht, noch sind sie bereit, eine entsprechende

Entscheidung des EuGH über die Richtlinie abzuwarten. So schlampig die Richtlinienumsetzung in zahlreichen anderen Bereichen funktioniert, so streng ist man wenn es um Überwachung geht.

Aufgrund dieser Vorgehensweise ist demnach evident: Die Republik Österreich ist für den Inhalt der zugrundeliegenden Richtlinie wesentlich verantwortlich, die österreichischen Entscheidungsträger identifizieren sich offensichtlich mit ihrem Inhalt und stehen somit der Überwachung der Bürger positiv gegenüber. Die grundsätzliche Kritik an der Vorratsdatenspeicherung richtet sich demnach genauso an den österreichischen Gesetzgeber und kann nicht mit dem Verweis auf Vorgaben aus Brüssel ignoriert werden.

Neben den prinzipiellen Bedenken gegenüber dem Vorhaben der Vorratsdatenspeicherung richtet sich die Kritik aber auch an die Art der österreichischen Umsetzung. Manches am vorliegenden Entwurf ist unklar und schlecht geregelt. Wesentlich ist aber: 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.

2. Vorratsdatenspeicherung als massiver Grundrechtseingriff

Auch wenn es in den vergangenen Wochen nur zu oft wiederholt wurde, muss es hier noch einmal klargestellt werden: Der Schritt zur Vorratsdatenspeicherung ist der massivste grundrechtliche Dammbruch der vergangenen Jahre. Letztendlich bedeutet er nichts anderes, als dass vom Prinzip der Unschuldsvermutung in einem wesentlichen Bereich abgegangen werden soll und die Türe hin zur präventiven Verdächtigung und zu präventiven Verfolgungsmaßnahmen gegen die eigenen Staatsbürger geöffnet wird. An die Stelle des rechtsstaatlichen Prinzips, dass die behördliche Verfolgung von Einzelpersonen daran gemessen wird, ob es konkrete Verdachtsmomente gegen diese gibt, regiert der Grundsatz: Überwachen wir präventiv gleich alles, irgendetwas werden wir schon finden und ein Verdächtiger wird eben beweisen müssen, dass er unschuldig ist.

Damit wird der Übergang von einer freien Gesellschaft zu einer Alibigesellschaft, in der nur derjenige als unbescholten gilt, der lückenlos seine Schuldlosigkeit beweisen kann, vollzogen.

Dieser Grundgedanke zeigt dabei nicht nur von absoluter Ignoranz gegenüber den Rechten der einzelnen Person sondern ist auch Ausdruck einer offenbaren Hilflosigkeit der Verantwortungsträger, mit verschiedenen Entwicklungen der vergangenen Jahre umzugehen. Man sieht bereits an den Erwägungsgründen der zugrundeliegenden Richtlinie, die ausdrücklich auf die Terroranschläge von London verweisen, woher der Wind bläst. Da verwundert es auch nicht, dass offenbar know-how und finanzielle Mittel aus dem Umkreis des militärisch-elektronischen Komplexes der USA eingesetzt werden sollen, um die Vorratsdatenspeicherung europaweit tatsächlich umzusetzen.

Wie im Fall "SWIFT" zeigt sich hier die Unfähigkeit und der Unwillen der europäischen Regierungen, gegenüber dem großen Bruder auf der anderen Seite des Atlantiks in Grundrechtsfragen einen eigenständigen Kurs einzuschlagen. Das Paradoxon, dass man offenkundig vermeint, Angriffen auf den Rechtsstaat ausgerechnet dadurch beikommen zu können, dass man diesen aushöhlt und abschafft, schlägt im Rahmen der Vorratsdatenspeicherung voll durch.

