nemox.net
THE SOLUTION GROUP

An das
Bundesministerium für Verkehr, Innovation und Technologie (BMVIT)
Sektion III, Abteilung PT 2
Ghegastraße 1
A-1030 Wien
Austria

Innsbruck, 11. 01. 2010

Stellungnahme zum Entwurf BMVIT-630.333/0001-III/PT2/2009
Novelle des TKG 2003 zur Umsetzung der
Richtlinie über die Vorratsdatenspeicherung 2006/24/EG

Zum Ministerialentwurf 117/ME (XXIV. GP) Änderung des TKG 2003 nehmen wir mit Ersuchen um Kenntnisnahme und Berücksichtigung wie folgt Stellung:

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.

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 das 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, E-Mail, IP-Adressen, Benutzerkennungen 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

nemox.net
Steiner und Würtenberger OEG
Eduard-Bodem-Gasse 9
A-6020 Innsbruck

Telefonnr.: +43 5 0234-0
Faxnr.: +43 5 0234-9
E-Mail: info@nemox.net

Bank Austria / Creditanstalt
Kontonummer.: 51538098801
Bankleitzahl.: 12000

UID-Nummer.: ATU50232305
Steuernummer: 013/2811
Firmennummer: 199483 h

nemox.net
THE SOLUTION GROUP

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 „organisierte Kriminelle“ 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 zB das sogenannte *„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 zB 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. Ein solches *„quick freeze“*-Verfahren kennt beispielsweise die europäische Cybercrime-Convention und wird auch in den USA praktiziert.

3) 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 (zB 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 zB zwischen Arzt und Patient, Anwalt und Mandant oder zwischen Redakteur und Informant (Redaktionsgeheimnis, Informantenschutz) nachhaltig gestört wird.

4) 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

nemox.net
Steiner und Würtenberger OEG
Eduard-Bodem-Gasse 9
A-6020 Innsbruck

Telefonnr.: +43 5 0234-0
Faxnr.: +43 5 0234-9
E-Mail: info@nemox.net

Bank Austria / Creditanstalt
Kontonummer.: 51538098801
Bankleitzahl.: 12000

UID-Nummer.: ATU50232305
Steuernummer: 013/2811
Firmennummer: 199483 h

nemox.net
THE SOLUTION GROUP

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.

5) 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.

6) 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 E-Mails, 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, wobei das Justizministerium nur anonymisierte statistische Werte erhalten soll. Diese Protokolldaten sind jedoch doppelbödig: sie geben Namen und Anschrift der „suspekten“ Personen wieder, nämlich jener, die abgefragt wurden, jedoch einschließlich jener, die erfolglos, irrtümlich oder sonst „mitabgefragt“ wurden. Hierdurch entsteht das - kaum lösbare - Dilemma, dass die Protokollierung für den Rechtsschutz gleichzeitig den Grundrechtseingriff fortschreibt und eine weitere Gefahrenquelle darstellt. In diesem Zusammenhang ist erneut auf die mangelnde Unabhängigkeit der Datenschutzkommission hinzuweisen, ein Mangel, der auch durch die aktuelle DSG-Novelle nicht behoben wurde.

7) Fehlende öffentliche Diskussion der Grundrechtsfragen

Bedauerlich ist ferner, dass für das Begutachtungsverfahren die Weihnachtszeit gewählt wurde und derart erneut eine breite Diskussion der wichtigen Grundrechtsfragen vermieden wurde. Wie wichtig es ist, die Probleme und Risiken beim Namen zu nennen und die entsprechenden

nemox.net
Steiner und Würtenberger OEG
Eduard-Bodem-Gasse 9
A-6020 Innsbruck

Telefonnr.: +43 5 0234-0
Faxnr.: +43 5 0234-9
E-Mail: info@nemox.net

Bank Austria / Creditanstalt
Kontonummer.: 51538098801
Bankleitzahl.: 12000

UID-Nummer.: ATU50232305
Steuernummer: 013/2811
Firmennummer: 199483 h

nemox.net
THE SOLUTION GROUP

Debatten in einer informierten Öffentlichkeit zu führen, zeigt die Entscheidung des Rumänischen Verfassungsgerichts Nr. 1258 vom 08. Oktober 2009, das als erstes europäisches Verfassungsgericht die Vorratsdatenspeicherung an sich unter Verweis auf deren Menschenrechtswidrigkeit für verfassungswidrig erklärt hat.

8) Außerachtlassung legistischer Grundprinzipien

Das Vorblatt stellt lapidar fest, dass die Höhe der mit der Umsetzung des Gesetzesentwurfes verbundenen Kosten nicht vorhersehbar, mit einer Kostensteigerung jedoch zu rechnen sei. Die RL 2006/24/EG wurde am 15. März 2006 beschlossen, womit zum heutigen Zeitpunkt zumindest eine grobe Kostenschätzung vorliegen sollte, andernfalls § 14 Bundeshaushaltsgesetz (BHG) schlichtweg als politische Scheinbestimmung zu werten ist. Dies umso mehr, als der Gesetzesentwurf in § 94 Abs. 1 und 2 sowie § 99 Abs. 5 für die Anbieter und Betreiber von Telekommunikationsdiensten einen Ersatz der Investitionskosten, der Kosten der laufenden Mitwirkung und der Auskunftserteilung vorsieht. Dies legt nahe, dass die Kosten entweder nicht budgetiert werden können oder bewusst verschleiert werden.

In Anbetracht der durch die TKG-Novelle angeordneten massiven und dauerhaften Eingriffe in die Grundrechte fordern wir:

1. **Keine Vorratsdatenspeicherung in Österreich**
2. **Keine Vorratsdatenspeicherung in Europa**
3. **Österreich soll die Richtlinie zur Vorratsdatenspeicherung nicht umsetzen sondern bekämpfen**

Von dieser Stellungnahme wird eine Ausfertigung dem Präsidium des Nationalrates übermittelt.

Mit freundlichen Grüßen

nemox.net
info@nemox.net

Steiner

Rudolf E. Steiner
r.steiner@nemox.net