

Unsere Regierung dreht langsam durch

Beitrag von „darkdiver“ vom 16. November 2006 um 08:40

Vorratsdatenspeicherung soll auch für Anonymisierungsdienste gelten

Der jetzt komplett verfügbare Referentenentwurf zur Neuregelung der Telekommunikationsüberwachung, den Bundesjustizministerin Brigitte Zypries vergangene Woche in Grundzügen [vorgestellt hat](#), bittet deutsche Betreiber von Anonymisierungsservern zum umfassenden Datenprotokoll. Auch "wer einen Anonymisierungsdienst betreibt und hierbei die Ausgangskennung des Telekommunikationsnutzers durch eine andere ersetzt", betreibe einen Telekommunikationsdienst für die Öffentlichkeit und unterliege damit den gleichzeitig vorgeschlagenen Verpflichtungen zur verdachtsunabhängigen Speicherung von Verbindungsdaten für sechs Monate, heißt es in dem [Papier](#) (PDF-Datei), das die Humanistische Union online gestellt hat.

Für den [Arbeitskreis Vorratsdatenspeicherung](#) und sieben weitere Bürgerrechtsorganisation sind die Pläne ein weiteres Anzeichen dafür, dass die von Zypries vorangetriebene "Totalspeicherung der Telekommunikation der gesamten Bevölkerung vollkommen unverhältnismäßig" sei. Mit einer [Videobotschaft](#) an Bundeskanzlerin Angela Merkel, die auf einer [Demonstration gegen den Überwachungsstaat](#) in Bielefeld entstand, fordern sie einen Stopp der Umsetzung der [EU-Vorgaben zur Vorratspeicherung](#) von Kommunikationsdaten. Zuvor hatten Datenschützer [gehofft](#), dass etwa der vom Unabhängigen Landeszentrum für den Datenschutz Schleswig-Holstein (ULD) mitbetriebene Anonymisierungsdienst [AN.ON](#) als Teledienst gefasst und damit von den Verpflichtungen zur Datenjagd unberührt bleiben würde. Sie verwiesen darauf, dass sich in Verdachtsfällen der Verkehr von bestimmten IP-Adressen durch die Betreiber der AN.ON-Mixe bereits im Stil des "Quick Freeze"-Verfahrens aufbewahren lasse, bei dem Verbindungsdaten für einen aktuellen Anlass auf Zuruf der Strafverfolger archiviert werden.

Wie aus der Begründung des Referentenentwurfs hervorgeht, hält das Justizministerium das "Einfrieren" von Kommunikationsdaten generell für unzureichend. Es gehe "notwendig ins Leere", wenn die erwünschten "Verkehrsdaten" vom Diensteanbieter "überhaupt nicht gespeichert oder zwischenzeitlich bereits gelöscht wurden". Dies sei aufgrund der Verbreitung von Pauschaltarifen, bei denen Provider Verbindungsdaten für Abrechnungszwecke nicht benötigen und diese daher nach geltendem Recht [nicht speichern dürfen](#), immer häufiger der Fall. Der Entwurf räumt zwar ein, dass "Verkehrsdaten einen besonders schutzwürdigen Aussagegehalt haben, da sie im Einzelfall erhebliche Rückschlüsse auf das Kommunikations- und Bewegungsverhalten" der Nutzer zulassen würden. "Hinzu kommt, dass die Datenspeicherung unabhängig von einem im Einzelfall bestehenden Tatverdacht erfolgt und eine unbestimmte Vielzahl von Personen erfasst". Trotzdem überwiege das öffentliche Interesse "der Gewährleistung einer wirksamen Strafverfolgung". Zur Erfüllung dieses Auftrags leiste die

gesicherte Verfügbarkeit der umfassenden Nutzerspuren für die Ermittler einen "wichtigen", in einigen Deliktsbereichen wie der Aufklärung komplexer Täterstrukturen und bei "mittels Telekommunikation begangenen Straftaten" gar "unverzichtbaren Beitrag".

Insgesamt geht das Justizministerium davon aus, dass der insgesamt über 200 Seiten starke Entwurf keine Datensammlung "auf Vorrat zu unbestimmten oder noch nicht bestimmbar Zwecken" verlangt und daher mit der verfassungsrechtlichen Rechtsprechung vereinbar ist. Er legt unter anderem fest, dass es für Universitäten oder die Betreiber unternehmensinterner Netze keine Speicherpflicht gibt. Betont wird zudem, dass keine Inhaltsdaten etwa in Form von URLs erfasst werden dürfen. Dies könnte Provider bei der bislang von technischen Protokollen vorgesehenen Verknüpfung von Verbindungs- und Inhaltsdaten bei E-Mail aber [in die Bredouille bringen](#). Überhaupt sieht das Papier in einer Änderung von Paragraph 111 Telekommunikationsgesetz (TKG) vor, dass künftig auch die Anbieter von E-Mail-Konten Kundendaten erheben und ihre Nutzer so eindeutig identifizieren müssen. Die rasche Eröffnung eines Accounts ohne Vorlage eines Personalausweises bei einem deutschen Webmail-Dienst dürfte damit passé sein.