Der Weg, der durch die Vorratsdatenspeicherung eingeschlagen wird, kann anbetracht "der beträchtlichen technischen Fortschritte" - wie es die Richtlinie selbst höhnend formuliert - in eine sehr gefährliche Richtung führen: Mit gezieltem Softwareeinsatz wird es für die Behörden problemlos möglich, die sozialen Kontakte von Personen aufzuzeichnen, soziale Netzwerke von Personen zu erstellen, deren Kontakte zu verwerten - kurz: Das Privatleben der Bürger uneingeschränkt zu durchleuchten -wohlgemerkt: ohne, dass jemals eine Straftat begangen wurde, sondern lediglich aus Vermutungen heraus, dass dies vielleicht mal passieren könnte. Jeder ist verdächtig, das Gegenteil soll er selbst beweisen. Der Weg zum gläsernen Menschen ist damit offen.

Dass vorläufig im Rahmen der Vorratsdatenspeicherung nur „Verkehrs-" und „Stammdaten" und keine "Inhaltsdaten" verarbeitet werden sollen, tröstet kaum Einerseits erlaubt schon die alleinige Aufzeichnung der Verkehrsdaten einen umfassenden Einblick in das soziale Netzwerk von Menschen und damit massive Eingriffe in das Privatleben, andererseits zeigt die Vergangenheit: Ist einmal der erste Schritt getan, fällt der nächste Überwachungsschritt umso leichter. Es ist unschwer auszumalen, was passieren wird, sollte ein nächster Terroranschlag in Europa - der sich auch mit der Vorratsdatenspeicherung nicht verhindern lassen wird - stattfinden. Man wird den Verantwortungsträgern - mit Recht - vorhalten, dass sich die eingeschlagenen Maßnahmen trotz massiver Grundrechtseingriffe als untauglich erwiesen haben, um die Bürger zu schützen. Es ist kaum anzunehmen, dass zugegeben wird, dass die Vorratsdatenspeicherung ein Fehlschlag war.

Wer politische Mechanismen kennt, weiß, dass dann erst recht Begehrlichkeiten nach immer neuen Grundrechtseingriffen geweckt werden. Das Argument wird dann lauten: Die Vorratsdatenspeicherung war prinzipiell schon richtig, aber nicht ausreichend. Nächster Schritt wäre dann natürlich eine Ausweitung auf eine präventive Überwachung inhaltlicher Nachrichten. Die Demontage des Rechtsstaates findet in westlichen Demokratien heute nicht über Revolutionen sondern scheibchenweise immer "zum Besten der Bürger" - statt.

Im Ohr klingen auch die Beteuerungen, dass entsprechende Maßnahmen ohnedies unabhängigen Richtern unterworfen werden, ohne die nicht selbständig ausgewertet werden darf. Die Botschaft hört man wohl, massive Skepsis ist aber angebracht. Wer sich an die vor wenigen Jahren stattgefundene "Spitzel-Affäre" erinnert, weiß, dass rechtsstaatliche Garantien auf dem Papier und die Behördenrealität auch in Österreich oft weit auseinanderklaffen. Wenn man Berichte über den Zustand der Wiener Polizei in den vergangenen Jahren Ernst nimmt, kann einem letztendlich nur Angst und Bang werden, wann immer behördliche Kompetenzen ausgeweitet werden.

Aus rechtlicher Sicht ist evident, dass die beschlossene Richtlinie dem Art. 8 EMRK nicht genügen kann. Im eigentlichen Sinne geht es nämlich nicht um "vorbeugende

Gefahrenabwehr", die sich auf einzelne Fälle konzentriert. Vielmehr soll vorab- ohne Anlass- soviel wie nur möglich gespeichert werden, das man dann im konkreten Anlassfall verwerten will. Derartige "Präventivrundumschläge" gegen alles und jeden können aber jedenfalls nicht als angemessene Einschränkung der Privatsphäre im Sinne des Art. 8 EMRK gesehen werden.

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 auf konkreten Verdacht hin tätig wird, hin zum Unrechtsstaat, der vorsorglich mal alle verdächtigt und präventiv auch ohne Ansatzpunkt tätig wird, dar.

