ARGE DATEN

DB RECHT11158 / STELL / Unser Zeichen: vorrat-stellung-2010.doc

per FAX: +43.1.71162 65 4109

An das
BMVIT
Sektion III, Abteilung PT 2

Ghegastraße 1
1030 Wien

Wien, 10. Jänner 2010

Betreff: **BMVIT-630.333/0001-III/PT2/2009**
Stellungnahme der ARGE DATEN zum Entwurf der Novelle des Telekommunikationsgesetzes 2003 hinsichtlich der Umsetzung der EU-Richtlinie 2006/24/EG über die Vorratsspeicherung

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

_____
Dr. Hans G. Zeger (Obmann)

Anlage:
Stellungnahme

Ergeht in Kopie an:
Parlamentsdirektion (☑ *begutachtungsverfahren@parlinkom.gv.at,* ☐ Druckversion)

Eine Kopie der Stellungnahme wird weiters an folgende Adresse(n) verschickt:
☑ jd@bmvit.gv.at, evamaria.weissenburger@bmvit.gv.at [electronic mail]

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

ARGE DATEN - Österr. Gesellschaft für Datenschutz A-1160 Wien, Redtenbacherg. 20 ☎ +43/676/9107032, Fax +43/1/4803209
www.argedaten.at DVR 0530794 info@argedaten.at Gerichtsstand Wien
ZVR 774004629 UID ATU 56627966 PSK 7.214.741 (BLZ 60000, IBAN: AT15 6000 0000 0721 4741, BIC: OPSKATWW)

An die
Parlamentsdirektion
Begutachtungsverfahren

1010 Wien

Wien, 10. Jänner 2010

Betreff: **BMVIT-630.333/0001-III/PT2/2009**
Stellungnahme der ARGE DATEN zum Entwurf der Novelle des Telekommunikationsgesetzes 2003 hinsichtlich der Umsetzung der EU-Richtlinie 2006/24/EG über die Vorratsspeicherung

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

elektronisch erstellt
Dr. Hans G. Zeger (Obmann)

Stellungnahme elektronisch übermittelt (*begutachtungsverfahren@parlinkom.gv.at)*

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

ARGE DATEN - Österr. Gesellschaft für Datenschutz A-1160 Wien, Redtenbacherg. 20 ☎ +43/676/9107032, Fax +43/1/4803209
www.argedaten.at DVR 0530794 info@argedaten.at Gerichtsstand Wien
ZVR 774004629 UID ATU 56627966 PSK 7.214.741 (BLZ 60000, IBAN: AT15 6000 0000 0721 4741, BIC: OPSKATWW)

Stellungnahme zum Entwurf der Novelle des Telekommunikationsgesetzes 2003 hinsichtlich der Umsetzung der EU-Richtlinie 2006/24/EG über die Vorratsspeicherung

1. Einleitung

Das Bundesministerium für Verkehr, Innovation und Technologie hat den Entwurf einer Novelle des Telekommunikationsgesetzes 2003 ausgearbeitet und das Begutachtungsverfahren eingeleitet. Ausgearbeitet wurde der Entwurf durch das Ludwig Boltzmann Institut für Menschenrechte (BIM). Den Kernpunkt des Begutachtungsentwurfs bilden die Bestimmungen zur Umsetzung der EU-Richtlinie 2006/24/EG über die Vorratsspeicherung.

Nach Darstellung des BIM verfolgt der Entwurf unter anderem das Ziel, die Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten so umzusetzen, dass zwar ihr Zweck innerstaatlich erreicht werde, zugleich aber durch gesetzliche Vorkehrungen sichergestellt sei, dass die mit der Vorratsdatenspeicherung verbundenen Grundrechtseingriffe so gering wie möglich ausfallen sollen. Quelle:http://www.univie.ac.at/RI/Datenvorratsspeicherung/Grundzuge%20des%20BIM-Entwurf%20zur%20TKG%20Novelle%202010.pdfSoferne dies tatsächlich das Ziel gewesen sein sollte, wurde es mit dem vorliegenden Entwurf jedenfalls nicht erreicht.