Darüber hinaus öffnet der Entwurf eine Hintertür zur Vorratsdatenspeicherung von erfolglosen oder unbeantwortet bleibenden Anrufen. Dazu wird den Anbietern zunächst etwa freigestellt, Abrechnungsdaten künftig sechs Monate lang vorzuhalten. Mit dem neuen Paragraph 110a TKG mit den Einzelregelungen über die bei der Vorratsdatenspeicherung zu erfassenden Nutzerspuren wird dann aber vorgeschrieben, dass die für diesen Zweck gespeicherten oder generell mitprotokollierten Daten über nicht zustande kommende Anrufe "auch nach Maßgabe dieser Vorschrift" aufbewahrt werden müssen. Dies gelte etwa auch für den Fall, dass ein Mobilfunkanbieter Kunden per SMS über einen Anrufversuch informiere. Bei der Standortdatenabfrage drängt der Entwurf Mobilfunkern zudem zu möglichst genauen Angaben. So sollen sie bei den zu speichernden Bezeichnungen von Funkzellen auch Daten vorhalten, "aus denen sich die geografische Lage" der jeweiligen Zelle sowie "die Hauptstrahlrichtung der Funkantennen ergibt".

Nicht ohne Brisanz ist auch die Ausgestaltung des deutlich aufgebohrten Paragraphen 100g Strafprozessordnung (StPO), der die "Erhebung" von Verkehrsdaten durch die Ermittler bei Straftaten regelt - und zwar teilweise in "Echtzeit", wie die Begründung ausführt und dabei etwa auf Auflagen aus der umstrittenen [Cybercrime-Konvention des Europarates](#) verweist. Zur Relativierung schlägt das Ministerium hier vor, dass bei der Aufklärung von Delikten von "im Einzelfall erheblicher Bedeutung" eine räumlich und zeitlich "hinreichend bestimmte Bezeichnung der Telekommunikation" genügt, wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre.

Bei "mittels Telekommunikation" begangener Straftaten soll die Datenabfrage ferner im Gegensatz zu schwerwiegenderen Fällen nur zulässig sein, wenn die Gesetzeshüter anderweitig nicht vorankommen "und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht". So möchte das Ministerium etwa verhindern, dass Strafverfolger schon bei einer reinen Beleidigung am Telefon auf die Datenhalden zugreifen. Bei [zivilrechtlichen Auskunftsansprüchen](#) etwa von Rechthaltern ist ebenfalls keine Datenabfrage vorgesehen. Gemäß Entwurf entfällt aber gleichzeitig die bisher in 100g enthaltene Formulierung, wonach Standortdaten nur "im Falle einer Verbindung" erhoben werden dürfen.

Dies mache die umstrittene Übersendung einer "[stillen SMS](#)" entbehrlich, da künftig eine Ortung auch dann möglich sei, wenn ein eingeschaltetes Mobiltelefon nicht aktuell genutzt werde.

Für heftige Auseinandersetzungen dürfte letztlich das Vorhaben zählen, der Wirtschaft trotz einer inzwischen [eingereichten Verfassungsbeschwerde](#) keine gesonderte Kostenerstattung für die Übernahme der neuen Hilfssheriff-Leistungen zu zahlen. Das Justizministerium geht zunächst sehr vage davon aus, dass die "Anzahl zusätzlicher entschädigungspflichtiger Auskunftersuchen zwischen 500 und 10.000 pro Jahr liegen wird". Dies ergebe nach dem vom [JVEG](#) vorgegebenen Stundensatz von maximal 17 Euro pro Auskunftersuchen ein zusätzliches Ausgabevolumen von 8500 bis 170.000 Euro pro Jahr. Den Aufwand der betroffenen Unternehmen für das Beantworten von Verkehrsdatenabfragen will der Entwurf damit abgegolten wissen.

Die "zur Erfüllung der Speicherungspflichten erforderlichen Investitionen" und gegebenenfalls gesteigerten Betriebskosten tut der Entwurf als Peanuts ab. Ein "großer deutscher Diensteanbieter" mit einem Jahresumsatz von annähernd 60 Milliarden Euro habe die Zusatzkosten auf 700.000 Euro pro Jahr beziffert, was 0,00116 Prozent der Einnahmen ausmache. Sollten die Provider diese Aufwendungen auf ihre Kunden "abwälzen" wollen, würde das Verbraucherpreisniveau wohl "allenfalls geringfügig steigen". Der Arbeitskreis Vorratsdatenspeicherung appelliert dagegen dafür, "die über 500 Millionen Euro, welche die geplante Totalprotokollierung Wirtschaft und Staat kosten würde", in ein Programm zur Kriminalitätsprävention vor Ort etwa an Schulen oder einzelnen Stadtteilen zu investieren.

Zur Auseinandersetzung um die Vorratsspeicherung sämtlicher Verbindungs- und Standortdaten, die etwa beim Telefonieren im Fest- oder Mobilfunknetz und der Internet-Nutzung anfallen, siehe den Online-Artikel in "[c't Hintergrund](#)" (mit Linkliste zu den wichtigsten Artikeln aus der Berichterstattung auf [heise online](#)):