XXIII. GP.-NR
1006 /J
19. Juni 2007

ANFRAGE

der Abgeordneten Dr Gabriela Moser, Freundinnen und Freunde

an den Bundesminister für Verkehr, Innovation und Technologie

betreffend Speicherung von Telefon/Handy-, SMS- und E-Mail-Daten

Als Reaktion auf den geplanten, aber aufgedeckten Terroranschlag in London sollen unter dem Schlagwort "Vorratsdatenspeicherung" in Zukunft laut einer EU-Richtlinie alle per Telefon, Handy oder SMS zustande gekommenen Kommunikationsverbindungen sowie die kontaktierten Internetportale mindestens ein halbes Jahr (auf Vorrat) gespeichert werden. Damit wird es auch möglich, nachträglich die Kontakte einer Person oder eines Unternehmens zu analysieren und offen zu legen.

Am 21.2.2006 stimmte der Rat der Justiz- und Innenminister einem Richtlinienvorschlag über die Vorratsspeicherung von Daten zu, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden. Das Europäische Parlament hatte bereits am 14.12.2005 mehrheitlich seine Zustimmung gegeben. Erfasst werden Verkehrs- und Standortdaten einschließlich Teilnehmer- und Nutzerdaten, die im Rahmen von Telefonie, SMS und Internet-Protokollen erzeugt werden, wobei die Inhalte der Kommunikation nicht erfasst werden. Diese Daten müssen durch die Telekommunikationsunternehmen gespeichert werden.
Die Mitgliedstaaten haben bei Umsetzung der Richtlinie dafür zu sorgen, dass die genannten Datenkategorien für einen Zeitraum von mindestens sechs Monaten und nicht mehr als zwei Jahren ab dem Zeitpunkt der Kommunikation auf Vorrat gespeichert werden.
Für die Umsetzung der Richtlinie ist eine Frist von 18 bis 36 Monaten vorgesehen.

Die Österreichische Umsetzung der EU-Richtlinie sieht einen Zugriff auf die Daten bereits vor, wenn diese zur Verfolgung von „mit beträchtlicher Strafe bedrohten Handlungen" benötigt werden. Auch ist nicht sichergestellt, dass die Beauskunftung nur aufgrund einer schriftlichen gerichtlichen Anordnung erfolgen darf. Verbindungsdatenspeicherung ermöglicht es, soziale Netze automatisiert zu analysieren.
In der vorliegenden TKG-Novelle sollen auch die bisher von den Telekom-Gesellschaften nicht gespeicherten Notrufe, passiven Anrufe und nicht zu Stande gekommenen Verbindungen gespeichert werden.

Im Falle diffuser Bedrohungsbilder wie Terrorismus oder "organisierte Kriminalität" könnte damit flächendeckend das Kommunikationsverhalten aller BürgerInnen offengelegt und ausgeforscht werden.

Die Kritik an diesem Vorstoß umfasst mehrere zentrale Punkte:

1. Die Maßnahmen sind ineffizient und unverhältnismäßig
Die vorgeschlagenen Maßnahmen stehen nicht in einer angemessenen Zweck-Mittel-Relation, da sie weder geeignet noch erforderlich sind und eine unzumutbare Härte für die Betroffenen darstellen. TeilnehmerInnen aus dem Umfeld der Organisierten Kriminalität und des Terrorismus werden die Verfolgbarkeit ihrer Daten leicht zu verhindern wissen (anonyme Accounts, Pre-paid-mobiles, öffentliche Internet-Terminals, Ausweichen auf Provider außerhalb der EU, usw.). Von der Vorratsdatenspeicherung wären daher in erster Linie unbeteiligte BürgerInnen betroffen. Aufgrund der enormen Menge anfallender Daten ist ein effizientes Durchsuchen des Datenvorrats kaum möglich, die rasche Verfügbarkeit der angeforderten Daten ist somit nicht gegeben. Es würden riesige "Datenfriedhöfe" ohne signifikanten ermittlungstechnischen Wert entstehen. Darüber hinaus werden in der Praxis von den Strafverfolgungsbehörden ca. 85% der Daten innerhalb von 3 Monaten und ca. 95% der Daten innerhalb von 6 Monaten nach ihrer Entstehung angefordert.

