

Bundesministerium für Verkehr, Innovation und Technologie
Abteilung III/PT2 (Recht)
Ghegastraße 1
1030 Wien

BMVIT-630.333/0001-III/PT2/2009
Entwurf eines Bundesgesetzes, mit dem das
Telekommunikationsgesetz 2003 (TKG 2003) geändert wird;
Begutachtungsverfahren

Wien, am 15.1.2010
GZ: 762/09; smp

Sehr geehrte Damen und Herren!

Mit Schreiben vom 20. November 2009, bei der Österreichischen Notariatskammer am 24. November 2009 eingelangt, hat das Bundesministerium für Verkehr, Innovation und Technologie den Entwurf eines Bundesgesetzes, mit dem das Telekommunikationsgesetz 2003 (TKG 2003) geändert wird (Umsetzung der Richtlinie 2006/24/EG über die Vorratsdatenspeicherung), übersendet und ersucht, dazu bis 15. Jänner 2010 eine Stellungnahme abzugeben.

Die Österreichische Notariatskammer bedankt sich für die Möglichkeit einer Äußerung zum vorliegenden Entwurf und erlaubt sich, nachstehende

Stellungnahme

abzugeben:

I. Umsetzung der Richtlinie?

Das **deutsche Bundesverfassungsgericht** verhandelt derzeit eine Beschwerde von 35.000 Privatpersonen gegen die Umsetzung der Richtlinie 2006/24/EG über die Vorratsdatenspeicherung. Das **rumänische Verfassungsgericht** hat die Umsetzung wegen Verstoßes gegen Art 8 EMRK (Privatsphäre) untersagt. Jedenfalls im Fall Rumäniens wird der EuGH zu entscheiden haben. Im Fall Deutschland wird entweder der EuGH tätig werden (bei Vorlage des BVerfG an den EuGH oder Ablehnung der Vorratsdatenspeicherung durch das BVerfG) oder – bei Bestätigung der Grundrechtskonformität durch das BVerfG – von den Beschwerdeführern der EGMR in Straßburg angerufen



werden¹⁾). Die Argumente sind bekannt: Kritisiert wird unter anderem, dass Kriminelle, die Wertkartentelefone, Telefonzellen, E-Mail-Accounts in Internet-Cafés oder Drittstaaten benützen, mit der Vorratsdatenspeicherung praktisch nicht überwacht werden können, sodass die Richtlinie für den eigentlich angestrebten Zweck weitgehend nutzlos und damit als Grundrechtseingriff unverhältnismäßig ist.

Der **Umsetzungsverzug Österreichs** ist angesichts dieser Ausgangslage nicht zu kritisieren. Österreich befindet sich dabei in Gesellschaft mehrerer anderer Mitgliedstaaten. Die erste Empfehlung geht daher dahin, die Richtlinie **bis zur Entscheidung in den Fällen Deutschland und Rumänien** überhaupt nicht umzusetzen. Staaten im Umsetzungsverzug (einschließlich Österreichs) sind allerdings derzeit mit Vertragsverletzungsverfahren der EU konfrontiert.

II. Grundrechtliche Rechtfertigung durch Verfolgung „schwerer Straftaten“?

Eingriffe staatlicher Behörden in die Telekommunikation des Einzelnen müssen stets im Hinblick auf ihre grundrechtliche Rechtfertigung – insbesondere auf ihre Verhältnismäßigkeit – geprüft werden. Dass der Diensteanbieter als verlängerter Arm staatlicher Gewalt angesehen werden muss, kann nicht geleugnet werden. Der ursprünglich privatrechtlich auftretende Diensteanbieter wird durch die Verpflichtung zur Datenspeicherung im Auftrag staatlicher Strafverfolgung tätig und ist insoweit dem Staat zuzurechnen. Daher sind die ihm auferlegten Handlungspflichten auf ihre grundrechtliche Zulässigkeit zu prüfen.