3. Vorratsdatenspeicherung wirkungslos

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" 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; innerhalb der EU werden diese Fremdhandys dann über Roaming-Verträge unidentifizierbar genutzt; Anonymisierungsdienste; Wertkartenhandys; Telefonzellen; Internetcafes; etc... Das sind die Möglichkeiten, die schon dem Normalbürger spontan einfallen. Daher: Wenn ein Krimineller auch nur einigermaßen professionell agiert, wird er sich eben auf die neuen Rahmenbedingungen problemlos umstellen können. Soll man da auch ansetzen und Freiheitsrechte weiter einschränken? Ausweispflicht im Internetcafe, PIN-Code bei der Telefonzelle, Handys nur mehr registriert, etc..? Auch das wird nichts nutzen, da angesichts des "beträchtlichen, technischen Fortschritts" mit Sicherheit nicht alle Umgehungsmöglichkeiten ausgeschlossen werden können.

Wie die Herkunft von eMails zu verschleiern ist, 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 Würmern entsprechende Serverprogramme installiert wurden.

BotNets, dass sind illegale Internetnetzwerke, werden von der organisierten Kriminalität in Zukunft nicht nur für Hackerangriffe genutzt werden, sondern auch für unerkannte Internettelefonie oder für eMail- und Web-Kommunikation. Mehrere tausend derartiger BotNets sind heute schon bekannt, beginnend mit einigen tausend bis zu einer Million infizierten Rechnern, allesamt geknackte PrivatPCs, die als unerkannte Plattform für illegale Aktionen genutzt werden.

Das bedeutet nun nicht, dass die Vorratsdatenspeicherung- vor allem so, wie sie der

österreichische Entwurf umsetzen will - in der Verfolgung von Straftaten gänzlich ohne Anwendungsbereich bleiben wird. Tatsächlich gibt es ja auch genug unprofessionelle und schlicht dumme Kriminelle, aber auch Personen, denen auf Grund krankhafter Neigungen das Unrechtsbewußtsein fehlt (z.B. Stalker), die sich nicht ausreichend umstellen werden. Diese wird man in Einzelfällen ausforschen können.

Allgemeine Kriminalitätsbekämpfung ist gar nicht das Ziel der Richtlinie - wie es sich aus den Erwägungsgründen eindeutig ergibt - sondern die Verfolgung von Terrorismus und organisierter Kriminalität. Der vorliegende Entwurf zur Novelle des TKG macht aber keinen Unterschied und setzt nur bei der Höhe der Strafdrohung an. Offenbar möchte man in Österreich die Vorgaben der EU, die sich auf Terrorismus und organisierte Kriminalität beziehen, ausnutzen, um sich neue Befugnisse zur Verbrechensbekämpfung zu verschaffen, die auf Grundrechte keine Rücksicht nehmen. Die lästige Diskussion kann man dabei - angenehmerweise - mit dem Totschlagargument "ist ja durch die EU so vorgegeben, da kann man gar nix machen" umgehen.

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 und falsche Verdächtigungen und Auswertungsfehler ins Visier der "Sicherheitsorgane" gerät wird große Aufwendungen in der Beseitigung der Verdachtsmomente haben. In Einzelfällen wird ihm das gar nicht gelingen, in vielen Fällen wird er mit einer nachhaltigen Beeinträchtigung und Schädigung seines Ansehens rechnen müssen, es wird ihm aber im Gegenzug dazu kaum der positive Effekt - "erhöhte Sicherheit" - geboten werden.

4. Vorratsdatenspeicherung ist kostenintensiv

Die Einschränkung der Bürgerrechte lässt man sich offenbar gerne etwas kosten. Während in anderen Bereichen Gelder fehlen und stets auf den Sparzwang verwiesen und das ausgeglichene Budget betont wird, ist für die Vorratsdatenspeicherung offenbar nichts zu teuer. Angesichts der offensichtlichen Wirkungslosigkeit solcher Instrumentarien in Hinblick auf ihre Ziele, ist es nicht vermessen hier von "Geldverschwendung" zu sprechen.

