Österreichischer Rechtsanwaltskammertag | Die österreichischen Rechtsanwälte

Bundesministerium für Verkehr
Innovation und Technologie

Ghegastraße 1
1030 Wien
opfb@bmvit.gv.at

Zl. 13/1 07/119

GZ 630.333/0001-III/PT2/2007
BG, mit dem das Telekommunikationsgesetz 2003 - TKG 2003 geändert wird (Anm: Vorratsdatenspeicherung)

Referent: Mag. Georg Bürstmayr, Rechtsanwalt in Wien

Sehr geehrte Damen und Herren!

Der Österreichische Rechtsanwaltskammertag erstattet zu dem oben angeführten Gesetzesentwurf folgende

S t e l l u n g n a h m e :

A. Vorbemerkung:

Der vorliegende Entwurf zur TKG – Novelle bricht in Umsetzung der Richtlinie 2006/24/EG mit der unseren Rechtsstaat prägenden Tradition, in die (grund)rechtlich geschützten Positionen des Einzelnen zu Strafverfolgszwecken nur bei Vorliegen entsprechender Verdachtsmomente einzugreifen.

Nach dem Entwurf sollen die im Zuge eines Kommunikationsdienstes erzeugten oder verarbeiteten Verkehrs- und Standortdaten aller ÖsterreicherInnen ohne Unterschied, verdachtsunabhängig und flächendeckend auf Vorrat gespeichert werden. Eine solche Maßnahme stellt zweifelsohne einen Eingriff in das Recht auf Achtung der Privatsphäre aber auch der Korrespondenz („Briefverkehr“) wie es in Art. 8 EMRK zum Ausdruck kommt dar.

Die so erfassten Daten können im Vergleich zu Inhaltsdaten (also etwa dem aufgezeichneten Inhalt eines Gesprächs) computerunterstützt ungleich effizienter, im größerem Umfang und kürzerer Zeit ausgewertet werden. Darüber hinaus können mit Hilfe dieser Daten aber auch soziale Netzwerke bis ins letzte Detail nachvollzogen und – je nach Telefonierverhalten – mehr oder weniger genaue Bewegungsprofile jedes(r) Österreichers/In erstellt werden. Diesem massiven Eingriff in das Grundrecht auf Achtung der Privatsphäre und der Korrespondenz steht ein nur sehr bescheidener Gewinn für Zwecke der Strafverfolgung gegenüber. Schon jeder

Tuchlauben 12 | A-1010 Wien | Tel. +43 (1) 535 12 75 | Fax +43 (1) 535 12 75-13 | rechtsanwaelte@oerak.at | www.rechtsanwaelte.at

technische Laie kann mit einfachsten Mitteln der Erfassung von auf ihn/sie rückführbaren Daten entgehen. So genügt die Inanspruchnahme eines außereuropäischen – und somit an den Regelungsgehalt der Richtlinie nicht gebundenen – Emailproviders oder etwa die Verwendung von Wertkartenhandys und Telefonzellen. Es ist davon auszugehen, dass kriminelle Vereinigungen und Terroristen, zu deren Bekämpfung die Richtlinie ja in erster Linie beschlossen wurde, über ungleich bessere technische Möglichkeiten und auch entsprechendes Wissen verfügen. Falls jemand also der Erfassung von auf seine/ihre Person rückführbarer Daten entgehen will, wird dies ihm/ihr ohne weiteres möglich sein. Voraussichtlich erfasst werden somit aber die Daten jener Personen, die entweder keine Kenntnis von der Vorratsdatenspeicherung haben oder kein Interesse an den Tag legen, derselben zu entgehen, also die Daten ganz normaler „Durchschnittsbürger".

Da - wie dargelegt - einem massiven Eingriff in die durch Art. 8 EMRK geschützten Positionen ein nur sehr bescheidener Mehrwert für Zwecke der Strafverfolgung gegenübersteht, stellt sich die Frage, ob die Vorratsspeicherung der Verkehrs- und Standortdaten aller Österreicher/Innen nicht unverhältnismäßig ist und somit eine Verletzung dieses Artikels darstellt.