Im Zusammenhang mit der Vorratsdatenspeicherung kommen als potentiell beeinträchtigte Grundrechte die Achtung des Privat- und Familienlebens (Art 8 Abs 1 EMRK), der Schutz des Fernmeldegeheimnisses (Art 10a StGG) und das Grundrecht auf Datenschutz (§ 1 DSGVO) in Betracht. Eine gesteigerte Bereitschaft, diese Grundrechte unter dem Deckmantel der Terrorismusbekämpfung entschieden einzuschränken, darf – wie der **EGMR** ausgesprochen hat²⁾ – keinesfalls eine kritische Betrachtung und die Einführung wirksamer Garantien gegen Missbrauch verhindern.

Zunächst ist festzustellen, dass bereits die Sammlung und Speicherung der Daten einen Eingriff in die genannten Grundrechte darstellt³⁾. Der Eingriff erfolgt nicht nur im Einzelfall, sondern wird flächendeckend verdachtsunabhängig angeordnet. Auch deshalb ist eine Prüfung der **Verhältnismäßigkeit** unumgänglich.

Als rechtfertigender Zweck findet sich in § 102a Abs 1 (Speicherung) und § 102b Abs 1 (Auskunftspflicht) des Entwurfs die „Ermittlung, Feststellung und Verfolgung schwerer Straftaten“. Dies wird aus Art 1 der Richtlinie 2006/24/EG übernommen, allerdings ohne die dort geforderte nähere Präzisierung durch den jeweiligen Mitgliedstaat. Damit bleibt offen, was der Entwurf unter „**schweren Straftaten**“ versteht. Eine klare Definition der in Betracht kommenden Delikte ist dringend erforderlich

¹⁾ Die Presse vom 13.12.2009 („Datenspeicherung: Ausstieg möglich?“).

²⁾ EGMR 29.6.2006 Weber und Saravia gg. Deutschland, Appl Nr 54934/00 Z 106.

³⁾ *Reindl-Krauskopf*, „Data Retention: Sicherheit versus Freiheit“ in „Goodbye Privacy – Grundrechte in der digitalen Welt“ (2008) 67.

und soll offenbar noch durch das BMJ „nachgeliefert“ werden⁴⁾. Sofern Österreich in der Umsetzung hier weiter geht, als die Richtlinie zwingend vorschreibt, ist das Gesetz an der österreichischen Verfassung zu messen. Dies gilt gerade auch für die Frage, bei welchen Straftaten die Daten für Ermittlungszwecke verwendet werden dürfen. Verlangt man im österreichischen Recht die Herausgabe der Daten bei Bagatelldelikten, wie zB Urheberrechtsverstößen, dann wäre dies grundrechtswidrig; der VfGH müsste das Gesetz dann aufheben⁵⁾. Der derzeitige Stand des Entwurfes, den zentralen Begriff der „schweren Straftaten“ nicht verfassungswidrig, dafür aber überhaupt nicht zu definieren, ist nicht zu empfehlen.

In den Erwägungsgründen 7–10 wird als zentrale Zielsetzung der Richtlinie die Bekämpfung von **Terrorismus und organisierter Kriminalität** erkennbar. Daraus lässt sich für die Auslegung des Entwurfes ableiten, dass diese Bereiche unter den Tatbestand der „schweren Straftat“ fallen müssen.

Fest steht damit umgekehrt auch, dass die Einbeziehung niederschwelliger Delikte keine Deckung in der gemeinschaftsrechtlichen Vorgabe findet.

Zwischen der jedenfalls richtliniengegenständlichen Terrorismusbekämpfung und jedenfalls *nicht* richtliniengegenständlichen Bagatelldelikten besteht freilich eine Grauzone.

Eine Mindeststrafdrohung von einem Jahr Freiheitsstrafe wäre als Grenze jedenfalls zu niedrig angesetzt. Sie würde zB auch schwere Eingriffe in das Fischereirecht (§ 138 StGB), üble Nachrede in einem Druckwerk (§ 111 Abs 3 StGB), gewerbsmäßige Urheberrechtsverstöße (§ 91 Abs 2a UrhG) etc erfassen. Mit der Zielsetzung der Richtlinie (Bekämpfung von Terrorismus und organisiertem Verbrechen) hätte dies definitiv nichts zu tun.

