Bures schickt Novelle zur Vorratsdatenspeicherung in Begutachtung

Wien, 20.11.2009

Speicherdauer auf sechs Monate beschränkt - Größtmöglicher Schutz persönlicher Daten

Infrastrukturministerin Doris Bures hat heute einen Entwurf für eine Novelle des Telekommunikationsgesetzes (TKG), mit der die EU-Richtlinie zur Vorratsdatenspeicherung umgesetzt werden soll, in Begutachtung geschickt. Sie betont dazu: "Im Umgang mit personenbezogenen Daten ist größte Sorgfalt geboten. Dieser Entwurf soll den größtmöglichen Schutz persönlicher Daten sicherstellen. Da es sich um eine Speicherung von Daten auf Vorrat handelt, also ohne, dass es Verdachtsmomente gegen eine bestimmte Person gibt, sind höchste datenschutzrechtliche und rechtsstaatliche Standards ein absolutes Muss. Daher will ich auch nur eine Mindestumsetzung der EU-Richtlinie, also eine maximal sechsmonatige Speicherdauer der Daten, Verwendung nur für die Aufklärung von schweren Straftaten und nur mit gerichtlicher Anordnung." ****

Die EU-Richtlinie, die 2006 von den Justiz- und Innenministern unter dem Eindruck der Terroranschläge in New York und Spanien beschlossen wurde, sieht die Speicherung von Verbindungsdaten vor, im Wesentlichen wer, mit wem, wann, wie lange, von wo aus (geographisch) und über welchen Dienst (E-Mail, SMS, Mobil- und Festnetztelefonie, Internettelefonie, Internet) kommuniziert hat, nicht aber die Inhalte. Laut EU-Richtlinie soll die Datenspeicherung mindestens sechs Monate und maximal zwei Jahre verpflichtend sein. Diese Daten sollen laut Richtlinie von den Strafverfolgungsbehörden zur Aufklärung schwerer Straftaten abgerufen werden können.

Die Richtlinie hätte bereits 2007 umgesetzt werden müssen. Es ist bereits ein Vertragsverletzungsverfahren gegen Österreich beim EuGH anhängig. Um Strafzahlungen zu vermeiden, ist es wichtig, dass Österreich jetzt einen Entwurf vorlegt und in Begutachtung schickt. Trotzdem ist die Vorratsdatenspeicherung "viel zu sensibel, um eine Regelung übers Knie zu brechen", argumentiert die Ministerin. Deshalb hat sie mit acht Wochen bewusst eine außerordentlich lange Begutachtungsfrist vorgesehen. "Bei diesem Thema ist eine möglichst breite Diskussion notwendig", sagt Bures. Sie will eine möglichst umfassende Einbindung der Zivilgesellschaft, was einerseits bei der Erstellung des Entwurfs durch das Boltzmann-Institut für Menschenrechte geschehen ist, und jetzt bei der Diskussion im Rahmen der Begutachtung und im parlamentarischen Verfahren so beibehalten werden soll.

Der vorliegende Entwurf wurde von einer Expertengruppe unter Federführung des Boltzmann-Instituts für Menschenrechte (BIM) ausgearbeitet. Das BIM war ausdrücklich damit beauftragt, einen Vorschlag zu erarbeiten, der die geringstmögliche Umsetzung der Richtlinie bedeutet und den größtmöglichen Schutz persönlicher Daten und der Grundrechte beinhaltet. Daher sieht der Entwurf bei der Speicherdauer vor, dass die Daten nach sechs Monaten gelöscht werden müssen, und dass die Vorratsdaten nur für die Aufklärung von schweren Straftaten und nur mit gerichtlicher Anordnung herausgegeben werden dürfen.

Wie die Ministerin erläutert, soll es von der restriktiven Regelung beim Zugriff auf die Daten nur dann eine Ausnahme geben, wenn es um die Abwehr einer konkreten Gefahr für das Leben oder die Gesundheit eines Menschen geht. Das bezieht sich konkret auf Standortdaten, also die Ortung von Mobiltelefonen. Ein denkbarer Fall wäre etwa die Suche nach einem Vermissten in den Bergen oder die Ortung eines Entführungsopfers.

Über weite Strecken findet der Entwurf die Zustimmung des Koalitionspartners. Keine Einigung gibt es derzeit allerdings bei der Regelung über den Zugriff auf die IP-Adressen zugeordneten Personendaten. Grundsätzlich steht das Verkehrsministerium auf dem Standpunkt, dass die Personendaten zu IP-Adressen in den Schutzbereich des Fernmelde- und Kommunikationsgeheimnisses fallen. Der Zugang sollte also ebenfalls den strengen Regelungen unterliegen. Dies insbesondere deshalb, weil im Gegensatz zur Telefonie mit der Kenntnis von IP-Adressen und den zugeordneten Personendaten auch der Inhalt der jeweiligen Kommunikation ersichtlich wird.