Zudem bedeutet die gänzliche Überwälzung der Kosten der Vorratsspeicherung auf die Anbieter/Betreiber (und letztendlich wohl auf den Konsumenten), einen Eingriff in deren Recht auf Achtung des Eigentums wie es in Art. 1 des 1. ZP zur EMRK zum Ausdruck kommt. Auch ein solcher bedarf selbstverständlich einer Rechtfertigung.

Es ist davon auszugehen, dass die Vorratsspeicherung früher oder später der nachprüfenden Kontrolle nicht nur des Verfassungsgerichtshofs, der natürlich den Vorrang des Gemeinschaftsrechtes zu beachten hätte, und – über den Weg eines Vorabentscheidungsverfahrens – des EuGH, sondern auch jener des Europäischen Gerichtshofs für Menschenrechte unterzogen wird, wobei fraglich ist, ob die auf europäischer Ebene beschlossenen Maßnahme dieser Kontrolle standhalten wird.

Daher wird im Sinne einer eingriffsminimierenden Vorgangsweise und zur Vermeidung frustrierter Aufwendungen empfohlen, die Richtlinie nur im unbedingt erforderlichen Ausmaß umzusetzen.

B. Zum Entwurf

1. Grundsätzliches:

Die anwaltliche Kommunikation ist bislang zu Recht in besonderer Weise geschützt.

In diesem Sinne ist auch die Überwachungsmöglichkeit eines auf einen Rechtsanwalt lautenden Teilnehmeranschlusses nur unter sehr eingeschränkten Bedingungen zulässig. Ein solcher darf nämlich nur dann überwacht werden, wenn der Rechtsanwalt selbst (!) der Tat, derentwegen die konkrete Überwachung erfolgen soll, *„ dringend verdächtig"* ist. (§ 149a Abs. 3 Z 2 StPO)

Der vorliegenden Entwurf sieht dagegen eine flächendeckende, verdachts*unabhängige* Vorratsspeicherung der Verkehrs- und Standortdaten und

Tuchlauben 12 | A-1010 Wien | Tel. +43 (1) 535 12 75 | Fax +43 (1) 535 12 75-13 | rechtsanwaelte@oerak.at | www.rechtsanwaelte.at

somit Überwachung zum Zwecke der Strafverfolgung iwS aller Teilnehmer an elektronischen Kommunikationsvorgängen ohne Unterschied vor. Die Tatsache, dass somit (auch) die Anschlüsse von Rechtsanwälten ohne das Vorliegen eines entsprechenden Verdachts überwacht werden, bedeutet das (partielle) Ende des oben angesprochenen besonderen Schutzes der anwaltlichen Kommunikation. Daran vermag auch der Umstand, dass eine Abfrage der Daten hinsichtlich dieser Anschlüssen an strengere Voraussetzungen gebunden bleibt, nichts zu ändern, da ja schon das Erfassen und Speichern der Daten zu Strafverfolgungszwecken für sich genommen jedenfalls eine Überwachungsmaßnahme darstellt.

Wohl wurden auch bisher Verbindungsdaten in eingeschränktem Umfang gespeichert. Während diese aber, sobald sie insbesondere für die Bereitstellung des Services und die Abrechung nicht mehr erforderlich waren, grundsätzlich gelöscht werden müssen/mussten, wird nun diese (in grundrechtlicher Hinsicht eingriffsminimierende und auch das besondere Schutzbedürfnis der anwaltlichen Kommunikation wahrende) Löschungsverpflichtung in eine Speicherungspflicht verkehrt.