Die Kostenfrage ist bislang überhaupt nicht geklärt. Bei den Kosten sind verschiedene Elemente zu berücksichtigen: Die Kosten der Vorbereitung treffen sowieso die Allgemeinheit. Fraglich ist, wer die Kosten dafür tragen soll, dass die entsprechenden Diensteanbieter speichern und Abfragen behandeln sollen. Die Aufwendungen für tatsächliche Abfragen sollen mit einem Ersatz für die entsprechenden Unternehmen abgegolten werden: Zahlen soll also die Allgemeinheit. Die Kosten der Speicherung selbst sind allerdings nicht geregelt, müssten demnach von den Diensteanbietern selbst getragen werden, die sich - aus deren Sicht verständlich - dagegen aussprechen. Umgekehrt gilt, warum soll die Allgemeinheit für diese Aufzeichnung zahlen, also auch Personen die Finanzierung tragen müssen, die die entsprechenden Dienste nicht in Anspruch nehmen und somit gar nicht als Verdächtige in Frage kommen?

Der Bürger zahlt seine eigene Freiheitseinschränkung somit gleich doppelt: Für konkrete Abfragen steht er als Steuerzahler gerade, die Datenspeicherung zahlt er als Kunde über verteuerte Tarife mit.

5. Gesetzesentwurf benutzt Terrorismusbekämpfung als Vorwand zur Totalüberwachung

Während die österreichischen Entscheidungsträger in der Öffentlichkeit betonen nur "Minimalstandards" - und das auf Druck der EU- umzusetzen, ergibt sich bei Betrachtung des vorliegenden Gesetzesentwurfs ein ganz anderes Bild:

Der vorliegende Entwurf geht in seiner Reichweite über die Vorgaben der EU in beträchtlichem Ausmaß hinaus: Während das Ziel der Richtlinie sich auf Terrorismusbekämpfung und organisierte Kriminalität konzentriert, möchte der österreichische Gesetzgeber anhand des vorliegenden Entwurfs gleich alle Straftaten, die mit mehr als einem Jahr Strafe bedroht sind, erfassen. Möglich wird dies durch den Verweis des vorliegenden Entwurfs auf § 17 SPG, der als mit beträchtlicher Strafe bedrohte Delikte jene gerichtlich strafbaren Handlungen definiert, die mit mehr als einjähriger Freiheitsstrafe bedroht sind.

Welche Straftaten die Mitgliedsländer als schwer genug betrachten, um eine Vorratsdatenspeicherung zu rechtfertigen, liegt letztlich bei ihnen selbst. Dem jeweiligen nationalen Gesetzgeber wird das Recht gegeben, diese gesetzlich zu bestimmen. Zu orientieren hat er sich dabei an den Erwägungsgründen der Richtlinie, welche die Richtlinie erst interpretierbar machen. 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 willkürlich und durch die Vorgaben der EU nicht gedeckt.

Nicht verzichtet werden soll darauf, einige Delikte beispielsweise zu nennen, bei denen künftig Auswertungen der Daten zulässig sein sollen: Mitwirkung am Selbstmord (§78 StGB); Fahrlässige Tötung unter besonders gefährlichen Verhältnissen (§81 StGB), Raufhandel (§91 StGB), Auskundschaftung eines Geschäfts- oder Betriebsgeheimnisses (§123 StGB), Schwere Sachbeschädigung (§126 StGB) sowie etwa 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).

Dank expliziter Aufführung im Entwurf zu §102a TKG sind auch die gefährliche Drohung und der Anti- Stalkingparagraph umfasst. (§§107 und 107a StGB)

Die obige Aufzählung erhebt keinerlei Anspruch auf Vollständigkeit, sondern soll lediglich stellvertretend dafür stehen, was der österreichische Gesetzgeber aus einer Richtlinie, die

der Bekämpfung von internationalem Terrorismus und organisierter Kriminalität dienen soll, macht. Selbstverständlich enthält jedes der aufgeführten Delikte für sich einen strafrechtlichen Handlungsunwert und soll nicht bagatelisiert werden. Mit den eigentlichen Zielen der zugrundeliegenden Richtlinie hat dies nichts mehr zu tun.

