Trotz umstrittenen Massnahmen nur wenig Kritik

28. Februar 2014

Der Bundesrat will die Telefon- und Internetüberwachung der technologischen Entwicklung anpassen. Kritiker sehen darin einen Angriff auf die Grundrechte. Auch bei den Dienstanbietern regt sich Widerstand.

Jan Flückiger, NZZ

Bisher war es erstaunlich still um die anstehende Gesetzesrevision. Dabei geht es um eine grundlegende Frage: Wie stark darf der Staat im Namen der Sicherheit in die Privatsphäre unbescholtener Bürger eindringen? In der Märzsession wird sich der Ständerat mit dieser Frage beschäftigen, wenn er die Revision des Bundesgesetzes über die Überwachung des Post- und Fernmeldeverkehrs (Büpf) behandelt.

Ziel der Revision ist gemäss Bundesrat, das Gesetz an die technologische Entwicklung der letzten Jahre anzupassen und dabei, soweit möglich, auch künftigen Entwicklungen Rechnung zu tragen. Tatsächlich hat sich die Welt der Telekommunikation in den letzten Jahrzehnten rasant entwickelt. Kommuniziert wird nicht mehr nur über Post, Telefon und E-Mail, sondern beispielsweise auch via verschlüsselte Dienste im Internet. Auch Straftäter nutzen diese Technologien. Die Strafverfolgungsbehörden haben jedoch heute keine Möglichkeit, diese zu überwachen.

Nur mit Gerichtsbeschluss

Die grundsätzliche Notwendigkeit einer Gesetzesrevision wird denn auch kaum bestritten. Zumal Überwachungen weiterhin nur in einem laufenden Strafverfahren angeordnet werden können. Dazu braucht es einen begründeten Antrag der Staatsanwaltschaft sowie einen richterlichen Beschluss. Ausnahmen sind die Fahndung nach einer vermissten Person sowie neu die Fahndung nach einem flüchtigen Straftäter, gegen den eine Freiheitsstrafe verhängt wurde.

Dennoch geben diverse Punkte des Gesetzesentwurfs Anlass zur Kritik, vor allem vonseiten der betroffenen Anbieter von Telekommunikations-Dienstleistungen (Provider) und von Organisationen, welche die Einschränkung der Grundrechte befürchten. Konkret sind vor allem folgende Punkte umstritten: die Verlängerung der Vorratsdatenspeicherung, die Einführung von Bundestrojanern sowie die Ausweitung der Mitwirkungspflicht.

Zur Vorratsdatenspeicherung: Bereits heute werden Verbindungsdaten beispielsweise von Mobiltelefonen gespeichert und müssen von den Providern mindestens sechs Monate aufbewahrt und auf Ersuchen der Behörden ausgehändigt werden. Aus diesen Daten wird ersichtlich, wer wann wie lang mit wem telefoniert hat. Nicht gespeichert werden die Inhalte, also die Gespräche selber. Neu sollen die Daten den Behörden 12 Monate statt 6 Monate rückwirkend zur Verfügung stehen. Die Provider befürchten einen höheren Aufwand, da die Aufbewahrung der Daten teuren Speicherplatz beansprucht.

Sämtliche Nutzer erfasst

Organisationen wie etwa der Verein «Digitale Gesellschaft» kritisieren die Vorratsdatenspeicherung grundsätzlich, weil damit die Daten sämtlicher Nutzer gespeichert werden, unabhängig davon, ob gegen jemanden eine Ermittlung läuft oder nicht. Das sei ein schwerer Eingriff in die persönliche Freiheit. Zudem sei unklar, wieso die heutige Aufbewahrungsfrist von 6 Monaten nicht reiche. In der Botschaft des Bundesrates heisst es, die Erfahrungen der Strafverfolger hätten gezeigt, dass die Frist zu kurz sei. Oft sei sie bereits abgelaufen, wenn die Behörden in der Lage seien, eine Überwachung anzuordnen.

Ebenfalls stark umstritten sind die sogenannten Bundestrojaner; im Gesetz werden sie als «GovWare» bezeichnet. Mit dieser Software können die Ermittler in fremde Computer eindringen (allerdings bei einem eingeschränkten Katalog von Delikten). Dies sei nötig, um beispielsweise Telefongespräche abzuhören, die via verschlüsselte Dienste wie Skype geführt würden, so der Bundesrat. Die Trojaner bergen aber diverse Risiken, was der Bundesrat in seiner Botschaft auch nicht verhehlt. So sei es aus Sicht von Fachleuten nicht möglich, «GovWare» zu betreiben, «die unter allen Umständen korrekt funktioniert und keinen Einfluss auf andere Programme und Funktionen hat». Unter anderem bestehe die Gefahr, dass bei der Einschleusung des Trojaners Sicherheitslücken im Ziel-Computer entstünden, welche dann von Dritten genutzt werden könnten, um ebenfalls in den Computer einzudringen.