Seitens der österreichischen Verantwortungsträger wurde im Rahmen des Umsetzungsprozesses der Richtlinie schon im Rahmen der Präsentation des ersten Entwurfs der Umsetzung im Jahre 2007 fast entschuldigend angemerkt, man sei eben an die Vorgaben der EU gebunden und habe "ohnedies nur Minimalstandards" umgesetzt.

Die verdachtsunabhängige Speicherung von Kommunikationsdaten aller Nutzer elektronischer Kommunikationsdienste stellt einen massiven Eingriff in die Grundrechte, insb. das Gebot der Achtung der Privatsphäre des Art. 8 EMRK, das Grundrecht auf Datenschutz des Art. 1 DSG, das Fernmeldegeheimnis des Art. 10a StGG und das Kommunikationsgeheimnis des § 93 TKG, das Recht auf freie Meinungsäußerung der Art. 10 EMRK und Art. 13 StGG sowie die Unschuldsvermutung des Art. 6 Abs. 2 EMRK dar. Auch wenn der vorliegende Gesetzesentwurf versucht, Grundrechtsverletzungen möglichst gering zu halten, kann nicht darüber hinweggetäuscht werden, dass bereits die Speicherung von Kommunikationsdaten an sich grob unverhältnismäßig in Grundrechte eingreift. Die Verletzung der Grundrechte entsteht hierbei nicht erst durch die Nutzung der gespeicherten Daten, sondern bereits durch die gesetzliche Anordnung der fortwährenden, pauschalen Speicherung von Kommunikationsdaten.

Das gewählte Vorgehen ist aus unserer Sicht nicht zulässig und typisch für den Umgang der österreichischen Politik bei der Umsetzung von europarechtlichen Normen. Üblicherweise werden durch den österreichischen Gesetzgeber zahlreiche europarechtliche Standards, die 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 etwa auf die mangelhafte Umsetzung der EU-Datenschutzrichtlinie und anhängige Beschwerden bei der EU-Kommission zu den datenschutzrechtlich relevanten Fragen des Fehlens einer unabhängigen Datenschutzbehörde sowie der rechtswidrigen Regelung der indirekt personenbezogenen Daten in Österreich.

Umgekehrt präsentiert sich der österreichische Gesetzgeber im Falle der "Vorratsdatenspeicherung", die gravierende Einschränkungen der persönlichen Rechte des einzelnen Bürgers mit sich bringt, als Musterschüler. Auf inhaltliche Kritik wird nicht eingegangen, sondern die Verantwortung nach „Brüssel“ delegiert, um sich den lästigen Diskurs mit den eigenen Bürgern über die Einschränkung von deren Rechten zu sparen. Dabei ist darauf zu verweisen, dass die Republik Österreich im

Rahmen der Vorarbeiten zur Entstehung der zugrundeliegenden Richtlinie kaum Kritik und Engagement gezeigt hat, die Rechte ihrer Bürger im Rahmen des Gesetzwerdungsprozesses zu schützen. Zu erinnern ist daran, dass Slowakei und Irland zumindest ein Verfahren vor dem Europäischen Gerichtshof angestrengt haben, um zu klären, ob die Richtlinie über die Vorratsspeicherung von Daten auf einer gültigen Rechtsgrundlage beschlossen wurde. Die österreichischen Verantwortungsträger haben nicht daran gedacht, sich für die Grundrechte ihrer Bürger einzusetzen. Die entsprechende- zu Recht überaus umstrittene- Entscheidung des EuGH fiel bekanntermaßen zugunsten der Richtlinie aus, wobei die Grundrechtskonformität ausdrücklich ungeklärt bleibt.

Nach Ergehen der EuGH-Entscheidung hatte es der österreichische Gesetzgeber eilig, den Umsetzungsprozess abzuschließen. So schlampig die Richtlinienumsetzung in zahlreichen anderen Bereichen funktioniert, so streng ist man wenn es um mehr Überwachung geht.