Derzeit werden IP-Adressen nur für wenige Tage gespeichert, es gibt für die Betreiber keine Speicherverpflichtung, weil diese Daten für Verrechnungszwecke nicht notwendig sind. Im Gegenteil: die Betreiber sind derzeit verpflichtet solche Daten zu löschen. Die EU-Richtlinie schreibt die Speicherung von Internetverbindungsdaten aber vor. Damit werden diese Daten für die Sicherheitsbehörden unter den genannten Voraussetzungen (Aufklärung einer schweren Straftat, gerichtliche Anordnung) zugänglich. Das Innenministerium tritt hingegen dafür ein, dass die Behörden auch präventiv, das hieße, ohne dass bereits eine Straftat vorliegt, Zugang zu Internetverbindungsdaten bekommen.

Dieses Thema soll im Laufe der Begutachtung noch mit den betroffenen Ministerien besprochen werden. Aus Sicht des Verkehrsministeriums wäre eine Regelung denkbar, wonach die Sicherheitsbehörden Auskünfte über die Zuordnung von IP-Adressen zu bestimmten Teilnehmern zu einem bestimmten Zeitpunkt unter genau definierten Bedingungen erhalten. Und zwar zur Abwehr von konkreten Gefahren für Leben, Gesundheit und Freiheit eines

Menschen. Dazu müssten allerdings auch im Sicherheitspolizeigesetz Anpassungen bezüglich des Rechtsschutzes gemacht werden im Hinblick auf Informationspflichten und Einbindung der Datenschutzkommission.

Die Eckpunkte des Entwurfs

* Speicherdauer sechs Monate *Verwendung nur für die Aufklärung von schweren Straftaten * Zugriff auf die Daten nur mit gerichtlichem Befehl; einzige Ausnahme ist eine drohende Gefahr für Gesundheit oder Leben * Strenge Verwendungskontrolle der Daten (Dokumentationspflicht, Informationspflicht) * Restriktiver Datenumfang (nicht mehr, als von der Richtlinie verlangt) * Speicherung und Übergabe der Daten soll bestmöglich vor Missbrauch geschützt werden (Kontrolle durch die Datenschutzkommission, nur Einzelabfragen, keine Verknüpfungen).

Die Regelung im Detail

Grundsätzlich verfolgt der Entwurf das Ziel, die Richtlinie so umzusetzen, dass zwar ihr Zweck - die Ermittlung, Feststellung und Verfolgung von schweren Straftaten mittels auf Vorrat gespeicherter personenbezogener Daten - innerstaatlich erreicht wird, um den Strafverfolgungsbehörden die Verwendung zeitgemäßer technischer Mittel zu ermöglichen, zugleich aber durch gesetzliche Vorkehrungen sichergestellt ist, dass

* die mit der Vorratsdatenspeicherung verbundenen Grundrechtseingriffe so gering wie möglich ausfallen, * die Sicherheit der Daten sowohl bei den Telekommunikationsbetreibern als auch bei den zur Datenanwendung berechtigten Behörden bestmöglich gewährleistet ist, * den datenschutzrechtlich erforderlichen Informationspflichten nachgekommen wird, * alle notwendigen Rechtsmittel zur Verfolgung der datenschutzrechtlichen und grundrechtlichen Interessen Betroffener zur Verfügung stehen, * darüber hinausgehende unabhängige datenschutzrechtliche Kontrollen vorgesehen werden, und * die wirtschaftlichen Auswirkungen der Vorratsdatenspeicherung auf die zur Speicherung und Auskunft verpflichteten Telekommunikationsbetreiber grundrechtskonform zu gestalten sind.

Der Entwurf sieht vor, dass über die schon bisher für Telekommunikationsbetreiber bestehende Berechtigung zur Speicherung und Verarbeitung von Daten für betriebsnotwendige, insbesondere für Verrechnungszwecke (in der Regel für einen Zeitraum von drei Monaten) hinaus in Umsetzung der Vorgaben der Richtlinie bestimmte, näher umschriebene Daten (insbesondere IP-Adressen und Standortdaten) ab dem Zeitpunkt der Erzeugung oder Verarbeitung bis sechs Monate nach Beendigung der Kommunikation zu speichern sind (vorgeschlagener § 102a TKG).