Selbst die Übernahme der Zweiteilung der Delikte in Verbrechen und Vergehen (§ 17 StGB) und eine Anwendung der Vorratsdatenspeicherung ausschließlich auf Verbrechen (vorsätzliche Straftaten, die mit mehr als dreijähriger Freiheitsstrafe bedroht sind) erscheint bei Bedachtnahme auf die Motivation der Richtlinie als zu weit gefasst. Für bloße Vergehen scheidet eine Anwendung dann ohnehin aus. Aber auch innerhalb der Verbrechen muss eine klare Grenze gezogen und die Gefahr einer Zweckentfremdung der Vorratsdatenspeicherung für andere als die ursprünglich verfolgten Interessen verhindert werden.

Als beachtliche Delikte können jedenfalls §§ 278a (kriminelle Organisation), 278b (terroristische Vereinigung) und 278d StGB (Terrorismusfinanzierung) ins Zentrum gerückt werden, hiervon inhaltlich weit entfernte Delikte sollten aus dem Anwendungsbereich herausfallen.

Ein Verständnis des Begriffes der „schweren Straftat“ im Sinne des § 100a iVm § 100g der deutschen StPO ginge für die österreichische Rechtsordnung zu weit. Wenn dort eine Überwachung der Telekommunikation bereits bei Abgeordnetenbestechung, Betrug oder Steuerhinterziehung angeordnet wird, muss bezweifelt werden, dass diese Delikte als ähnlich schwere Straftaten wie

⁴⁾ Die Presse 13.12.2009 („Auf der Suche nach der schweren Straftat“).

⁵⁾ Berka, Die Presse vom 13.12.2009 („Datenspeicherung: Ausstieg möglich?“).

Terrorismus und organisierte Kriminalität qualifiziert werden können. Eine Orientierung an der deutschen Umsetzung ist daher nicht zu empfehlen, wenn eine Zweckentfremdung der Vorratsdatenspeicherung verhindert werden soll.

III. Speicherfrist

Nach Art 6 der Richtlinie haben die Mitgliedstaaten dafür zu sorgen, dass die in Art 5 angegebenen Datenkategorien für einen Zeitraum von mindestens sechs Monaten und höchstens zwei Jahren ab dem Zeitpunkt der Kommunikation auf Vorrat gespeichert werden.

§ 102a Abs 1 des Entwurfs bestimmt in Ausführung dieser Richtlinienvorgabe, dass die Daten ab dem Zeitpunkt der Erzeugung oder Verarbeitung bis **sechs Monate** nach Beendigung der Kommunikation zu speichern sind. Die Festlegung der kürzest möglichen Speicherfrist ist im Hinblick auf die Intensität des Grundrechtseingriffs durch die Vorratsdatenspeicherung und unter der Berücksichtigung der Tatsache, dass die von den Strafbehörden nachgefragten Daten größtenteils nicht älter als sechs Monate sind, zu begrüßen.

Nach Ablauf der Speicherfrist sind die Daten unbeschadet des § 99 Abs 2 TKG unverzüglich, spätestens jedoch einen Monat nach Ablauf der Speicherfrist, zu löschen (§ 102a Abs 8 des Entwurfs). Nach Art 7 lit d der Richtlinie sind die Daten jedoch (mit Ausnahme jener Daten, die abgerufen und gesichert worden sind) am Ende der Vorratsspeicherungsfrist, also **nach genau 6 Monaten**, zu vernichten. Insoweit geht der Entwurf über die Vorgaben der Richtlinie hinaus, weil im Ergebnis eine Speicherung der Daten für einen Zeitraum von bis zu 7 Monaten ermöglicht wird. Zum einen widerspricht eine Speicherung der Daten über die Speicherfrist hinaus Art 7 lit d der Richtlinie, zum anderen lässt der Entwurf offen, was im siebenten Monat – abgesehen vom Auskunftsverbot (§ 102a Abs 8) – mit den Daten geschehen soll.

IV. Ausnahmen von der Speicherpflicht

Nach Art 1 Abs 2 bezieht sich die Richtlinie nur auf Verkehrs- und Standortdaten, nicht aber auf Inhaltsdaten. Dementsprechend sind unter „Daten“ im Sinne der Richtlinie nur Verkehrsdaten und Standortdaten sowie alle damit in Zusammenhang stehenden Daten zu verstehen, die zur Feststellung des Teilnehmers oder Benutzers erforderlich sind (Art 2 Abs 2 lit a). Von der Vorratsdatenspeicherung sind solche „Daten“ (also Verkehrs- und Standortdaten) ausgenommen, sofern sie **Aufschluss über den Inhalt einer Kommunikation** geben (Art 5 Abs 2 der Richtlinie).