Aufgrund der bisherigen 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 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.

Es ist davon auszugehen, dass die Umsetzung über das von der EU geforderte Niveau weit hinausgeht. Es ist - wie noch dargestellt wird - noch in keiner Weise geklärt, bei welchen Straftaten es überhaupt zu einer Auskunft der vorratsgespeicherten Daten kommen soll. Eine Einschränkung im Sinne einer teleologischen Interpretation der Richtlinie ist im vorliegenden Entwurf in keiner Weise enthalten. Der vorliegende Entwurf ist somit - entgegen seinen eigenen Erläuterungen - nicht bloß die verpflichtende Umsetzung der Richtlinie 2006/24/EG sondern bildet eine eigenständige Grundlage für eine bislang in einem Rechtsstaat nicht dagewesene Form der präventiven Überwachung der eigenen Bürger durch die staatlichen Organe.

Die österreichischen Abgeordneten sollten diesem Entwurf ihre Zustimmung verweigern und stattdessen, unter Hinweis auf die seit 1. Dezember 2009 geltenden EU-Grundrechtscharta, den Verflichtungen der Europäischen Menschenrechtskonvention und den verfassungsgesetzlich garantierten Grund- und Freiheitsrechten auf eine Aufhebung der EG-Richtlinie 2006/24/EG hinarbeiten.

2. Vorratsdatenspeicherung als massiver Grundrechtseingriff

1.) Missachtung des Gebotes der Achtung der Privatsphäre

Art. 8 EMRK schützt sowohl das Privatleben als auch die Kommunikation in umfassender Weise: vom Schutzbereich erfasst werden persönliche Beziehungen als solche ebenso wie die „äußeren" Kommunikationsdaten sämtlicher Korrespondenz, also Zeit, Ort, Kommunikationspartner und Art der Kommunikation. Auch das Grundrecht auf Datenschutz des Art. 1 DSG schützt Kommunikationsdaten – als personenbezogene Daten – vor unzulässiger Verwendung.

Die Vorratsdatenspeicherung greift massiv in Recht auf Achtung des Privatlebens und der Korrespondenz ein, indem sie die wahllose Speicherung der Kommunikationsdaten sämtlicher Nutzer ohne jegliches Verdachtsmoment anordnet. Bei Kenntnis sämtlicher Verbindungs-, Standort- und Internetzugangsdaten (Telefonate, SMS, MMS, Email, IP-Adresse, Benutzerkennung usw.) einer bestimmten Person, also mit wem diese Person wann, von wo aus, wie lange und in welcher Form elektronisch kommuniziert hat, können umfassende Personenprofile erstellt und soziale Netzwerke, private und berufliche Kontakte sowie Bewegungsprofile sichtbar gemacht werden, auch Rückschlüsse auf persönliche Eigenschaften und Neigungen etc. werden möglich.

Ein derartig massiver Eingriff in Art. 8 EMRK ist unverhältnismäßig und desavouiert die demokratische Gesellschaft. Die bislang nur behauptete aber nicht nachgewiesene Eignung der Vorratsdatenspeicherung zur Erfüllung des in der RL 2006/24/EG definierten Zweckes, nämlich die Ermittlung, Feststellung und Verfolgung schwerer Straftaten zu fördern, ist in Frage zu stellen. Dies angesichts der meist unzuverlässigen Aussagekraft der aus den Daten abgeleiteten Informationen sowie der gleichzeitig relativ einfachen Umgehungsmöglichkeiten (Eintragung einer falschen E-Mail Absenderadresse, Mailserver außerhalb der EU, anonyme Remailer und Proxies, Prepaid-Wertkarten, Einsatz von Instant-Messaging Programmen). Daraus ergibt sich eine Unangemessenheit des äußerst intensiven Eingriffs, da er zur Erreichung der gewünschten Zwecke nur in sehr geringem Maße geeignet ist. Lückenlos erfasst werden primär die Kommunikationsprofile argloser und unbescholtener Bürger, während es für „schwere Straftäter" ein Leichtes ist, sich der Überwachung zu entziehen.