2. Unklarheit betreffend die zu speichernden Datenarten
In der Richtlinie ist nicht ausreichend klar formuliert, welche Einzelheiten von Internet-Kommunikation gespeichert werden sollten. Dies betrifft va. Emails, was angesichts der Tatsache, dass der weltweite Email-Verkehr zu einem großen Teil aus SPAM besteht, eine nicht zielführende Maßnahme ist.

3. Keine Vereinbarkeit mit Artikel 8 der Europäischen Menschenrechtskonvention
Es ist überdies sehr wahrscheinlich, dass die Richtlinie in Widerspruch zu Artikel 8 EMRK (Recht auf Privatleben) steht. Die vorgesehene Verpflichtung zur routinemäßigen, flächendeckenden Vorratsspeicherung sämtlicher Verkehrs-, Nutzer- und Teilnehmerdaten würde die ausnahmsweise zulässige Überwachung zur evident unverhältnismäßigen Regel machen. Die Richtlinie betrifft nicht nur einzelne Personen, die auf Grund besonderer Gesetze überwacht werden, sondern alle BürgerInnen, die die elektronische Kommunikation nutzen. Dass eine so umfangreiche Speicherung von Verkehrsdaten der einzig gangbare Weg zur Bekämpfung der Kriminalität oder zur Wahrung der nationalen Sicherheit ist, dafür liefert die Richtlinie keine überzeugenden Argumente.

4. Keine Vereinbarkeit mit dem Grundrecht auf Datenschutz
Die österreichische Rechtslage spricht derzeit gegen eine Vorratsspeicherung von Telekommunikationsdaten. Nach dem Datenschutz-Gesetz wäre es unzulässig, diese auf Vorrat anzulegen, nur weil sie in Zukunft für die Strafverfolgung benötigt werden könnten. Die europäische Vorgabe macht die österreichischen Bestimmungen jedoch hinfällig. Dies gilt auch für die Verfassungsbestimmung des § 1 DSG 2000.

5. Unzumutbare Belastungen für die Telekommunikationsindustrie
Zusätzlich sind enorme Belastungen für die europäische Telekommunikationsindustrie, insbesondere für kleinere und mittlere Telekommunikationsunternehmen zu befürchten. Kosten erwachsen aus der Anpassung der Systemtechnik zur Generierung und Speicherung der Daten, der Anpassung der betrieblichen Abläufe zur sicheren Archivierung der Daten sowie der Bearbeitung und Auswertung von Anfragen der Sicherheitsbehörden.

Der erforderliche Investitionsaufwand im Bereich der klassischen leitungsvermittelten Telefonie liegt nach Schätzungen größerer Unternehmen innerhalb der Mitgliedstaaten bei 180 Mio. Euro im Jahr pro Unternehmen mit jährlichen Betriebskosten bis zu 50 Mio. Euro. Für kleinere und mittlere Unternehmen wäre daher der Geschäftsbetrieb gefährdet. Die Belastungen im Bereich des Internets würden den Investitionsaufwand bei der klassischen leitungsvermittelten Telefonie um ein Vielfaches übersteigen. Für diese Kosten werden am Ende immer die BürgerInnen aufkommen müssen, ohne allerdings einen signifikanten Sicherheitsgewinn zu genießen: Entweder über höhere Kosten für Telekommunikationsleistungen oder über vom Staat eingehobene Steuern.

Die Verfassung garantiert das Recht auf unbeobachtete elektronische Kommunikation (Kommunikationsgeheimnis), das auch das Recht umfasst, unbeobachtet seinen Kommunikationspartner auswählen zu dürfen. Eine offene, demokratische Gesellschaft lebt davon, dass Menschen unbeobachtet, unkommentiert und unzensuriert Ideen und Meinungen austauschen. Innovationen, neue Geschäftsideen, aber auch kreative Lösungen entstehen oft erst durch Diskussion naturgemäß unausgegorener, für Außenstehende zunächst oft missverständlicher Ideen.

Das Wissen der permanenten Beobachtung, die Gefahr ein bestimmtes Kommunikationsverhalten rechtfertigen zu müssen, schränkt die Bereitschaft zur offenen Kommunikation ein.

