DAS STASI-GESETZ

Was Fekter und Bandion mit der Vorratsdatenspeicherung wirklich planen

Details über den Regierungsanschlag auf die Internetfreiheit

in TKG, StPO und SPG

Seit Jahren ringt die österreichische Politik um die Umsetzung der Richtlinie zur Vorratsdatenspeicherung. Diese EU-Regelung sieht vor, dass Telekommunikationsanbieter sämtliche Verbindungsdaten (Telefonie, Internet, E-Mail, Standortdaten uvm) ihrer Kunden mindestens 6 Monate speichern müssen. Ziel ist den Strafverfolgungsbehörden den Zugriff auf diese Daten zu sichern, und zwar ausschließlich zur Bekämpfung schwerer Straftaten und Terrorismus.

Von Beginn an wurde die Richtlinie von MenschenrechtsexpertInnen scharf kritisiert. Die verdachtsunabhängige Speicherung der Kommunikationsdaten sämtlicher BürgerInnen stellt einen derart massiven Eingriff in deren Privatsphäre dar, dass die Verhältnismäßigkeit nicht mehr gegeben ist. Das umso mehr, als die Datenspeicherung mit minimalem Know-How leicht umgangen werden kann. Daneben bestehen auch zahlreiche Missbrauchsgefahren, von Datenklau bis zu übereifrigen Polizeibehörden.

Mittlerweile haben bereits vier Verfassungsgerichte europäischer Staaten (Deutschland, Rumänien, Bulgarien, Zypern) die nationalen Umsetzungsversuche der Richtlinien als verfassungswidrig aufgehoben. Der irische Supreme Court hat die sinnvollste Entscheidung gefällt, und den EuGH zur Überprüfung der Grundrechtskonformität der Richtlinie angerufen. Die Europäische Kommission hat im Herbst einen Evaluierungsprozess zur Richtlinie eingeleitet, dessen Ergebnisse Mitte März 2011 erwartet werden.

Österreich hat bisher die Richtlinie nicht umgesetzt und wurde dafür bereits einmal vom EuGH verurteilt (aus rein formalen Gründen ohne inhaltliche Prüfung). Jetzt drohen ein zweites Verfahren und die Verhängung von Strafgeldern.

In dieser Phase der europaweiten Rechtsunsicherheit startet nunmehr die Bundesregierung ihren neuesten Umsetzungsversuch. Statt die bisher ergangenen Erkenntnisse in Europa und die zahlreiche Kritik im Begutachtungsverfahren zu berücksichtigen, sollen nach dem Willen der Ministerinnen Fekter und Bandion-Ortner die Vorgaben der EU-Richtlinie sogar noch deutlich übertroffen werden. Wenn es nach BMI und BMJ geht, bekommt Österreich als erster Staat der EU ein Stasi-Gesetz.

Das Geheimpapier

Den Grünen liegt jenes streng geheime Verhandlungspapier vor, das vergangenen Dienstag in den Ministerrat kommen hätte sollen, dann aber noch einmal vertagt wurde.

Schon aus diesem Entwurf ergeben sich zahlreiche wesentliche Verschlechterungen gegenüber jener Fassung, die im Jahr 2010 vom BMVIT gemeinsam mit den ExpertInnen des Ludwig-Boltzmann-Institutes für Menschenrechte ausgearbeitet wurde.

Um nur einige der wesentlichsten Verschlechterungen zu nennen:

- Die Grenze der „schweren Straftat" soll bei nur einem Jahr Freiheitsstrafe als Höchststrafrahmen liegen – das hat mit dem Zweck der Richtlinie nichts mehr zu tun. Damit kann auf Vorratsdaten schon bei Ladendiebstahl oder Vermögensdelikten mit einem Schaden über 2000 Euro zugegriffen werden.

- Der Zugriff auf die wichtigsten Vorratsdaten soll ohne richterliche Genehmigung, nur auf Anordnung der Staatsanwaltschaft möglich sein. Damit wird die richterliche Kontrolle ausgeschaltet.

- Die 2007 überfallsartig eingeführten §53 Abs 3a und 3b SPG ermöglichten den Zugriff der Polizei auf IP-Adressen und Standortdaten bei „konkreter Gefahr". Da so die Polizei ohne richterliche Kontrolle und ohne Rechtsschutz das Internetverhalten ermitteln konnte, lag darin nach ExpertInnenmeinung ein verfassungswidriger Eingriff in das Fernmelde- und Kommunikationsgeheimnis. Diese Regelung wird jetzt auch im TKG bestätigt und soll so rechtlich abgesichert werden. Die im Boltzmann-Entwurf vorgesehene Beschränkung auf den Schutz von Leben und Gesundheit wurde gestrichen.