Zudem existieren Alternativen zur Vorratsdatenspeicherung, die weniger eingriffsintensiv und hinsichtlich der Betroffenen zielgerichteter sind. Art. 1 Abs. 2 DSG verlangt überdies ausdrücklich die Wahl des gelindesten zum Ziel führenden Mittels. So ermöglicht z.B. das in den USA praktizierte „*quick freeze*"-Verfahren im Verdachtsfall die kurzfristige Anordnung der Speicherung von Kommunikationsdaten, auf die – sollte sich der Verdacht erhärten – unter den üblichen Voraussetzungen des Strafverfahrens (in Österreich z.B. eine richterliche Genehmigung) zugegriffen werden kann. Damit wird einerseits der Verlust möglicherweise relevanter Daten im Ermittlungsverfahren verhindert, andererseits sind nur jene Personen Ziel einer derartigen Maßnahme, gegen die begründete Verdachtsmomente vorliegen.

2.) Aushöhlung des Fernmelde- und des Kommunikationsgeheimnisses

Das Fernmeldegeheimnis des Art. 10a StGG wird in § 93 TKG als Kommunikationsgeheimnis einfachgesetzlich näher ausgestaltet. Das Fernmeldegeheimnis umfasst sowohl Kommunikationsinhalte als auch die Tatsache, ob eine Kommunikation stattgefunden hat, also Verkehrsdaten, und erlaubt Eingriffe nur bei richterlicher Genehmigung. Das Kommunikationsgeheimnis führt das Fernmeldegeheimnis weiter aus und verbietet das Mithören, Abhören, Aufzeichnen, Abfangen und sonstige Überwachen von Nachrichten und der damit verbundenen Verkehrs- und Standortdaten, wenn nicht eine Einwilligung aller beteiligten Benutzer, eine Genehmigung für eine Fangschaltung oder ein Notruf vorliegen. Die Vorratsdatenspeicherung verlangt nun in vollkommener Ignoranz des Fernmelde- und des Kommunikationsgeheimnisses die pauschale Speicherung aller Verkehrs- und Standortdaten sämtlicher Nutzer. Auch wenn Kommunikationsinhalte von der Vorratsdatenspeicherung prinzipiell nicht erfasst sind, kann bei Kenntnis des Adressaten (z.B. hilfe@krebshilfe.at, frauennotruf@wien.at, info@akvorrat.at) und der Art, Häufigkeit und des Zeitpunkts der Kontakte vielfach auf die Inhalte der Kommunikation rückgeschlossen werden, wodurch das Fernmelde- und das Kommunikationsgeheimnis auch in Hinblick auf die Kommunikationsinhalte ausgehöhlt werden. Selbst besonders geschützte Personen-

oder Berufsgruppen werden unterschiedslos erfasst, womit das besondere Vertrauensverhältnis z.B. zwischen Arzt und Patient, Anwalt und Mandant oder zwischen Redakteur und Informant (Redaktionsgeheimnis, Informantenschutz!) nachhaltig gestört wird.

3.) Beschränkung des Rechts auf freie Meinungsäußerung

Die Vertraulichkeit der Kommunikation ist unabdingbare Vorraussetzung für die freie Bildung und den Austausch von Meinungen in einer liberalen und demokratischen Gesellschaft. Die intensive und beständige Kommunikationsüberwachung unter Bruch des Fernmelde- und Kommunikationsgeheimnisses wird auch das Recht auf freie Meinungsäußerung einschließlich des Rechts auf Freiheit zum Empfang und zur Mitteilung von Nachrichten verletzt. Kommunikation ist nicht mehr frei, sondern wird protokolliert, um im Nachhinein kontrollierbar zu sein. Das Wissen um die Protokollierung der Kommunikationsdaten reicht aus, um das Kommunikationsverhalten empfindlich zu verändern. Bereits die Speicherung (und nicht erst die Verwendung!) führt somit zu einer Verletzung der in Art. 10 EMRK und Art. 13 StGG verbürgten Grundrechte.

