Wirtschaft

120 Millionen Euro für Verbindungsdaten

Über Sinn und Unsinn der Speicherung von Verbindungsdaten der Telefonie und Internet wurde jahrelang diskutiert. Jetzt, wo die EU-Direktive umgesetzt werden soll, wird dagegen gewettert. Eines ist heute schon gewiss: Die Zeche zahlt der österreichische Kunde in Form von Steuern oder erhöhten Telekommunikationsgebühren.

Klaus Lackner

Die Justiz- und Innenminister der EU-Staaten sowie die EU-Kommission wollen die Telekom- und Internetanbieter verpflichten, die Verbindungsdaten der 450 Mio. Europäer bis zu vier Jahre zu speichern. Bis zu sechs Wochen nach Rechnungslegung sind die Unternehmen in Österreich derzeit verpflichtet, die Daten zu speichern.

Ziel der EU ist es, genau Protokoll zu führen, wer mit wem und wie lange über Festnetz-, Mobil- und Internet-Telefon kommuniziert hat, wer wem eine E-Mail geschickt hat, welche Websites ein Nutzer besucht hat. Außerdem soll, wie in Österreich bereits praktiziert, nachvollziehbar sein, wo Menschen mit ihren Mobiltelefonen unterwegs waren.

Überwachungsstaat perfekt

Nach ersten Schätzungen österreichischer Internet Provider wird diese Überwachung der Benutzer jährlich 80 bis 120 Mio. Euro kosten. Die Kosten werden Konsumenten und Steuerzahler zu tragen haben und entsprechen etwa einer 13. Monatsgebühr. Fest- und Mobiltelefonie erwarten zusätzliche Belastungen im mehrstelligen Millionenbereich.

Der Sinn der Sache, warum Telekomunternehmen und Internet Provider gezwungen werden, alle Verbindungsdaten ihrer Kunden auf Dauer aufzuzeichnen, ist ein simpler: Polizei und Geheimdienste in ganz Europa sollen Zugriff auf diese Daten bekommen. Als Speicherdauer sind bis zu vier Jahre vorgesehen, zwölf Monate aber realistisch.

Nicht einmal in den USA, wo als Folge der Anschläge vom 11. September 2001 Bürgerrechte zum Teil empfindlich eingeschränkt wurden, gibt es eine solche Speicherpflicht von Verbindungsdaten, neudeutsch „Data Retention“ genannt. Der US-Kongress hat entsprechende Gesetzesvorhaben mehrfach mit der Begründung abgelehnt, dass eine Vorratsdatenspeicherung zu weit in die Grundrechte eingreife. Doch nicht so in Europa, wo EU-Parlament und EU-Kommission bereits über die Bürgerköpfe hinweg entschieden haben. Vielen Menschen scheint auch gar nicht bewusst zu sein, welche Auswirkungen dies auf ihre persönliche Freiheit haben wird.

Sind die Daten einmal gespeichert, kann der Zweck von der in der EU-Direktive geforderten Verwendung gegen Terrorismus oder organisiertes Verbrechen schnell erweitert werden. In aktuellen Entwürfen ist bereits von einer Ausdehnung auf minderschwere Vergehen und Überwachung von Filesharing-Netzen – man erinnere sich an Napster – die Rede.

Telefonierer und Internetsurfer hinterlassen Spuren, die nach wenigen Wochen vernichtet werden. Jetzt wird der Spieß umgedreht: Bis zu vier Jahre soll gespeichert werden. Foto: economy

Fragliche Durchführbarkeit

In Österreich haben sich vor allem Arbeiterkammer, Wirtschaftskammer, Datenschützer und die Internet Service Provider Austria (Ispa) gegen dieses Vorhaben ausgesprochen. Als schlicht „undurchführbar“ bezeichnet Ispa-Präsident Georg Chytil die geplante Speicherung. Das österreichische Justizressort will die Daten maximal zwölf Monate speichern lassen. Die Anbieter von Speicherlösungen stehen schon bereit, um Provider mit Datenspeichern nachzurüsten. Sie wittern Millionenumsätze.

Doch auch die personellen Ressourcen der Provider müssten sich in diesem Bereich erhöhen. Friedrich Bock, Obmann des Fachverbandes Unternehmensberatung und Informationstechnologie (Ubit) der Wirtschaftskammer Österreich, erläutert: „Bislang fehlt verlässliches Datenmaterial, das die Folgen für die Unternehmen und den Nutzen evaluiert und die Notwendigkeit der Datenspeicherung auf Vorrat dokumentiert.“

Neben der technischen Machbarkeit geht es auch um das Grundrecht auf vertrauliche Kommunikation. Nun ist das Europaparlament am Zug. Denn die Speicherung personenbezogener Verbindungsdaten ist nach Artikel 8 der Europäischen Menschenrechtskonvention untersagt. Artikel 10a des Staatsgrundgesetzes sowie das Datenschutzgesetz 2000 stellen sicher, dass das Fernmeldegeheimnis nicht verletzt werden darf und Ausnahmen nur über richterliche Befehle zulässig sind.

„Die Sicherheit für die Bevölkerung und damit auch der vorbeugende Verbrechensschutz ist wichtig“, bekräftigt Daniela Zimmer, Konsumentenschutz-Expertin der Arbeiterkammer (AK). Doch potenzielle Straftäter würden mühelos Umgehungsmöglichkeiten, wie Telefonkarten, die über Mittelsmänner gekauft würden, oder öffentliche Telefonzellen oder Mailadressen, die verändert oder von Internetanbietern außerhalb der EU stammen würden, finden, so die AK-Expertin. „Letztendlich werden auch die Kosten einer Vorratsspeicherung den Konsumenten aufgebürdet werden“, warnen die Konsumentenschützer.

Florian Pollak, Unternehmenssprecher beim Mobilfunker One, zur derzeitigen Situation: „Wir haben bis jetzt noch nichts investiert. Doch einen Teil der geplanten Investitionen wird sicher die öffentliche Hand tragen. Es wird bald eine Diskussion mit dem Finanzministerium und dem Innenministerium bezüglich der Finanzierung geben. Wir wollen dabei unsere Partner, unsere Kunden, natürlich schützen.“