Dies ist keineswegs europarechtlich zwingend, eine andere Form der Umsetzung fände durchaus Deckung in der Textierung der Richtlinie. Art. 5 Abs. 2 ordnet ausdrücklich an, dass keinerlei Daten auf Vorrat gespeichert werden dürfen, die *„die Aufschluss über den Inhalt einer Kommunikation geben“.* In vielen Fällen, so auch bei einer telefonischen Kontaktaufnahme mit einer Anwaltskanzlei, wird aber aus den Verkehrsdaten auf den Inhalt rückgeschlossen werden können. So wird ein Anruf in einer Anwaltskanzlei häufig, wenn nicht regelmäßig eine anwaltliche Konsultation zum Inhalt haben. Gleiches gilt selbstverständlich für andere Berufe, aber auch Service- und Beratungsangebote, wie etwa ein Anruf bei der „Aidshilfe“, der „Aktion Leben“ oder etwa bei „Rat auf Draht“. Solche Telefonate werden in aller Regel eine entsprechende Beratung oder Hilfestellung zum Inhalt haben.

Dass der Rückschluss auf den Inhalt nicht zwingend inhaltlich „richtig“ sein muss, vermag an dem Umstand nichts zu ändern, dass diese Daten, Aufschluss über den (höchstwahrscheinlichen) Inhalt der Kommunikation geben. Die vom Richtliniengeber gewählte Formulierung (*„… Aufschluss über den Inhalt einer Kommunikation …“)* weist in auffallender Weise Parallelen zu Art. 8 Abs. 1 der Richtlinie 95/46/EG auf. Dieser Bestimmung zu Folge dürfen Daten, *„aus denen die rassische und ethnische Herkunft, politische Meinungen (...) hervorgehen sowie (...) Daten über die Gesundheit oder Sexualleben“* (sog. sensible Daten) grundsätzlich nicht verarbeitet werden. Für die „Sensibilität“ eines Datum ist es nun keinesfalls erforderlich, dass das sensible Faktum, also etwa die ethnische Herkunft oder die politische Meinung, selbst Gegenstand des Datums ist, sondern es genügt, wenn auf dieses rückgeschlossen werden kann. Als Beispiel sei auf die Mitgliedschaft bei einer Vereinigung, der die Nähe zu einer Partei nachgesagt wird, verwiesen. Das Datum „Mitgliedschaft“ bei dieser Vereinigung wäre ein sensibles, obgleich die „politische Meinung“, also das die Sensibilität begründende Faktum, nicht selbst Gegenstand des Datums ist, sondern aus der Mitgliedschaft auf diese rückgeschlossen würde. Ähnlich verhält es sich mit dem Datum "Besuch beim Lungenfacharzt". Dieses Datum wird als sensibles angesehen, obwohl es sich ja auch um einen Freundschaftsbesuch „bei Kaffee und Kuchen“ handeln könnte. In beiden Fällen ist

Tuchlauben 12 | A-1010 Wien | Tel. +43 (1) 535 12 75 | Fax +43 (1) 535 12 75-13 | rechtsanwaelte@oerak.at | www.rechtsanwaelte.at

also das die Sensibilität begründende Faktum nicht selbst Inhalt des Datums, sondern kann mit einiger Wahrscheinlichkeit auf dieses rückgeschlossen werden.

Da die anwaltliche Kommunikation in besonderer Weise zu schützen ist und die im Rahmen der Vorratsspeicherung hinsichtlich der Kommunikation von und mit Rechtsanwälten zu erfassenden Verkehrsdaten – wie es in Art. 5 Abs. 2 der Richtlinie heißt – „*Aufschluss über den Inhalt einer Kommunikation geben*“ würden, sollten diese Daten nicht erfasst und eine entsprechende Ausnahmeregelung in den Gesetzesentwurf aufgenommen werden.

Es wird daher angeregt, die derzeit geltende Regelung in Ansehung von Rechtsanwälten beizubehalten.

2. Ausführungen zu einzelnen Punkten des Entwurfs:

Zu Z 5 des Entwurfs:
Wie dargelegt, sollte die Richtlinie vom Ziel der Eingriffsminimierung in grundrechtlich geschützte Positionen und der Vermeidung letztendlich möglicherweise frustrierter Aufwendungen getragen nur im unbedingt erforderlichen Mindestausmaß umgesetzt werden.