Wesentlicher Teil offener Kommunikation ist auch die freie Wahl seiner Gesprächspartner, sei es am Telefon oder Internet. Aus gutem Grund verbietet daher das Telekommunikationsgesetz die Speicherung von Verbindungsinformationen, also wer mit wem wie lange telefoniert hat. Nur bis Abschluss der Abrechnung dürfen Telefonanbieter diese Daten aufbewahren, dürfen sie aber nicht zu anderen Zwecken auswerten oder analysieren.

Kontakte sind heute, insbesondere in der Wirtschaft, die Triebfeder des Erfolgs. Zu wissen, wer welche Kunden hat, wer wem ein Angebot stellt und wer eventuell bei einem Mitbewerber Alternativofferte einholt, kann den Wettbewerb entscheidend beeinflussen. Aus der Frequenz, wie oft jemand welche Telefonnummer anruft, lässt sich leicht auf den Status des Betroffenen zurück schließen, Kunden werden den Kundendienst, Interessenten den Verkauf usw. anrufen. Diese Angaben reichen, um sich ein Bild über das wirtschaftliche Netzwerk eines Unternehmens zu machen. Plant der Inhaber den Unternehmensverkauf oder eine groß angelegte Kooperation wird dies aus den Telefonkontakten genauso erkennbar sein, wie Verlust oder Zustrom von Kunden.

Kritische BürgerInnen oder Beamte könnten nicht mehr unbeobachtet zur Aufdeckung von Missständen zB via Medien beitragen, Rechtsanwaltskanzleien müssten damit rechnen, dass Klientenlisten angelegt werden, Patienten müssten bei Anrufen rechnen, dass die Information, welchen Facharzt sie wie oft konsultiert haben, in falsche Hände gerät.

Speicherung wird zudem mit falschen Argumenten gerechtfertigt:

Vielfach wird behauptet, dass ja nur die Daten aufgehoben, nicht jedoch ausgewertet würden. Tatsache ist aber, dass ein nicht verwerteter Datenfriedhof keinen Sicherheitsgewinn brächte. Es müssten daher umfangreiche und teure Auswertungseinrichtungen angeschafft werden. Schon in der Vergangenheit zeigte sich regelmäßig, dass einmal aufgebaute Datenbestände auch für andere Zwecke genutzt werden. Wenn es keinen Terroranschlag gibt, könnte man doch damit sehr gut nach "organisiertem Verbrechen", Geldwäsche, Menschen- und Drogenhandel, Asylmissbrauch, Sozialhilfemissbrauch, Steuerhinterziehung, Verkehrsübertretungen, ... forschen. Je geringfügiger das Delikt, desto höher auch die „Erfolgs"chancen.

Bei diesen Auswertungen ist jedenfalls auch mit Zufallsfunden zu rechnen ("Das ist ja interessant, dass der Beamte XY 5mal die ABC-Nachrichtenredaktion angerufen hat"), die dann zu weiterer Überwachung motivieren.

Fest steht, schon um bei gezielten Überwachungen einen positiven Treffer (Täter) zu landen, müssen Daten von mehreren tausend unschuldigen Personen ausgewertet werden, bei der geplanten ziellosen Überwachung würde somit das Kommunikationsverhalten hunderttausender Personen offen gelegt.

Hinzu kommt, dass hohe Kosten zu erwarten sind:

In Österreich bestehen rund 12-14 Millionen Telefonanschlüsse, die etwa 20-40 Mrd. Telefonaten pro Jahr entsprechen, rund 40 Mrd. Mails werden jährlich verschickt bzw. empfangen. Zieht man die derzeit gültige Überwachungskostenverordnung (BGBl II 322/2004) heran, käme man bei flächendeckender Auswertung ("Gefahrenanalyse, Gefahrenabwehr und Gefahrenerforschung") rasch zu Beträgen von mehreren hundert Millionen bis einigen Milliarden Euro. Stehen doch den Telekomunternehmen Kostenersätze von 64,- Euro pro Telefonnummer für die Einrichtung und 6,50 Euro pro Tag und Nummer zu.

Wie hoch die gesamten Kosten tatsächlich wären, kann nicht endgültig festgestellt werden, da derzeit kein Kostenersatz für die Maildatenaufzeichnung (Absender und Empfänger eines Mails) festgelegt wurde. Derartige Aufzeichnungen passieren derzeit überhaupt nicht und müssten von den Internetprovidern erst neu eingerichtet werden. Nimmt man nur einen Kostenersatz von 1 Cent pro Datensatz an, wären das immerhin 200 bis 400 Millionen EUR pro Jahr.