§ 102a Abs 7 des Entwurfs stellt klar, dass der Inhalt der Kommunikation und insbesondere Daten über im Internet aufgerufene Adressen auf Grund dieser Vorschrift nicht gespeichert werden dürfen (hier wird § 113a Abs 8 des deutschen TKG übernommen). Dadurch werden aber nicht Verkehrsdaten, die Aufschluss über den Inhalt einer Kommunikation geben, sondern Inhaltsdaten ausgenommen (vgl EB zu § 102a Abs 7 des Entwurfs).

In den EB wird festgehalten, dass häufig keine klare Trennung zwischen Verkehrsdaten und jenen Daten, die Aufschluss über den Inhalt einer Kommunikation geben, möglich ist. Weiters wird festgestellt, dass „bloße“ Verkehrsdaten über eine inhaltliche Aussagekraft verfügen können, mitunter sogar Aufschluss über den Inhalt einer Kommunikation geben können. Auch auf die Parallele zu Art 8 Abs 1 der Datenschutzrichtlinie⁶⁾, wonach die Verarbeitung personenbezogener Daten, aus denen die rassistische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Daten über Gesundheit oder Sexualleben (unter Vorbehalt des Art 8 Abs 2) untersagt ist, wird hingewiesen.

Dem wird im Entwurf allerdings nicht Rechnung getragen, denn die Richtlinie schließt nach ihrem klaren Wortlaut auch Verkehrsdaten von der Speicherung aus, sofern sie im konkreten Fall Aufschluss über den Inhalt einer Kommunikation geben (zB Bestellbestätigung einer Onlineapotheke, Anruf bei „Licht ins Dunkel“, nicht hingegen Anrufe zwischen Privatpersonen). Art 5 Abs 2 der Richtlinie über die Vorratsdatenspeicherung wird daher nicht umgesetzt. Freilich bleibt unklar, wie man vorweg Verkehrsdaten, die Aufschluss über den Inhalt einer Kommunikation geben, von sonstigen Verkehrsdaten unterscheiden und ihre Speicherung ausschließen könnte. Auch in der deutschen Literatur zu § 113a Abs 8 dTKG wird dieses Problem nicht aufgegriffen. Dort wird vertreten, Art 5 Abs 2 der Richtlinie wiederhole die gleichbedeutende Aussage des Art 1 Abs 2 Satz 2⁷⁾ und die technische Umsetzung der Trennung zwischen Verkehrsdaten, die Rückschlüsse auf das Kommunikationsverhalten ermöglichen, und Inhaltsdaten sei „im Einzelnen nicht unproblematisch“⁸⁾.

V. Kostenersatz

Nach § 94 Abs 1 des Entwurfs ist der Anbieter nach Maßgabe der gem Abs 3 und 4 erlassenen Verordnungen verpflichtet, alle Einrichtungen bereitzustellen, die zur Überwachung von Nachrichten sowie zur Auskunft über Daten einer Nachrichtenübermittlung einschließlich der Auskunft über Vorratsdaten nach den Bestimmungen der StPO erforderlich sind. Der Bundesminister für Justiz hat im Einvernehmen mit dem BMVIT und dem BMF durch Verordnung einen angemessenen Kostenersatz vorzusehen.

Nach bisheriger Rechtslage ist ein Kostenersatz für die Bereitstellung von Einrichtungen iS des § 94 Abs 1 weder in der ÜVO⁹⁾ noch in der ÜKVO¹⁰⁾ vorgesehen (letztere sieht nur einen Kostenersatz für die Mitwirkung an der Überwachung einer Telekommunikation nach den Bestimmungen der StPO

⁶⁾ Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

⁷⁾ *Westphal*, Die neue EG-Richtlinie zur Vorratsdatenspeicherung – Privatsphäre und Unternehmerfreiheit unter Sicherheitsdruck, EuZW 2006, 555.

⁸⁾ *Scheurle/Mayer/Fellenberg*, TKG² (2008) § 113a Rdnr 29.

