Brief der Digitalen Gesellschaft an die Mitglieder der Rechtskommission SR bezüglich der BÜPF Revision

21. April 2013

Ausweitung des Geltungsbereichs

Bisher beschränkte sich die Mitwirkungspflicht bei der Durchführung von Überwachungsmassnahmen auf die Post- und Fernmeldedienstanbieter. Die Ausweitung auf Gewerbebetriebe wie Hotels oder Internet-Cafés und insbesondere auf die sehr offen formulierte Kategorie von «Anbieterinnen abgeleiteter Kommunikationsdienste» bürdet einer grossen Anzahl von (Privat-) Personen und Organisationen Pflichten auf, denen diese nicht nachkommen können. Die Kompetenz, den maximalen Geltungsbereich einzugrenzen, wird dem Gesetzgeber entzogen und dem Bundesrat übertragen.

Angesichts der Tatsache, dass etliche der populären Anbieter wie GMX oder WhatsApp weder Geschäftssitz noch Infrastruktur in der Schweiz haben und deshalb nach wie vor nicht zur Mitwirkung verpflichtet werden können, ist diese Verschärfung noch weniger nachvollziehbar.

Ausbau der verdachtsunabhängigen Vorratsdatenspeicherung

Die verdachtsunabhängige Speicherung der Randdaten sämtlicher Telekommunikationsteilnehmer stellt einen unzulässigen Eingriff in das verfassungsmässig garantierte Fernmeldegeheimnis dar, insbesondere wird während eines grossen Zeitraums aufgezeichnet, wer wann mit wem wie lange kommuniziert hat. In der Botschaft des Bundesrats zum neuen BÜPF steht einzig, dass die Vorratsdatenspeicherung "zur Bekämpfung der Kriminalität unerlässlich" sei. Allerdings wird diese Aussage nicht weiter begründet. Vergleicht man die Aufklärungsrate der schweizerischen Polizei mit derjenigen, der deutschen (wo die Vorratsdatenspeicherung nicht zulässig ist), sind allerdings keine Unterschiede ersichtlich.

Die Verlängerung der Aufbewahrungsfrist ist nicht zielführend und deshalb unnötig.

Einsatz von GovWare

Der Einsatz von Spionage-Software soll erlaubt werden, um den Inhalt von Kommunikation und Randdaten in unverschlüsselter Form abzufangen, falls dies nicht anders möglich ist. Das Gesetz rechnet bereits damit, dass die eingesetzte Software über weiterreichende Funktionen verfügt und schreibt daher vor, dass gesammelte Daten, die nicht zu den erwähnten Kategorien gehören, sofort gelöscht werden müssen. Erkenntnisse, die auf solchen Daten beruhen, sollen nicht verwendet werden dürfen. Es ist

schwer vorstellbar, wie ermittelnde Personen den Verstoss gegen diese Vorschrift vermeiden sollen.

Das Einschleusen von GovWare via Internet ist mit erheblichen technischem Aufwand verbunden, da Schutzmechanismen auf dem Zielgerät umgangen werden müssen. Gelingt es

die Software zu installieren, beeinträchtigt deren Betrieb die Sicherheit des Systems und stellt daher die Integrität der potentiellen Beweise infrage. Der technische Fortschritt kann diesen Widerspruch nicht auflösen.

Das Gesetz erlaubt den Einsatz von Spionage-Software bereits bei relativ geringen Delikten wie Diebstahl und schwerer Sachbeschädigung.

Risiken und Nutzen stehen beim Einsatz von GovWare in keinem Verhältnis, und daher ist von einer Legalisierung dieses Mittels abzusehen.

Anders als in der Botschaft versprochen, wird mit der vorgeschlagenen Revision die Überwachung tatsächlich stark ausgeweitet. Wurde bis anhin bei den Post- und Fernmeldedienstanbieter angesetzt, sollen nun beide Enden der Kommunikation mit einbezogen werden: Auf dem Benutzer-Computer per GovWare und auf der Server-Seite durch Ausweitung des Geltungsbereichs auf sämtliche Diensteanbieter. Zusätzlich soll die Dauer der Vorratsdatenspeicherung verdoppelt werden.

Staatstrojaner und uferlose Internet-Überwachung