Dr. Alexander Grunicke, LL.M.
1150 Wien

Wien, den 14.1.2010

An
Bundesministerium für Verkehr, Innovation und Technologie
1030 Wien

Parlamentsdirektion
1017 Wien

Betrifft: BMVIT-630.333/0001-III/PT2/2009, GZ 117/ME

Stellungnahme zum Ministerialentwurf betreffend eines Bundesgesetzes, mit dem das Telekommunikationsgesetz 2003 – TKG 2003 geändert wird

Sehr geehrte Damen und Herren!

Im Rahmen des Begutachtungsverfahrens zum oben bezeichneten Ministerialentwurf erlaube ich mir, nachfolgende Stellungnahme abzugeben:

1. Grundsätzliches

„Die flächendeckende Erfassung des Telekommunikationsverhaltens der Bevölkerung droht, die Unbefangenheit des Kommunikationsaustausches und das Vertrauen in den Schutz der Unzugänglichkeit der Telekommunikationsanlagen insgesamt zu erschüttern." Dies ist einer der wesentlichen Gründe aus denen das deutsche BVerfG per einstweiliger Anordnung[1] die Anwendung der zentralen Bestimmung des deutsche TKG zur Vorratsspeicherung vorläufig nur unter strengen Auflagen genehmigt hat. Schließlich soll das verfassungsrechtlich normierte Recht des Fernmeldegeheimnisses und das Recht auf Achtung der Privatsphäre den für eine demokratische Gesellschaftsordnung so wichtigen freien und ungezwungenen Gedankenaustausch gewährleisten.

Beim Studium der Erläuterungen wird der Eindruck erweckt, dass die Verfasser selbst nicht von der Grundrechtskonformität ihres Entwurfes überzeugt sind. Allein die Tatsache, dass Verkehrsdaten Rückschlüsse auf den Inhalt einer Kommunikation zulassen, zeigt die politische und rechtliche Brisanz der Vorratsdatenspeicherung[2]. Die Vorratsdatenspeicherung ist weder geeignet, Kriminalität oder Terrorismus zu verhindern noch ist sie verhältnismäßig. Vielmehr ist zu befürchten, dass die in den letzten Jahren publik gewordenen teils politisch teils geschäftlich motivierten Datenmissbräuche (z.B. EKIS in AT, Entwendung von Kundendaten eines Telekombetreibers in GB) und Pannen (Verlust von Steuerdaten in GB) zunehmen werden.

M.E. wurde bis dato im Begutachtungsverfahren kaum darauf hingewiesen, dass auch juristische Personen den Schutz der Grundrechte (auf Datenschutz und auf Fernmeldegeheimnis) genießen. Für Unternehmen besteht nämlich ein doppeltes Risiko: Zum einen können Unternehmensdaten im Rahmen der präventiven Kontrolle (Stichwort Terrorismusbekämpfung) abgefragt werden. Zum anderen steht zu befürchten, dass Vorratsdaten, seien diese nun rechtmäßig oder rechtswidrig gespeichert, auch Rückschlüsse auf Betriebs- und Geschäftsgeheimnisse (z.B. Kundendaten) zulassen.

---

[1] BVerfG, 1 BvR 256/08 vom 11.3.2008
[2] Z.B. Anruf oder e-mail bei / an psychologische oder gesundheitliche Beratungseinrichtungen,

Schon nach geltender Rechtslage stehen den Strafverfolgungsbehörden gemäß §§ 135 ff StPO weitgehende Befugnisse und Instrumentarien zur Verfügung. Dazu zählen im Besonderen die Auskunft über Daten einer Nachrichtenübermittlung, die (inhaltliche) Überwachung von Nachrichten, die optische und akustische Überwachung sowie der Datenabgleich.

Darüber hinaus wurden mit den letzten Novellen zum SPG die Befugnisse der Sicherheitsbehörden hinsichtlich Ermittlung und Verarbeitung im Rahmen der (vorbeugenden) Gefahrenabwehr erheblich erweitert. So sind beispielsweise die Sicherheitsbehörden gemäß § 53 Abs. 3 a SPG ermächtigt, ohne richterliche Genehmigung und bei bloßer „Annahme einer konkreten Gefährdungssituation" von Telekombetreibern und Anbietern gemäß ECG Auskunft über die Stammdaten eines bestimmten Anschlusses sowie Namen und Anschrift eines Benutzers, dem eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen wurde, zu verlangen. Nur am Rande sei auch erwähnt, dass sich im SPG keine hinreichend klaren Legaldefinitionen der diversen Gefahrenbegriffe finden.

2. Zu den Regelungen des Entwurfes im einzelnen

2.1 Definition der „Vorratsdaten" in § 92 Abs. 3 Z 6b und Speicherverpflichtung

Die vorgeschlagene Definition in § 92 Abs. 3 Z 6b sollte wie folgt ergänzt werden:
Daten, die ausschließlich aufgrund der Speicherverpflichtung gemäß § 102a gespeichert werden dürfen. Es soll vorkommen, dass schon heute einige Provider die in § 102 a näher beschriebenen Daten speichern. Ansonsten könnte in Zukunft argumentiert werden, dass die Speicherung nicht ausschließlich aufgrund der neuen Verpflichtung erfolgt, womit solche Daten keine Vorratsdaten mehr wären.[3] Daher müsste auch der drittletzte Satz in § 99 Abs. 5 Z 2 wie folgt lauten: *Eine Verpflichtung oder Berechtigung zur Speicherung von Verkehrsdaten allein aufgrund dieses Absatzes besteht nicht.*