Viel geringer werden die Kosten nicht sein können, da ja besondere Sicherheitsmaßnahmen getroffen werden müssten, die ein irrtümliches Löschen oder Überschreiben der Aufzeichnungen verhindern. Bisher führte der Verlust von Verbindungsdaten bloß dazu, dass bestimmte Telefonleistungen nicht abgerechnet werden konnten und die Telekomfirmen mussten daher die Datensicherheit nur so hoch ansetzten, wie das wirtschaftliche Ausfallsrisiko betrug. Es wäre unsinnig gewesen, mehr Sicherheitsmaßnahmen zu setzen, als durch den Erlös bei der Abrechnung der Verbindungsdaten zu erwarten gewesen wäre. Eine verpflichtende Vorratsdatenspeicherung würde jedoch lückenlose Aufzeichnung und damit wesentlich teurere Sicherheitsmaßnahmen bedingen.

Fest steht, dass diese viele hundert Millionen Euro teure Überwachung vom Bürger zu bezahlen sein wird. Ob als SteuerzahlerIn in Form von Rückvergütungen an die

Telefongesellschaften oder durch höhere Telefongebühren, ist offen. Vermutlich wird es Zweiteres sein, lassen sich doch auf diesem Weg die Kosten leichter verschleiern.

Sollte diese Form der Überwachung kommen, müssten jedoch Internetprovider und Telekomunternehmen den Überwachungskostenanteil auf ihren Rechnungen unbedingt transparent machen.

Überwachung ist durch Kriminelle leicht zu unterlaufen:

Trotz der geplanten Vorratsdatenspeicherung können Personen und Gruppen, die tatsächlich zum engeren Kern organisierter Kriminalität oder terroristischer Vereinigungen zählen, die Überwachungsmaßnahmen leicht unterlaufen. Sei es durch Nutzung anonymer Wertkartenhandys, die Zusatzkosten von 10 Cent statt 1 Cent pro Minute werden wohl in Kauf genommen werden. Im Internet wird Verschlüsselung benutzt werden oder es wird schlicht mit kodierten Nachrichten gearbeitet. Schon ein Mailaccount auf einem Server außerhalb von USA und EU verhindert, dass die Mailkommunikation überwacht wird. Vielen Internetbenutzern ist weiters nicht bewusst, dass schon heute ein beträchtlicher Teil des Mailverkehrs nicht über Provider-Mailserver läuft, sondern zwischen den Servern verschlüsselt wird und daher gar nicht aufgezeichnet werden kann.

Fazit:
BürgerInnen, die nichts zu verbergen haben, daher ihre Telefon- und Interneteinrichtungen korrekt angemeldet haben, stünden dennoch im Visier der Überwacher. Netzwerke von Querdenkenden und der Opposition könnten dann aufgedeckt werden.
Fälle von Verbindungsdatenmissbrauch in Italien haben gezeigt, wie schwach die Überwacher selbst kontrolliert würden. Außerdem besteht die Möglichkeit, dass die Daten manipuliert werden.

Die Vorratsdatenspeicherung gilt ansonsten als eine sicherheitspolitische Sackgasse.
Vor allem aber: Die von Seiten der EU geplante Permanentüberwachung von Telefonverbindungen, eMail und SMS steht in Konflikt mit Grundfreiheiten.

Auch nach Ihren jüngsten Äußerungen und schriftlichen Festlegungen bleiben hier einige Frage offen.

Die unterfertigten Abgeordneten stellen daher folgende

ANFRAGE:

1. Warum wurde seitens der Bundesregierung bis jetzt nicht beim Europäischen Gerichtshof gegen die EU-RL über die Vorratsdatenspeicherung wegen Kompetenzüberschreitung geklagt, wie es seitens einzelner anderer Mitgliedsstaaten bereits erfolgte?

2. Warum wird nicht zumindest der Ausgang der in dieser Sache bereits laufenden Klagen abgewartet?

3. Haben Sie oder Ihre RegierungskollegInnen in dieser Sache bereits anderweitige Aktivitäten auf EU-Ebene gesetzt, um zB eine Änderung der Richtlinie zu erreichen (nachdem Sie diese kürzlich in einer parl. Anfragebeantwortung als „nicht vollkommen unberechtigt" ansehen, somit aber wohl als weitgehend unberechtigt)? Wenn nein, warum nicht?