Nach dem Entwurf dürfen Verkehrsdaten außer in den im TKG geregelten Fällen weder gespeichert noch verwendet werden und sind vom Betreiber nach Beendigung der Verbindung unverzüglich zu löschen oder zu anonymisieren (vorgeschlagener § 99 TKG). Mit dieser nun auch vom Wortlaut ausdrücklich abschließenden Regelung soll insoweit Rechtssicherheit geschaffen werden, als damit aus anderen gesetzlichen Bestimmungen weder eine Berechtigung noch gar eine Verpflichtung zur Speicherung von Verkehrsdaten abgeleitet werden kann.

Von der Speicherpflicht nicht erfasst sind Unternehmen, die mittels Bescheid als kleines Unternehmen gemäß der Empfehlung der EU Kommission 2003/361/EG eingestuft werden (vorgeschlagener § 102a Abs. 6 TKG). Diejenigen Telekommunikationsanbieter, die zur Speicherung verpflichtet sind, gelten zur rechtlichen Klarstellung in Bezug auf Vorratsdaten als Auftraggeber des öffentlichen Bereichs (vorgeschlagener § 102a Abs. 9 TKG). Die den Anbietern aus der Umsetzung der Vorratsdatenspeicherung entstehenden Kosten werden entsprechend vergütet (vorgeschlagener § 94 TKG).

Die auf Vorrat gespeicherten Daten dürfen ausschließlich aufgrund einer gerichtlichen Bewilligung und nur nach Maßgabe ausdrücklicher Gesetzesbestimmungen, die auf § 102a Bezug nehmen, zum Zweck der Ermittlung, Feststellung und Verfolgung von schweren Straftaten an die nach der StPO zuständigen Behörden übermittelt werden (vorgeschlagener § 102b TKG).

So wie bisher haben die zuständigen Behörden nach der StPO zur Verfolgung "niederschwelliger" Straftaten (also solcher, die keine "schweren Straftaten" sind) das Recht auf Beauskunftung der bei den Telekommunikationsbetreibern für betriebsnotwendige Zwecke gespeicherten Verkehrsdaten, wenn eine gerichtliche Bewilligung vorliegt (vorgeschlagener § 99 Abs. 5 Z. 1 TKG).

Ebenso wie bisher sind die nach dem SPG zuständigen Sicherheitsbehörden für die Erfüllung ihrer im SPG geregelten präventiven Aufgaben berechtigt, Auskünfte über die bei den Telekommunikationsbetreibern für betriebsnotwendige Zwecke gespeicherten Daten einzuholen.

Darüber hinaus sieht eine Verfassungsbestimmung vor, dass Sicherheitsbehörden für die Abwehr einer konkreten Gefahr für das Leben oder die Gesundheit eines Menschen unter bestimmten engen Voraussetzungen Auskünfte über Stammdaten und Standortdaten auch dann erhalten können, wenn dafür die Verwendung von Verkehrsdaten notwendig ist und deshalb in das unter Richtervorbehalt stehende Fernmeldegeheimnis eingegriffen wird

(vorgeschlagener § 99 Abs. 5 Z. 2 TKG).

Neben der positivrechtlichen Definition von einigen neuen, insbesondere technischen Begriffen beinhaltet der Entwurf die Definition, wie die IP-Adresse rechtlich einzuordnen ist. Entsprechend den jüngsten Entscheidungen des OGH wie auch des VwGH wird die IP-Adresse als Zugangsdatum und damit als Verkehrsdatum qualifiziert, wodurch sie in den Schutzbereich des Fernmelde- wie auch des Kommunikationsgeheimnisses fällt (vorgeschlagener § 92 Abs. 3 Z 16 TKG).

Der Entwurf sieht eine Trennung zwischen für betriebsnotwendige Zwecke und auf Vorrat gespeicherte Daten vor, für deren Speicherung besondere Sicherungsmaßnahmen vorgesehen sind. Die Kontrolle wird der Datenschutzkommission übertragen (vorgeschlagener § 102c Abs. 1 TKG). Jeder Zugriff auf Vorratsdaten ist zudem zu protokollieren (vorgeschlagener § 102c Abs. 2 und 3 TKG). Die Beauskunftung von Daten einer Nachrichtenübermittlung nach den Bestimmungen der StPO wie auch die Beauskunftung solcher Daten an die Sicherheitsbehörden hat verschlüsselt zu erfolgen (vorgeschlagener § 94 Abs. 4 TKG).

Schließlich sieht der Entwurf entsprechende neue Verwaltungsstraftatbestände vor (vorgeschlagener § 109 TKG).

(Schluss)

Rückfragehinweis: Susanna Enk Pressesprecherin Bundesministerium für Verkehr, Innovation und Technologie Tel.: +43 (0) 1 711 6265-8121 susanna.enk@bmvit.gv.at

Fundstelle: http://www.bmvit.gv.at/presse/aktuell/nvm/2009/20091120OTS0166/20091120OTS0166.html
Stand: 20.11.2009