4.) Pervertierung der Unschuldsvermutung

Die gesetzliche Anordnung der Speicherung von Kommunikationsdaten stellt alle Nutzer elektronischer Kommunikationsdienste von vornherein unter Verdacht, schwere Straftäter oder hochgradig gefährlich zu sein, zumindest aber mit solchen Personen zu kollaborieren, und verstößt somit gegen die in Art. 6 Abs. 2 EMRK verankerte Unschuldsvermutung. Private Telekommunikationsanbieter sollen durch vorliegenden Gesetzesentwurf zur Bürgerüberwachung verpflichtet werden und als Handlanger des Staates dienen. Während Telekommunikationsanbieter bislang lediglich im konkreten Verdachtsfall betriebsnotwendig vorhandene Daten an die Strafverfolgungsbehörden übermitteln, sollen sie künftig gegen finanzielle Entschädigung dem Staat möglichst umfassende Daten für allfällige spätere Verwendungen verschaffen. Eine für den Staat bequeme wenn auch ineffiziente und die Menschenwürde missachtende Ermittlungsmethode zur „Beruhigung“ des Bürgers.

5.) Fortgesetzte Datenverwendung, Missbrauchgefahr

Sind Daten erst vorhanden, so besteht stets Gefahr, dass neue Begehrlichkeiten in Hinblick auf die Verwendung der Daten entstehen und die Hemmschwelle für den Zugriff auf die Daten sinkt. Zudem besteht die Gefahr missbräuchlicher Datenverwendung bis hin zur wirtschaftlichen Nutzung der Daten. Der Nutzer hingegen hat de facto keine Kontrolle über die ihn betreffenden Kommunikationsdaten und die auf Basis dieser Daten evtl. fälschlich gezogenen Schlussfolgerungen über seine Person. Der Nutzer muss nicht mit allen hinter einer Telefonnummer oder Email-Adresse stehenden Personen in persönlicher Beziehung stehen, noch weniger hat der Nutzer Kontrolle über eingehende Anrufe oder Emails, die sein „Personenprofil“ nach außen jedoch verändern und ihn „verdächtig“ machen können.

Eine zusätzliche Gefahrenquelle stellen die nach § 102c Abs. 2 des Entwurfes von den Providern an die Datenschutzkommission (also das Bundeskanzleramt) und das Bundesministerium für Justiz zu liefernden Protokolldaten dar. Um Missbrauch hintan zu halten und für statistische Zwecke ist nach § 102c jeder Zugriff auf Vorratsdaten sowie jede Anfrage und Auskunft über diese zu protokollieren. Diese Protokolldaten sind jedoch doppelbödig: sie geben Namen und Anschrift der „höchst suspekten“ Personen wieder, nämlich jener, die abgefragt wurden, jedoch einschließlich jener, die erfolglos, irrtümlich oder sonst „mitabgefragt“ wurden. In diesem Zusammenhang ist

erneut auf die mangelnde Unabhängigkeit der Datenschutzkommission hinzuweisen, ein Mangel, der auch durch die aktuelle DSG-Novelle nicht behoben wurde.

6.) Gesetz bildet Übergang zur Alibigesellschaft

Auch wenn es im Laufe des Umsetzungsprozesses oftmals 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 in den Fällen "SWIFT" und „PNR-Daten“ 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.

Dass vorläufig im Rahmen der Vorratsdatenspeicherung 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 eben nicht anhand von Revolutionen sondern scheibchenweise immer "zum besten der Bürger" - wenn auch gegen deren Willen - 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; Anonymisierungsdienste; Wertkartenhandys; Telefonzellen; Internetcafes; etc... Das sind die Möglichkeiten, die schon dem Normalbürger spontan einfallen. 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 sind, zeigen uns die täglichen Phishingatacken. Mails werden nicht über offzielle und somit durch die Vorratsdatenspeicherung erfasste Mailserver verschickt, sondern heimlich über geknackte Privat-PCs, sogenannten Bot_netzen, auf denen mittels Würmer entsprechende Serverprogramme installiert wurden.