- Die Polizei soll im Rahmen des § 53 Abs 3a und 3b SPG sogar Zugriff auf Vorratsdaten der letzten drei Monate erhalten. Die Erläuterungen zum Entwurf gestehen selbst ein, dass eine derartige Nutzung der Vorratsdaten für „präventive Zwecke" wegen der massiven Missbrauchsgefahr (Beispiel: Tierschützer, Kunststudenten und andere Opfer der §§ 278a und 278b) sogar auf europäischer Ebene als zu gefährlich abgelehnt wurde. Damit hat die Polizei zum ersten Mal auf sämtliche E-Mail-Verbindungsdaten Zugriff. Die Polizei kann so die gesamten E-Mail-Verbindungen ohne richterlichen Befehl überwachen.

- Die vom Boltzmann-Institut vorgesehene verpflichtende Verständigung Betroffener entfällt. Wer nicht weiß, dass er überwacht wurde, kann sich aber auch nicht wehren. Nur bei der Nutzung von Standortdaten („Bergsteigerfall") wird das Versenden einer SMS zugestanden.

- Bei Anfragen wegen Stammdaten (Name, Adresse, aber auch Bonität) entfällt die Begründungspflicht für Polizei und Staatsanwälte, bei Gefahr in Verzug sollen solche Anfragen sogar mündlich möglich sein (und werden damit de facto unüberprüfbar).

Der Stasi-Plan der ÖVP

Doch selbst diese Umsetzungsvariante, die weit über die Anforderungen der Richtlinie hinausgeht, ist für Innenministerin und Justizministerin noch nicht genug. Die ÖVP ließ den Beschluss daher platzen.

Aus einem den Grünen vorliegenden Zwischenbericht zu den koalitionsinternen Verhandlungen ergeben sich folgende weiteren Wünsche der beiden ÖVP-Ministerinnen:

- Das BMI fordert Datenauskünfte an die Polizei, wenn nur die „Gefahr besteht, dass jemand eine Straftat begeht." Das ist die generelle Überwachungsermächtigung.
- Das BMI fordert den uneingeschränkten Zugang der Polizei zu den IP-Adressen.
- Das BMI fordert diesen Zugang ohne Ermächtigung oder nachträgliche Kontrolle durch den Rechtsschutzbeauftragten, ohne Information der Betroffenen und ohne Beschränkung auf bestimmte Rechtsgüter (zB Leben und Gesundheit) – also die Ausschaltung des Rechtsschutzes.
- Das BMJ fordert, dass das Erfordernis der „schweren Straftat" für den Zugriff auf Vorratsdaten überhaupt entfällt. Die Umsetzung ginge damit weit über den von der EU-Richtlinie vorgegebenen Rahmen hinaus.
- Das BMJ fordert, dass Vorratsdaten auch für sämtliche Zivilprozesse von Urheberrechtsprozessen bis hin zu Ehestreitigkeiten verwendet werden sollen.

Mit der Umsetzung dieser Forderungen wären die schlimmsten Befürchtungen aller Kritiker der Vorratsdatenspeicherung bestätigt. Die Polizei könnte völlig unkontrolliert Internetverhalten und Beziehungsnetzwerke beliebiger BürgerInnen überwachen. Wer Kontakt zu Verdächtigen hat, wird selbst verdächtig. Die Musikindustrie kann massenhaft Filesharer verklagen oder abmahnen, Ehegatten können das Internetverhalten ihrer Partner gerichtlich aufklären lassen, und kritische VertreterInnen der Zivilgesellschaft und JournalistInnen können "präventiv" von der Polizei ohne Richter, ohne Rechtsschutz und ohne Information der Betroffenen überwacht werden.

Exkurs: Wieso der Schutz von IP-Adressen wichtig ist

Die Vorratsdatenrichtlinie betrifft prinzipiell nicht Inhaltsdaten sondern Verkehrsdaten. Es wird damit also grundsätzlich nicht der Inhalt einer Kommunikation überwacht. Dafür sehen die Gesetze – noch – deutlich höhere Schranken vor, insbesondere die gerichtliche Genehmigung durch Richter im Einzelfall.

Mit Hilfe der Aufschlüsselung der einzelnen Usern zugewiesenen IP-Adressen sind jedoch unmittelbare Rückschlüsse eben auf den Inhalt der Kommunikation möglich. Die Versender bestimmter E-Mails werden nachvollziehbar, und durch Abgleich mit den Besuchsprotokollen von Webseiten wird auch das Surfverhalten nachvollziehbar. Der Zugriff auf die Namen hinter den IP-Adressen stellt daher einen Eingriff dar, der einer Inhaltsüberwachung gleich kommt, und müsste daher den selben Schutzvorschriften unterliegen. Davon kann jedoch nach den derzeitigen Plänen keine Rede mehr sein.

Ein weiteres Problem ergibt sich aus der fehlenden Zeitsynchronisation der Server im Internet: Da dynamische IP-Adressen mit jeder Internetnutzung von Usern neu vergeben werden, können unterschiedlich eingestellte Uhren der diversen Betreiber in vielen Fällen zu Falschauskünften und damit unbegründeten Verdachtslagen führen.