Gerade im Zusammenhang mit einem Modedelikt, wie Stalking, ließen sich zwar trefflich "Erfolgsmeldungen" produzieren. Fehlt doch vielen Stalkern mit ihrer oft krankhaften Neigung anderen Personen nachzustellen, jedes Unrechtsbewußtsein. Sie werden daher auch keine Verschleierungsmaßnahmen für ihre Taten treffen und könnten dann durch die Vorratsdatenspeicherung noch leichter ausgeforscht werden als es bisher schon der Fall ist.

Umgekehrt ist das Stalking-Delikt geradezu ein Musterbeispiel für den Missbrauch der neuen Datenaufzeichnungen. Charakteristisches Merkmal von Stalking ist die "Beharrlichkeit" in der Nachstellung. Ein Stalkingopfer hat daher schon jetzt durch zeitgerechte Anzeige und gezielte Überwachung ihres Telefonanschlusses jede denkbare Möglichkeit der Verfolgung und Aufklärung des Delikts. Das nachträgliche Herumschnüffeln in Daten unbescholtener Bürger ist dazu überhaupt nicht erforderlich.

Der österreichische Gesetzgeber geht somit mit seinem Entwurf über die Vorgaben der EU weit hinaus. Österreich ist hier nicht nur "EU-Musterschüler" sondern benutzt die Vorgaben der EU offenbar dazu, um diese als Rechtfertigung für massive Kompetenzausweitungen im sicherheitspolizeilichen Bereich heranzuziehen.

Ausgehend von den Vorgaben der Richtlinie wären zwei Vorgehensweisen anzudenken gewesen: Einerseits ist es denkbar, als Gradmesser für entsprechende Datenabfragen anstatt §17 SPG §17 StGB heranzuziehen, eine Abfrage von verarbeiteten Vorratsdaten somit davon abhängig zu machen, ob mit der entsprechenden Straftat ein "Verbrechen" verübt wurde. Das würde die Situation insoferne entschärfen als ein Zugriff auf gespeicherte Vorratsdaten nur mehr bei mit mehr als dreijähriger Freiheitsstrafe bedrohten Vorsatzdelikten möglich wäre.

Noch sinnvoller schiene es allerdings, im Geist der Richtlinie einen eigenen Katalog mit Delikten zusammenzustellen und einen Datenzugriff ausschließlich für diese dann genannten Straftaten zu gestatten. Eine solche Nennung von Delikten könnte sich auf jene beschränken, welche tatsächlich im Bereich der organisierten Kriminalität angesiedelt sind. Dann könnte Österreich einerseits darauf verweisen, seinen europarechtlichen Verpflichtungen nachgekommen zu sein, andererseits würde man den Eingriff in persönliche Freiheitsrechte auf ein vielleicht erträglicheres Ausmaß reduzieren.

6. Fazit

Die Vorratsdatenspeicherung bedeutet nicht nur einen Einschnitt im Umgang der Politik mit bürgerlichen Freiheitsrechten, der seinesgleichen sucht.

Das eigentliche Ziel des Vorhabens, dem internationalen Terrorismus und der organisierten Kriminalität Einhalt zu gebieten, wird man anhand des vorliegenden Gesetzesentwurfs nicht erfüllen können. Stattdessen wird man massenweise Daten

unbescholtener Bürger ohne irgendein Verdachtsmoment verarbeiten und diese dem Risiko aussetzen, dass mittels technischer Möglichkeiten deren persönliches Leben massiv durchleuchtet wird.

Über den Sinn der Richtlinie geht der vorgelegte Entwurf insoweit beträchtlich hinaus, dass er sich nicht auf Datenzugriffe bei tatsächlicher organisierter Kriminalität beschränkt, sondern dass undifferenziert bei sämtlichen Delikten, die mit mehr als einem Jahr Freiheitsstrafe bedroht sind, zugegriffen werden soll. Mit EU-Recht lässt sich der vorgelegte Entwurf nicht rechtfertigen, vielmehr bekundet er den Willen des österreichischen Gesetzgebers zur exzessiven Überwachung des Privatlebens seiner Bürger in allen Lebensbereichen.