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 genug unprofessionelle und schlicht dumme Kriminelle, die sich nicht ausreichend umstellen werden. Diese wird man in Einzelfällen ausforschen können.

Allgemeine Kriminalitätsbekämpfung ist jedoch nicht 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 bleibt hinsichtlich der Frage, bei welchen Straftaten es eigentlich zu einer Auskunft der vorratsgespeicherten Daten kommen soll, völlig unklar. Während der Begutachtungsentwurf aus 2007 - heftig kritisiert - noch einen klaren Verweis auf § 17 SPG enthalten hat und damit grundsätzlich Delikte mit eine Strafuntergrenze von über einem Jahr in den Auskunftsanspruch einbezogen hat, begnügt sich der vorliegende Entwurf damit, von „schweren Straftaten“ zu sprechen. Dieser Begriff ist allerdings weder im TKG noch in einer anderen Norm definiert, der Entwurf bleibt somit hinsichtlich einer der essentiellsten Fragen vollkommen unpräzise und ist –soferne es nicht zu Novellierungen anderer Gesetze kommt – isoliert betrachtet aufgrund der Unbestimmtheit in dieser Frage auch verfassungswidrig. Über die Beweggründe, warum man einen somit letztlich unvollständigen Gesetzesentwurf in Begutachtung bringt, lässt sich nur spekulieren. Auszugehen ist davon, dass der Gesetzgeber durch eine spätere Novellierung zB des SPG oder StGB „durch die Hintertür“ vollendete Tatsachen schaffen und sich somit einer lästigen Diskussion im Begutachtungsverfahren des TKG entziehen will - eine Vorgehensweise die wohl bei jedem Demokraten massive Bedenken auslösen muss.

Offenbar möchte man in Österreich die Vorgaben der EU, die sich auf Terrorismus und organisierte Kriminalität beziehen, ausnutzen, um sich neue Befugnisse zur allgemeinen Verbrechensbekämpfung zu verschaffen, die auf Grundrechte keine Rücksicht nehmen muss. Die lästige Diskussion kann man - angenehmerweise - mit dem Totschlagargument "ist durch die EU vorgegeben, da kann man gar nix machen" umgehen.

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

4. Vorratsdatenspeicherung kostenintensiv

Die Einschränkung der Bürgerrechte lässt man sich offenbar auch viel kosten. Während in anderen Bereichen Gelder fehlen und stets auf den Sparzwang verwiesen und das ausgeglichene Budget betont wird, ist für die Vorratsdatenspeicherung 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 nicht abschließend geklärt. Bei den Kosten sind verschiedene Elemente zu berücksichtigen: Die Kosten der Vorbereitung treffen sowieso die Allgemeinheit. Die Aufwendungen für die Überwachung und Abfragen soll mit einem Ersatz für die entsprechenden Unternehmen verbunden werden. Der Begutachtungsentwurf spricht hier von einem angemessenen Kostenersatz. Zahlen soll also die Allgemeinheit. Im Gegensatz zum Begutachtungsentwurf 2007, bei welchem die Kosten der Speicherung von den Diensteanbietern selbst getragen hätten werden müssen, kommt nun der Steuerzahler für sämtliche Kosten auf.

Hier stellt sich die Frage: 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 doppelt: Für konkrete Abfragen steht er als Steuerzahler gerade, die Datenspeicherung auf Vorrat 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, enthält der vorliegende Entwurf keine derartige, teleologische Einschränkung.