Österreich hat von der in Art. 15 der Richtlinie vorgesehenen Möglichkeit, die Anwendung derselben auf die Speicherung von Kommunikationsdaten betreffend Internetzugang, Internet-Telefonie und Internet-Email bis zum 15.März 2009 aufzuschieben, Gebrauch gemacht. Nicht nachvollziehbar ist daher, weshalb der vorliegende Entwurf bereits die Erfassung dieser Daten in Teilbereichen vorsieht.

Zu Z 7 des Entwurfs:
Nicht nur die Erfassung und Speicherung der Vorratsdaten greift in grundrechtlich geschützte Positionen ein, sondern auch die Übermittlung an Behörden bedeutet einen Grundrechtseingriff, der selbstverständlich einer Rechtfertigung bedarf. Nun sieht der Entwurf im neu gefassten § 102a vor, dass die Vorratsdaten *„zum Zwecke der Ermittlung, Feststellung und Verfolgung von mit beträchtlicher Strafe bedrohten Handlungen (§ 17 SPG), einschließlich der Tatbestände der §§ 107 und 107a StGB“* zu speichern sind. Ein Datenzugriff bei bloßem Vorliegen der Voraussetzungen des 17 SPG (gerichtlich strafbare Handlungen, die mit mehr als einjähriger Freiheitsstrafe bedroht sind) erscheint zum einen unverhältnismäßig, sodass die Rechtfertigung eines solchen Grundrechtseingriffs wohl nur schwer zu argumentieren sein wird. Zum anderen ist die hier übernommene Definition der „schweren Straftaten“ auch mit der ratio der Richtlinie schlicht unvereinbar. Wie nicht nur dem Werdegang der Richtlinie, sondern auch der Textierung der Richtlinie (Erwägungsgründe 7, 8, 9, und 10) zu entnehmen ist, wird die Notwendigkeit und somit der Zweck der Vorratspeicherung wiederholt mit der Bekämpfung organisierten Kriminalität und des internationalen Terrorismus argumentiert. **Die im vorliegenden Entwurf gewählte Vorgangsweise (auch wenn sie dem Wunsch des Rates entsprechen sollte) ist als richtlinienwidrig und unverhältnismäßig abzulehnen.**

Tuchlauben 12 | A-1010 Wien | Tel. +43 (1) 535 12 75 | Fax +43 (1) 535 12 75-13 | rechtsanwaelte@oerak.at | www.rechtsanwaelte.at

Es wird daher vorgeschlagen, die Z7 des Entwurfs wesentlich enger zu fassen, indem beispielsweise an Stelle der Wendung „(§ 17 SPG)“ die Wendung „(§ 17 Abs 1 StGB)“ gesetzt wird.

Zudem sollte die über den Speicherungszweck wohl beabsichtigte Zugriffbeschränkung aus gesetzessystematischer Sicht auch expressis verbis als solche in den Gesetzestext aufgenommen werden, sodass klargestellt wird, dass ein Zugriff auf die Vorratsdaten ausschließlich zum Zwecke der Ermittlung, Feststellung und Verfolgung oben umschriebener Straftaten und nur unter den vorgesehen Voraussetzungen (so insb. nur über gerichtliche Anordnung oder Bewilligung), rechtmäßig ist. Auf diese Weise sollte sichergestellt werden, dass auf die Vorratsdaten nicht zu anderen Zwecken oder zur Verfolgung anderer (mit geringerer Strafe bedrohte) Straftaten zugegriffen wird. In diesem Sinne sollte auch jede Datenzugriffs- oder Datenverwertungsmöglichkeit durch Dritte (auch durch die Telekommunikationsanbieter und –betreiber) ausdrücklich ausgeschlossen werden.

Wien, am 29. Mai 2007

DER ÖSTERREICHISCHE RECHTSANWALTSKAMMERTAG

Dr. Gerhard Benn-Ibler
Präsident

Tuchlauben 12 | A-1010 Wien | Tel. +43 (1) 535 12 75 | Fax +43 (1) 535 12 75-13 | rechtsanwaelte@oerak.at | www.rechtsanwaelte.at