REPUBLIK ÖSTERREICH
DATENSCHUTZKOMMISSION

A-1010 Wien, Ballhausplatz 1
Tel. ++43-1-531 15/0
Fax: ++43-1-531 15/2690
e-mail: dsk@dsk.gv.at
DVR: 0000027

Sachbearbeiter: Mag. Georg LECHNER, Klappe 2946
E-Mails in dieser Sache bitte an: dsk@dsk.gv.at
Faxsendungen bitte nur an die oben angegebene Nummer!

GZ K054.012/0002-DSK/2007

Novelle zum Telekommunikationsgesetz (Verkehrsdatenspeicherung)

Stellungnahme der DSK im Begutachtungsverfahren

An das
Bundesministerium für Verkehr, Innovation und Technologie
Sektion III, Abteilung PT 2

Ghegastraße 1
1030 Wien

Per E-Mail: jd@bmvit.gv.at

Betrifft: Entwurf eines Bundesgesetzes, mit dem das Telekommunikationsgesetz 2003 geändert wird, do. Zahl BMVIT-630.333/0001-III/PT2/2007

Bezugnehmend auf den Entwurf eines Bundesgesetzes, mit dem das Telekommunikationsgesetz 2003 geändert wird, gibt die Datenschutzkommission angesichts des Umstandes, dass sie mit wesentlichen Kontrollaufgaben nach diesem Entwurf betraut werden soll, folgende Stellungnahme ab:

Zu Ziffer 4 und 5 (§ 92 Abs. 3 Z 3 und „§ 92 Abs. 4a", richtig wohl § 92 Abs. 3 Z 4a)

1. In den Definitionen des § 92 Abs. 3 Z 3 lit. a soll der Ausdruck „Teilnehmernummer und sonstige Kontaktinformation für die Nachricht" durch den Inhalt der Z 4a lit. a ersetzt werden. Als Zweck wird in den Erläuterungen angegeben, dass hiermit klargestellt werden solle, dass dynamische IP-Adressen „Stammdaten" seien.

Diese Absicht beruht auf einer Verkennung technisch/logischer Zusammenhänge: Wenn eine statische IP-Adresse – ebenso wie eine Telefonnummer – einem namentlich bezeichneten Teilnehmer zugeschrieben wird, wird hiermit keine Aussage über eine tatsächlich stattgefundene Kommunikation getroffen; die statische IP-Adresse in Verbindung mit nur dem Namen des Teilnehmers ist daher tatsächlich kein „Verkehrsdatum". Anders ist

dies bei einer dynamischen IP-Adresse, die nur im Zusammenhang mit einer tatsächlich stattgefundenen Kommunikation einem bestimmten Teilnehmer zugeordnet werden kann. Jede Aussage darüber, dass einem bestimmten Teilnehmer eine dynamische IP-Adresse zugeordnet war, muss daher auf eine konkrete Kommunikation zu einem konkreten Zeitpunkt bezogen sein - solche Angaben stellen daher automatisch auch „Verkehrsdaten" dar. Dies durch eine gesetzliche „Definition" leugnen zu wollen, kann die Problematik der Speicherung von Verkehrsdaten zwar verdecken, aber nicht beseitigen.

Der Begriff der „Stammdaten" leitet sich aus dem Bereich der traditionellen Telephonie her und ist im Internet-Bereich nicht gleichermaßen anwendbar. So kennt etwa die Telekom-Datenschutz-Richtlinie 2002/58/EG den Begriff der „Stammdaten" überhaupt nicht. Es scheint nun nicht zulässig, den von dieser Richtlinie aufgestellten Vertraulichkeitsschutz für „Verkehrsdaten" dadurch zu unterlaufen, dass Daten, die bisher im TKG 2003 selbst als „Zugangsdaten" und damit eindeutig als „Verkehrsdaten" bezeichnet wurden, nunmehr als „Stammdaten" qualifiziert werden, womit sie offenbar aus dem besonderen grundsätzlichen Schutz des Telekommunikationsgeheimnisses heraus gelöst werden sollen.

2. Da sich die vorliegende Novelle entsprechend der abgegebenen österr. Erklärung zum Umsetzungszeitplan nur auf Telephonie beziehen soll, besteht auch derzeit gar kein Anlass, sich mit Begriffen der Internet-Kommunikation zu befassen, sodass eine Novellierung des § 92 Abs. 3 Z 3 am besten unterbleibt und die Klärung dieser Fragen weiterer Judikatur vorbehalten wird.