Der verwendete Begriff „schwere Straftat“ ist dem österreichischen Rechtsbestand in dieser Form- wie schon dargelegt- nicht bekannt. Auch die Erläuternden Bemerkungen geben keinerlei Aufschluss, was der Begutachtungsentwurf darunter versteht. Es lässt sich somit spekulieren, ob der Gesetzgeber damit auf § 17 SPG (mit „beträchtlicher Strafe“ bedrohte Straftaten, die mit mehr als einjähriger Freiheitsstrafe sanktioniert werden) oder den Verbrechensbegriff des § 17 StGB abstellen will (Verbrechen sind vorsätzliche Handlungen, die mit lebenslanger oder mit mehr als dreijähriger Freiheitsstrafe bedroht sind). Aufgrund der gewählten Vorgehensweise und der Tatsache, dass bereits der Begutachtungsentwurf 2007 auf § 17 SPG abgestellt hat, ist davon auszugehen, dass der Gesetzgeber auch diesmal mit mehr als einjähriger Freiheitsstrafe bedrohte Delikte einbeziehen will. Selbst wenn allerdings eine dreijährige Strafgrenze zugrunde gelegt werden sollte, würde dies wenig an der grundsätzlichen Problematik ändern.

Welche Straftaten die Mitgliedsländer als schwer genug betrachten, um eine Vorratsdatenspeicherung zu rechtfertigen, liegt 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 oder mehr als drei Jahre Freiheitsstrafe bedroht sind, massenweise Datenabfragen zu gestatten, lässt sich daraus keinesfalls ableiten.

Nicht verzichtet werden soll darauf, einige Delikte beispielsweise zu nennen, bei denen künftig Auswertungen der Daten – unterstellt man die einjährige Grenze - zulässig sein soll: 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 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).

Auch gewerbsmäßige Urheberrechtsverletzungen gem. § 91 UrhG wären bei Zugrundelegung einer einjährigen Strafbarkeitsschwelle in den Auskunftsanspruch einbezogen, da der Gesetzgeber fürsorglich im Rahmen der aktuellen StPO-Novelle gerichtliche Ermittlungsverfahren bei Privatanklagedelikten vorsieht, was im Vorfeld von der Musikindustrie bereits lautstark beklatscht wurde. Die Einbeziehung derartiger Delikte in die Vorratsdatenspeicherung hat mit dem Zweck der Richtlinie nichts mehr zu tun, zumal – zumindest im Falle von zivilrechtlichen Verfahren - der EuGH den Mitgliedsstaaten ausdrücklich freistellt, ob ein entsprechender Auskunftsanspruch bei Urheberrechtsverletzungen geschaffen wird.

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 ist, dass jedem der aufgeführten Delikte für sich ein strafrechtlicher Handlungsunwert innewohnt. Mit den eigentlichen Zielen der Richtlinie hat dies nichts mehr zu tun.

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 dazu, um diese als Rechtfertigung für massive Kompetenzausweitungen im sicherheitspolizeilichen Bereich zu heranzuziehen.

Ausgehend von den Vorgaben der Richtlinie wäre es sinnvoll gewesen, im Geist der Richtlinie einen eigenen Katalog mit Delikten zusammenzustellen und einen Datenzugriff ausschließlich für diese Straftaten zu gestatten. Eine solche Nennung von Delikten könnte sich auf jene beschränken, welche tatsächlich im Bereich der organisierten Kriminalität angesiedelt sind.

6. Fazit

Die Vorratsdatenspeicherung bedeutet einen höchst gefährlichen Einschnitt im Umgang der Politik mit bürgerlichen Freiheitsrechten.

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 deren persönliches Leben bloß auf Grund vager verdachtsmomente 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 undifferenziert und unklar bei „schweren Straftaten" 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.

Es wird daher empfohlen diesem Entwurf generell die Zustimmung zu verweigern und in einem allfälligen Verfahren vor dem EuGH unter Hinweis auf die seit 1. Dezember 2009 geltenden EU-Grundrechtscharta, den Verflichtungen der Europäischen Menschenrechtskonvention und der verfassungsgesetzlich garantierten Grund- und Freiheitsrechte auf eine Aufhebung der EG-Richtlinie 2006/24/EG hinzuarbeiten.