Besonderer Teil

Im folgenden Teil werden die rechtlichen Bedenken zu verschiedenen Teilen des vorliegenden Entwurfs behandelt.

§ 92 Abs. 3 Z 3 lit.a :

Die Auffassung, dass dynamische IP- Adressen Stammdaten sind, ist weder juristisch noch technisch haltbar und wird - entgegen den erläuternden Bemerkungen - auch nicht durch die regelmäßige Judikatur bestätigt.

Der Gesetzgeber unterliegt in diesem Zusammenhang der Fehlvorstellung, dass jemand, der mittels IP- Adresse Stammdaten des Teilnehmers wie Name und Anschrift abfrägt bereits in Kenntnis der "Adresse" des Teilnehmers im Sinne des jeweiligen "Anschlusses" agiert, somit bei der Zuordnung dynamischer IP-Adressen keine Verarbeitung von Verkehrsdaten stattfindet. Diese Fehlauffassung geht weiters davon aus, dass anhand einer IP-Adresse ein Teilnehmeranschluss bereits individualisiert ist. Damit wird ignoriert, dass - auch entsprechend den Ausführungen der DSK (K 213.000/0005-DSK/2006) - sehr wohl Verkehrsdaten verarbeitet werden müssen, um aufgrund einer IP-Adresse auf die Stammdaten des Teilnehmers zu schließen. Dies ist insbesondere in Bezug auf dynamische Adressen der Fall, da dort, um den jeweiligen Teilnehmer feststellen zu können, in einem Erstschritt ermittelt werden muss, welchem Anschluss zum jeweiligen Zeitpunkt die IP-Adresse zugeordnet war.

Letztendlich führt die Rechtsauffassung, dynamische IP-Adressen seien als "Stammdaten" zu interpretieren zu einem erheblich schlechteren Schutzniveau des jeweiligen Benutzers bei Internetdiensten gegenüber jenem bei Telefonie, insbesondere in Hinblick auf §149 a StPO. Einmal mehr zeigt sich anhand dieses Beispiels, dass das Aufkommen neuer Technologien seitens des Gesetzgebers leider oft dazu benutzt wird, anhand technisch und juristisch unrichtiger Argumente jene Schutzmechanismen, die bei Anwendung herkömmlicher technischer Gegebenheiten erkämpft wurden, auszuhebeln.

§ 102 a Abs. 1:

Wie bereits im Allgemeinen Teil der Stellungnahme erläutert wurde, entspricht die Einbeziehung sämtlicher Delikte nach §17 SPG sowie der §§107 und 107a 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, die 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 „schwere 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 etwa die §§278 ff StGB.

Auch die Speicherdauer ist im Entwurf letztlich unklar geregelt. Der Entwurf spricht zwar von einer Aufbewahrungsdauer von "sechs Monaten ab dem Zeitpunkt der Beendigung des Kommunikationsvorgangs" und davon, dass danach die Daten unverzüglich zu löschen sind. Unklar ist jedoch, was diese Löschungsbestimmung in der Praxis bedeuten soll.

Soll dies bedeuten, dass alle Daten die einen Tag älter als sechs Monate sind, gelöscht werden müssen, dies würde einerseits eine tägliche Löschung erfordern, andererseits bleibt unklar, welcher Zeitraum tatsächlich gemeint ist, 180 Tage, jeweils ganze Kalendermonate oder der jeweilige Datumsstichtag. Es ist zu befürchten, dass auf Grund dieser Unklarheiten die Daten noch wesentlich über die sechs Monate hinaus aufbewahrt werden.

102 a 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 Erklärung 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, bei der Übermittlung der in Bezug auf die genannten Berufsgruppen vorratsgespeicherten Daten auf den bestehenden Schutz Rücksicht zu nehmen.

§ 102 a 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. Diese Verpflichtungen bedürfen besonderer Präzisierung.

§ 102 b :

Die Verpflichtung zur Auskunft „sämtlicher Informationen, die für den Vollzug von §102a 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.