Gefahr des Missbrauchs

Den Ermittlern wird durch den Trojaner ermöglicht, auf sämtliche Daten des überwachten Computers zuzugreifen, also auch auf private Dokumente, Fotos und so weiter. Zwar verbietet das Gesetz den Ermittlern die Verwendung dieser Daten vor Gericht, doch gesammelt werden können sie trotzdem. Aus Sicht der Kritiker besteht deshalb ein erhebliches Missbrauchspotenzial.

Beim federführenden Bundesamt für Justiz (BJ) heisst es, man sei sich bewusst, dass die «GovWare» kein einfaches Instrument sei. Sie dürfe deshalb nur eingesetzt werden, wenn dies «technisch sauber» möglich sei und die Software die rechtlichen Vorgaben erfülle. Sämtliche gesammelten Daten, die nichts mit Telekommunikation zu tun hätten, müssten sofort gelöscht werden.

Nach geltendem Recht sind vom Büpf nur die Anbieter von Post- oder Fernmeldediensten betroffen, zu denen auch die Anbieter für den Internetzugang gehören, sowie die Betreiber von internen Fernmeldenetzen und Hauszentralen. Neu sollen auch die Anbieter von «abgeleiteten Kommunikationsdiensten» (etwa reine E-Mail-Provider) sowie Personen, die ihren Internetzugang Dritten zur Verfügung stellen (etwa Internet-Cafés oder Hotels, aber auch Private), zu den sogenannten Mitwirkungspflichtigen gehören.

Kritiker befürchten einen massiven Aufwand, gerade für private Betreiber von E-Mail-Diensten oder Foren und stellen die Verhältnismässigkeit infrage. Zumal ausgerechnet die grossen E-Mail-Provider dem ausländischen Gesetz unterstünden und nicht behaftet werden könnten. Das BJ relativiert: Der Bundesrat habe die Möglichkeit, kleinere Anbieter von gewissen Pflichten zu befreien. Der Geltungsbereich des Gesetzes werde im Vergleich zu heute nicht wesentlich ausgebaut.

Referendum angekündigt

Interessant ist, dass in der ständerätlichen Rechtskommission zu all diesen grundsätzlichen

Fragen praktisch keine Diskussion stattfand. Es gab einzig einen Minderheitsantrag, die Aufbewahrungsdauer für Verbindungsdaten auf 8 Monate zu beschränken. Und die Kommission hat die Entschädigung für die Provider gestrichen, welche deren Aufwand für die Überwachung zumindest teilweise abgilt (im letzten Jahr waren dies rund 10 Millionen Franken). Halten die Räte an diesem Antrag fest, hätte dies zweierlei zur Folge: Erstens hätten die Konsumenten künftig diese Kosten zu tragen. Zweitens wird befürchtet, dass die Behörden häufiger zum Mittel der Überwachung greifen könnten, wenn diese weniger kostet.

Auch ein Grund, wieso die Vorlage im Ständerat zumindest vorerst noch für keine Grundsatzdebatte gesorgt hat, könnte sein, dass sich die Ständeräte primär als Kantonsvertreter verstehen und deshalb die Position der Strafverfolgungsbehörden vertreten. Im Nationalrat dürfte die Gesetzesrevision für mehr Diskussionen sorgen.

Sollte es keine wesentlichen Anpassungen mehr geben, dann droht das Referendum. Dies haben sowohl Branchenvertreter wie auch diverse politische Organisationen, etwa die Grünen oder die Piratenpartei, angekündigt.

Mehr Überwachungen

Im Jahr 2013 wurden von den Strafverfolgungsbehörden 3945 Echtzeitüberwachungen angeordnet, 22 Prozent mehr als im Vorjahr. Anfragen für rückwirkende Verbindungsnachweise gab es 6915 (minus 0,6 Prozent). Dazu kamen 125 Antennensuchläufe (Rasterfahndung) und 5155 technisch-administrative Auskunftsbegehren zu Anschlüssen und Teilnehmern. Die aufzuklärenden Delikte betrafen zu je einem Drittel schwere Widerhandlungen gegen das Betäubungsmittelgesetz, schwere Vermögensdelikte sowie diverse andere Delikte. Für die Massnahmen entrichteten die Strafverfolgungsbehörden 14,7 Millionen Franken Gebühren.