Die in bb) bezeichneten Daten über Internet-Kommunikationen stellen im Übrigen einen Fremdkörper in der vorliegenden Novelle dar, und zwar nicht nur im Hinblick auf die bereits erwähnte österr. Erklärung zum Umsetzungszeitpunkt, sondern auch im Gesamtgefüge, da sie ausschließlich zur Identifizierung „der Quelle einer Nachricht" aufgezeichnet werden sollen. Da im Zeitpunkt der Verwendung einer IP-Adresse nicht bekannt ist, ob die damit bewerkstelligte Kommunikation später aus dem Blickwinkel des Senders oder des Empfängers geprüft werden wird, bedeutet dies die Speicherung sämtlicher Internet-Zugangsdaten, womit die bis 2009 aufgeschobene Umsetzung bereits jetzt durchgeführt wäre. Dies widerspricht dem diametral, was in der Öffentlichkeit bisher als politische Absicht präsentiert wurde (vgl. dazu auch die Erklärung auf der Website des BMVIT).

Zu Ziffer 7 - § 102a (Speicherung von Vorratsdaten)

Die Daten sollen zum Zweck der Ermittlung, Feststellung und Verfolgung von „mit beträchtlicher Strafe bedrohten Handlungen" (§ 17 SPG), einschließlich der Tatbestände der §§ 107 und 107a StGB gespeichert werden. Der Speicherungszweck der Daten ist daher auf Delikte beschränkt, die mit einer mehr als einjährigen Freiheitsstrafe bedroht sind (§ 17 SPG). Die Delikte der §§ 107 und 107a StGB („Gefährliche Drohung" und „Beharrliche Verfolgung", also Stalking) sind noch zusätzlich genannt.

Die Vorratsdatenspeicherung wurde zur Bekämpfung der organisierten Kriminalität und des Terrorismus eingeführt (siehe Erwägungsgründe 7 und 8 der Richtlinie 2006/24/EG) und sollte wegen der schwerwiegenden grundrechtlichen Implikationen keinesfalls auf andere Delikte ausgedehnt werden. Der Entwurf ersetzt die in der Richtlinie angeführte Zweckbestimmung durch einen pauschalen Verweis auf einen bestimmten Strafrahmen, womit die Verwendung von Vorratsdaten auch für ganz andere Delikte möglich wird. Der Entwurf weicht in diesem Punkt von den in der Richtlinie 2006/24/EG angeführten Zwecken ab und ist nach Auffassung der DSK überschießend:

Die Heranziehung des § 17 SPG erscheint der Datenschutzkommission im Lichte der Schwere des durch die Vorratsdatenspeicherung vorgenommenen Grundrechtseingriffs unverhältnismäßig, denn unter schweren Straftaten sind gewöhnlich nur Straftaten zu verstehen, die vom Strafgesetzbuch als Verbrechen eingestuft werden, nicht jedoch die als Vergehen eingestuften strafbaren Handlungen. Eine Prüfung der Auswirkungen des § 17 SPG anhand des StGB hat ergeben, dass etwa zwei Drittel der Straftatbestände des StGB den Voraussetzungen des § 17 SPG genügen – die Verwendbarkeit von gespeicherten Vorratsdaten zur Strafverfolgung wäre daher nicht mehr die Ausnahme vom Telekommunikationsgeheimnis sondern die Regel und käme daher substantiell der Abschaffung des Telekommunikationsgeheimnisses gleich.

Erschwerend kommt hinzu, dass die rechtlichen Voraussetzungen der Übermittlung der gespeicherten Daten zur Strafverfolgung äußerst unscharf geregelt sind:

Es wird zwar in § 102a Abs. 1 ein Zweck *der Speicherung* genannt, der § 17 SPG als Grenze erwähnt, doch ist dies insofern wertlos, als im Zeitpunkt der Speicherung keine Begrenzung der zu speichernden Daten vorgenommen werden kann, da ja nicht bekannt ist, ob die Kommunikation einer strafbaren Handlung dient bzw. gedient hat. Hinsichtlich des kritischen Moments einer *Übermittlung* der gespeicherten Daten zum Zweck der Strafverfolgung

a) wird der Umfang der zu übermittelnden Daten erweitert, indem neben den Vorratsdaten auch „alle sonstigen damit zusammenhängenden erforderlichen Informationen“ weiterzuleiten sind,
b) werden die Empfänger der Daten sehr allgemein mit „die für die Durchführung einer Überwachung einer Telekommunikation zuständigen Behörden“ umschrieben, und
c) wird als Zulässigkeitsvoraussetzung „eine gerichtliche Anordnung oder Bewilligung“ genannt, die in Abs. 4 Z 3 näherhin als „Anordnung gemäß § 149b StPO“ bezeichnet wird (- hinsichtlich der „Bewilligung“ fehlt ein näherer Hinweis auf ihre Rechtsgrundlage).