⁹⁾ VO der BMVIT über die Überwachung des Fernmeldeverkehrs, BGBl II 2001/418 idF BGBl II 2003/559.

¹⁰⁾ VO der BMJ über den Ersatz der Kosten der Betreiber für die Mitwirkung an der Überwachung einer Telekommunikation, BGBl II 2004/322.

vor). Die IKVO¹¹⁾ sieht nur einen auf 17 Millionen Euro für alle Betreiber zusammen und prozentuell auf 90 % begrenzten Kostenersatz vor (§ 4 IKVO).

Mit der Neuregelung in § 94 Abs 1 des Entwurfs entspricht der Gesetzgeber dem **Erkenntnis des VfGH** vom 27.2.2003¹²⁾, wonach bei der Inpflichtnahme privater Betreiber von Telekommunikationsdiensten für die Überwachung des Fernmeldeverkehrs und bei der Bereitstellung von entsprechenden Einrichtungen im Hinblick auf die Regelung der Kostentragung der Verhältnismäßigkeitsgrundsatz zu beachten ist.

Dass die Kosten für die Bereitstellung der Einrichtungen zur Vorratsdatenspeicherung künftig ersetzt werden, ist auch deshalb zu begrüßen, weil diese Kosten andernfalls von den Betreibern und Diensteanbietern auf die Benutzer überwältzt werden und weil ein vorhandener Kostenfaktor auf Staatsseite zur **regulativen Zurückhaltung** motiviert.

In den EB wird hinsichtlich der Kostenregelung eine Anpassung der IKVO an die neue Rechtslage vorgeschlagen. Im Hinblick auf den Verhältnismäßigkeitsgrundsatz sollte der bisherige § 2 Abs 1 IKVO dahin geändert werden, dass auch die **Kosten des Betriebes und der Instandhaltung** der Einrichtungen sowie sonstige laufend anfallende Kosten erfasst werden, weil nicht ersichtlich ist, wieso diese zur Gänze auf die Anbieter überwältzt werden sollen, obwohl sie im Laufe der Zeit die Anschaffungskosten überschreiten können. Solche Kosten werden auch nicht durch die ÜKVO abgedeckt, weil ein Kostenersatz dort von einer konkreten, gemäß § 138 Abs 3 StPO aufgetragenen Mitwirkung des Anbieters abhängt.

VI. Keine Pflicht zur Einrichtung eines Journaldienstes

Nach dem neu gefassten § 94 Abs 2 TKG ist

„der Betreiber verpflichtet, an der Überwachung von Nachrichten sowie der **Auskunft über Daten einer Nachrichtenübermittlung einschließlich der Auskunft über Vorratsdaten** nach den Bestimmungen der StPO im erforderlichen Ausmaß mitzuwirken.“

Die EB erläutern zwar, warum eine Erstreckung auf Vorratsdaten erfolgt, nicht aber, warum eine Erstreckung auf eine Mitwirkung an „*der Auskunft* (...) im erforderlichen Maß“ überhaupt erfolgt.

Damit ist auch die Frage einer Journaldienstverpflichtung der Betreiber zur Erteilung von Auskünften angesprochen. Betreiber sind bisher zur Mitwirkung an Wochenenden, Feiertagen und zur Nachtzeit nicht gesetzlich verpflichtet (auch nicht auf Grund der bloßen Kostenersatzregelung des § 5 ÜKVO). Notrufe werden jederzeit beauskunftet.

¹¹⁾ Verordnung der BMJ über den Ersatz der Investitionskosten der Betreiber für die Bereitstellung aller Einrichtungen, die zur Auskunft von Daten und zur Überwachung des Inhalts einer Telekommunikation erforderlich sind, BGBl II 2008/320.

¹²⁾ VfGH 27.2.2003, G 37/02.

Nach dem neuen § 102b Abs 2 TKG (Auskunft über Vorratsdaten) sind die

„nach § 102a zu speichernden Daten so zu speichern, dass sie **unverzüglich** an die nach den Bestimmungen der StPO und nach dem dort vorgesehenen Verfahren für die Erteilung einer Auskunft über Daten einer Nachrichtenübermittlung zuständigen Behörden übermittelt werden können.“

Nach den EB hierzu

„impliziert die Wendung „unverzüglich“ **keinesfalls, dass Anbieter zur Einrichtung eines Journaldienstes** zur Erteilung von Auskünften über Vorratsdaten verpflichtet sind. Eine Verpflichtung zur Beauskunftung außerhalb der Bürozeiten besteht daher nicht.“

Dies deutet darauf hin, dass dann nach dem neugefassten § 94 Abs 2 TKG nicht eine ebensolche Journaldienstverpflichtung – ganz im Gegenteil – doch bestehen kann. Dies sollte aber in den EB zu § 94 TKG klargestellt werden.

VII. Neudefinition der Stammdaten

Durch den Entwurf wird die Definition der Stammdaten geändert, im Gegensatz zur geltenden Rechtslage werden nunmehr auch juristische Personen erfasst (§ 92 Abs 3 Z 3). Die Änderung umfasst die gesamte Z 3 und zählt die Teilnehmernummer (bisher lit d), Informationen über Art und Inhalt des Vertragsverhältnisses (bisher lit e) und die Bonität (bisher lit f) nicht mehr auf.

Die ebenfalls neuen § 90 Abs 6 und 7 sprechen hingegen von „Stammdaten im Sinne von § 92 Abs 3 Z 3 lit a bis e“. In einer der beiden Bestimmungen dürfte daher ein Redaktionsversehen vorliegen. In den EB wird eine Einschränkung des Begriffes der Stammdaten nicht erwähnt.

VIII. Datensicherheit

Die Einführung der Pflicht zur **verschlüsselten Übertragung** per E-Mail (im CSV-Dateiformat) **für Auskunftserteilungen** in § 94 Abs 4, § 102b Abs 3 des Entwurfs in Umsetzung von Art 7 lit b der Richtlinie (entsprechende Verwaltungsstrafbestimmung in § 109 Abs 3 Z 25) ist zu begrüßen.

IX. Verwaltungsstrafbestimmungen

Der Entwurf ordnet in **§ 109 Abs 3 Z 22** Verstöße gegen die Speicherungspflicht für Vorratsdaten (§ 102a des Entwurfs) als Verwaltungsübertretung ein und sanktioniert sie mit einer Geldstrafe bis zu 37.000 Euro. Die Strafbarkeit besteht nicht, wenn die hierfür erforderlichen **Investitionskosten** noch nicht aufgrund einer nach § 94 Abs 1 erlassenen Verordnung abgegolten wurden.

Der Ausschluss der Strafbarkeit bis zur Abgeltung der Kosten ist zu begrüßen. Fraglich ist nur, wie der unveränderte **§ 109 Abs 4 Z 7 TKG** zu deuten ist, wonach eine Verwaltungsübertretung begeht und mit Geldstrafe bis zu 58.000 Euro zu bestrafen ist, wer entgegen § 94 Abs 1 nicht Einrichtungen zur Überwachung einer Telekommunikation bereitstellt.

Zum einen spricht die Bestimmung noch von „Einrichtungen zur Überwachung einer Telekommunikation“ und sollte an die neue Terminologie des § 94 Abs 1 angepasst werden, wie dies der Entwurf in § 109 Abs 3 Z 14 bereits vorsieht. Zum anderen ist nicht ersichtlich, warum ein Anbieter zwar alle Einrichtungen zur Speicherung von Daten und zur Auskunft über sie mit Inkrafttreten des Gesetzes bereitstellen muss, aber mit der Vorratsdatenspeicherung bis zur Abgeltung der Investitionskosten zuwarten kann. Deshalb sollte in § 109 Abs 4 Z 7 eine § 109 Abs 3 Z 22 entsprechende Ausnahme aufgenommen werden (Zuwarten bis zur Abgeltung der Investitionskosten).

Die Österreichische Notariatskammer lehnt aus dem Grund der Unverhältnismäßigkeit des Grundrechtseingriffes vor einer Entscheidung der Fälle Deutschland und Rumänien die Umsetzung der Richtlinie 2006/24/EG über die Vorratspeicherung von Daten ab. Im Falle der Umsetzung ersucht sie aus dem gleichen Grund um eine klare und sehr restriktive Festlegung der Delikte, die unter schweren Straftaten zu verstehen sind.

Mit vorzüglicher Hochachtung



Dr. Klaus Woschnak

(Präsident)