2.2 Zugriff der Sicherheitsbehörden auf Verkehrs- und Standortdaten im präventiven Bereich - § 99 Abs. 5

Obwohl in der Richtlinie 2006/24/EG die Verwendung für präventive Zwecke vom EU-Parlament abgelehnt wurde, sind die österreichischen Sicherheitsbehörden schon derzeit befugt, ohne richterliche Genehmigung Auskünfte über die bei den Telekombetreibern für „betriebsnotwendige" Zwecke gespeicherten Daten, also Stamm- und Verkehrsdaten, einzuholen. M.E. sind die §§ 53 Abs. 3 a SPG und der vorgeschlagene § 99 Abs. 5 TKG nicht grundrechtskonform ausgestaltet. Die vorgeschlagene Ausgestaltung des § 99 Abs. 5 als Verfassungsbestimmung samt den Erläuterungen dazu unterstreichen lediglich die Grundrechtsbedenken. Dieser Grundrechtseingriff wird auch nicht durch das in § 91c SPG normierte bloße Informationsrecht und die ex-post Kontrolle des Rechtsschutzbeauftragen geheilt.

2.3 Fehlende Definition des Begriffes "schwere Straftaten" in § 102 a

Der Entwurf hat die Übernahme des Begriffes „schwere Straftaten" wortgleich aus der Richtlinie 2006/24/EG übernommen, ohne diesen zu konkretisieren. Grundrechtseingriffe müssen nach herrschender Judikatur des VfGH hinreichend gesetzlich determiniert sein. Aus den Erwägungsgründen der Richtlinie ergibt sich, dass ursprünglich eine Zweckbindung der Vorratsdatenspeicherung an Terrorismusbekämpfung und schwere organisierte Kriminalität beabsichtigt war.

---

[3] *Franz Schmidbauer,* Die Vorratsbüchse der Pandora, www.internet4jurists.at/news/aktuell100a.htm

Es wird daher empfohlen, einen abschließenden Katalog von schweren Straftaten (organisierte Kriminalität, Verbrechen gegen Leib und Leben) oder Verbrechen mit einem bestimmten Mindeststrafrahmen zu definieren. Da die Vorratsdaten in der Eingriffsintensivität zwischen den Verkehrsdaten und den Inhaltsdaten liegen, sollte sich der Strafrahmen konsequenterweise zwischen jenen des § 135 Abs. 3 Z 3 StPO (Auskunft von Daten einer Nachrichtenübermittlung) und § 136 Abs. 1 StPO (optische und akustische Überwachung von Personen) bewegen.

2.4 Datensicherheit und Kontrolle - § 102 c

Die in § 102 c vorgeschlagenen Maßnahmen zur Datensicherheit und Kontrolle sind m.E. nicht ausreichend (determiniert). Die Anordnung der getrennten Speicherung der für betriebsnotwendige Zwecke und auf Vorrat gespeicherten Daten kann das grundsätzliche (technische und kriminelle) Risiko der Vermischung dieser Datenarten nur begrenzen, aber nicht gänzlich ausschalten. Darüber hinaus sollten die „besonders ermächtigten Personen“,[4] die ausschließlich Zugang zu Vorratsdaten haben, näher definiert werden. So sollten sowohl im Hinblick auf die betriebliche Organisation der Telekombetreiber (Zutrittskontrolle, sehr enge Begrenzung des autorisierten Personenkreises) als auch auf Qualifikation und Vertrauenswürdigkeit nähere Vorgaben gemacht werden.

2.5 Fehlende Berücksichtigung der Berufsgeheimnisse und des Redaktionsgeheimnisses

Gemäß § 144 Abs. 2 StPO sind die in den §§ 134 ff angeordneten Ermittlungsmaßnahmen unzulässig, soweit dadurch das Entschlagungsrecht einer der in § 157 Abs. 1 Z 2 - 4 StPO genannten Personen umgangen wird (Rechtsanwälte, Notare, Psychotherapeuten, Psychiater, Mediatoren, Medieninhaber und Medienmitarbeiter).

Wenn die StPO nicht nur den Inhalt einer Kommunikation sondern auch Verkehrsdaten zwischen Rechtsanwalt bzw. Journalisten einerseits und ihren Mandanten bzw. Informanten andererseits schützt, muss dies konsequenterweise auch für Vorratsdaten gelten. In § 144 StPO bzw. das TKG sollte dementsprechend zwecks Vermeidung der Umgehung des Entschlagungsrechtes für die oben genannten Berufsgruppen ausdrücklich die Speicherung und Verarbeitung von Vorratsdaten festgeschrieben werden.

3. Appell

Aufgrund der hier nur angerissenen massiven grundrechtlichen und demokratiepolitischen Bedenken gegen den Entwurf sowie die zugrunde liegende Richtlinie 2006/24/EG appelliere ich an den Gesetzgeber, die Umsetzung vorläufig auszusetzen. Stattdessen sollte nochmals auf EU-Ebene eine breite Diskussion über Sinn und Zweck einer Vorratsdatenspeicherung angestoßen werden.

Sollte dies politisch nicht durchsetzbar sein, ersuche ich höflich um Berücksichtigung der oben dargelegten Änderungsvorschläge.

Mit freundlichen Grüßen

Alexander Grunicke

[4] Obwohl in den Erläuterungen dieser unbestimmte Begriff kritisiert wird, übernimmt der Entwurf diesen wortgleich in § 102 c.