4. Werden Sie oder Ihre RegierungskollegInnen in dieser Sache anderweitige Aktivitäten auf EU-Ebene setzen, um zB eine Änderung der Richtlinie zu erreichen? Wenn nein, warum nicht?

5. In welcher Form, durch welche Ausnutzung nationaler Spielräume werden Sie bei einer etwaigen Umsetzung der EU-RL in der vorliegenden Form den Datenschutz gewährleisten?

6. In welcher Form, durch welche Ausnutzung nationaler Spielräume werden Sie bei einer etwaigen Umsetzung der EU-RL in der vorliegenden Form den Schutz der Grundrechte gewährleisten?

7. Zu welchem Ergebnis sind Sie bei der nochmaligen Evaluierung der Frage der Speicherung von Daten erfolgloser Anrufsversuche?

8. In welcher Höhe werden sich die Kosten für die Vorratsdatenspeicherung bewegen?

9. Wer soll die Kosten für die Vorratsdatenspeicherung konkret auf welchem Weg tragen, insbesondere a) soll die Überwachungskostenverordnung unverändert bleiben, b) sollen die Investitionskosten von jemand anderem als vom Staat bezahlt werden?

10. Wie wollen Sie im einzelnen die zahlreichen Umgehungsmöglichkeiten (wie etwa Telefonzellen, Internet-Cafes, die Nutzung von Anonymisierungsdiensten, die Wahl von Diensteanbietern außerhalb der EU, die Nutzung von nichtgewerblichen Dienstleistern, ... - siehe auch die Anfragebegründung) unterbinden?

11. Falls Sie diese Umgehungsmöglichkeiten nicht unterbinden wollen (oder können) – warum wollen Sie dennoch eine in vielerlei Hinsicht problematische Vorratsdatenspeicherung per Gesetz einführen, obwohl diese in vielerlei Hinsicht umgehbar und damit mit an Sicherheit grenzender Wahrscheinlichkeit weitgehend wirkungslos sein wird?

12. Inwieweit werden Tochterunternehmen österreichischer Unternehmen, die von außerhalb der EU aus operieren – zB Liechtenstein – von der von Ihnen geplanten Form der Richtlinienumsetzung erfasst werden?

13. Welchen Zeitplan sehen Sie für die Überarbeitung des Begutachtungsentwurfs und das eventuelle weitere Prozedere vor?

14. Wann werden Sie die Ihren Aussage zufolge ebenfalls bereits in Vorbereitung befindliche Richtlinienumsetzung im Internet-Bereich in die Begutachtung schicken?

15. Ist Ihnen bekannt, dass seitens Ihres Hauses bzw. infolge der Beteiligung Ihres Hauses in den letzten Jahren wiederholt EU-Richtlinien grob verspätet umgesetzt wurden, so etwa im Eisenbahnbereich oder auch bei der Einführung der SUP („Strategischen Prüfung Verkehr"), und wird dieser offensichtlich gegebene Spielraum auch bei dieser politisch und gesellschaftlich viel kontroversielleren EU-Umsetzung erneut genutzt werden, wenn nein, warum nicht?

16. Was haben Sie konkret gegenüber der EU-Kommission, zB bei Ihrem jüngsten Treffen im Rahmen des Verkehrsministerrates, im Hinblick auf eine spätere Umsetzung a) unternommen , b) erreicht?

17. Welche Schritte haben Sie gegenüber dem Bundesminister für Inneres gesetzt, der im Gegensatz zu Ihnen (als zuständigem Minister) und zu einer in der Begutachtung des Entwurfs manifest gewordenen großen Gruppe an Betroffenen vehement für eine Übererfüllung der EU-Richtlinie, also für noch weitergehende Vorratsdatenspeicherung mit noch weitreichenderen datenschutzrechtlichen und Freiheits-Eingriffen, eintritt?

18. Warum haben Sie einen Entwurf für eine TKG-Novelle zur Vorratsdatenspeicherung in Begutachtung geschickt, von dem Sie sich hernach über den Weg der Medien distanziert haben?