Der Rekurs auf § 149b StPO in § 102a TKG wirft viele Fragen auf, unter anderem auch diese: Ist eine solche Anordnung angesichts des Verweises auf § 149a Abs. 2 Z 1 und 2 im § 149b auch für strafbare Handlungen zulässig, die nur „mit mehr als sechsmonatiger Freiheitsstrafe bedroht sind“ (§ 149a Abs. 2 Z 1), also z.B. auch bei bestimmten Urheberrechtsverletzungen im Internet?

Generell muss gefordert werden, dass
1. eine Verwendungsbeschränkung für die Weitergabe der Vorratsdaten vorgesehen wird und nicht nur eine Zweckbindung bei der Speicheranordnung, die wirkungslos ist, da die Speicherverpflichtung ja schon aus logischen Gründen nur alle Vorratsdaten unterschiedslos betreffen kann;
2. im Hinblick auf die Weitergabe eine klare und eindeutige Aussage über die zulässigen Fälle der Datenanforderung getroffen wird, in der die Interpretationsuntiefen der §§ 149a und 149b StPO möglichst vermieden werden.

Zu Ziffer 10 - § 109 TKG (Strafbestimmung)

Mit der Novelle soll der Verstoß gegen die Speicherpflicht unter Strafe gestellt werden. Die Bestimmung ist wie eine Strafandrohung für ein punktuelles Ereignis formuliert ("17a. entgegen § 102a Daten nicht speichert"), aber ein Verstoß gegen die Speicherpflicht ist eine Unterlassung, kein punktuelles Ereignis. Es ist auch unklar, wie Verstöße festgestellt werden sollen. Ein Verstoß ist nur feststellbar, wenn die Daten angefordert werden und der Verpflichtete nicht liefern kann, es sei denn, dass regelmäßige Kontrollen stattfinden.

Es fehlen ebenfalls Strafbestimmungen gegen unerlaubte Zugriffe. § 51 DSG 2000 (Datenverwendung in Gewinn- oder Schädigungsabsicht) reicht dazu nicht aus, weil der Missbrauch dieser Daten wegen der gesetzlichen Pflicht zur Speicherung nicht nur dann strafbar sein soll wenn Gewinn- oder Schädigungsabsicht vorliegen, sondern grundsätzlich.

Es wäre daher zu prüfen, ob die sonst verschiedenen Strafbestimmungen unterschiedlichen Schutz gegen unbefugte Verwendung bieten.

Es fehlen auch Bestimmungen über eine Verpflichtung des Personals zur besonderen Verschwiegenheit im Umgang mit Daten aus der Vorratsdatenspeicherung.

Zu Ziffer 12 - § 114a TKG (Kontrolle durch die Datenschutzkommission)

Die Datenschutzkommission wird entsprechend dem Art. 9 der RL 2006/24/EG zur Vollziehung von § 102a (Speicherung von Vorratsdaten) berufen, was grundsätzlich für sinnvoll erachtet wird. Im Vorblatt zu den Erläuterungen ist allerdings unter „Finanzielle Auswirkungen" kein Ressourcenbedarf für die Wahrnehmung dieser Aufgabe angemeldet. Dies ist aus Sicht der DSK – mit der das BMVIT in der vorliegenden Sache bisher keinerlei Kontakt gepflogen hat – inakzeptabel. Die Verantwortung für die ordnungsgemäße Durchführung der Vorratsdatenspeicherung kann nur dann getragen werden, wenn die Voraussetzungen dafür geschaffen werden – dies betrifft sowohl Personalressourcen als auch entsprechende organisatorische Vorkehrungen wie Berichtspflichten seitens der Betreiber etc.

Der Passus „nach Maßgabe des § 1 Abs. 5 letzter Satz DSG 2000" ist im vorliegenden Zusammenhang im Übrigen unklar, da nicht erkennbar ist, ob es sich um die Durchsetzung von Betroffenenrechten handeln soll, oder um eine generelle Rechtmäßigkeitskontrolle nach § 30 DSG 2000 im Hinblick v.a. auf Datensicherheit (Art. 9 der RL 2006/24/EG). Insgesamt wäre es daher dringend geboten, Gespräche mit der DSK darüber aufzunehmen, welche Voraussetzungen für eine solche Kontrolle zu schaffen wären.

23. Mai 2007
Für die Datenschutzkommission
Der Vorsitzende:
HR des OGH Dr. SPENLING

Für die Richtigkeit
der Ausfertigung: