Mehr Überwachung im Strafprozess

3. Februar 2014

Viktor Györffy**,** plädoyer 1/14

Grundrechte · Der Bundesrat will die Überwachung des Post- und Fernmeldeverkehrs massiv ausdehnen. Mit dem Zugriff auf die digitalen Daten drohen schwere Eingriffe in die Grundrechte. Und das Missbrauchpotenzial steigt.

Das Bundesgesetz betreffend Überwachung des Post- und Fernmeldeverkehrs - kurz Büpf - soll totalrevidiert werden. Gemäss der Botschaft des Bundesrats vom 27. Februar 2013 will man sicherstellen, dass die Überwachungen nicht durch neue Kommunikationsformen verhindert werden. Gesetz und Strafprozessordnung (StPO) sollen deshalb an die technische Entwicklung angepasst werden.

Der Bundesrat sagt, das Ziel bestehe darin, nicht mehr, sondern besser zu überwachen. Im Ergebnis führt die Vorlage jedoch zu einer deutlichen Erweiterung: Der Anwendungsbereich des Gesetzes wird massiv ausgedehnt, die Daten sollen länger gespeichert und die technischen Überwachungsmöglichkeiten ausgebaut werden. Der Ständerat hat die Änderung am 19.März mit 30 zu 2 Stimmen bei 4 Enthaltungen angenommen. Im Juni wird der Nationalrat darüber befinden.

Ausdehnung des Anwendungsbereichs

Heute erfasst das Büpf die Anbieter von Post- und Fernmeldediensten und die Internet-Access-Provider. Mit der Revision nimmt der Bundesrat weitere ins Visier:

- Anbieter von Post- und Kurierdiensten
- Anbieter von Fernmeldediensten (Telefon, Internetzugang)
- Anbieter von Diensten, die sich auf Fernmeldedienste stützen (E-Mail, Hosting, Cloud-Dienste, Chats, Foren) inklusive Private oder Vereine, die einen solchen Dienst anbieten Betreiber unternehmensinterner Fernmeldenetze (Intranets)
-

Personen, die ihren Netzzugang Dritten zur Verfügung stellen, wie Hotels, Internet-Cafés, Spitäler, Schulen; gemäss Botschaft fällt darunter auch eine Privatperson, deren Zugang Dritten absichtlich oder unabsichtlich offensteht

- professionelle Wiederverkäufer von Prepaid-Karten und ähnlichen Diensten, die den Zugang zu einem öffentlichen Fernmeldenetz ermöglichen.

Die Mitwirkungspflichten werden für jede Kategorie gesondert definiert. Das Gesetz regelt die Grundzüge, im Detail legt der Bundesrat die Pflichten per Verordnung fest. Die Mitwirkungspflicht kann darin bestehen, dass ein Anbieter bestimmte Daten für die Überwachung abliefern muss. Neu ist vorgesehen, dass ein Anbieter die Daten nicht selber erfassen und liefern, sondern stattdessen dulden muss, dass der Dienst eine Überwachung bei ihm durchführt. Und: Auf Verlangen müssen Anbieter jederzeit ausführlich über ihre aktuellen und innert sechs Monaten geplanten Dienstleistungen informieren. Das entspricht der Stossrichtung des Entwurfs: Jede elektronische Kommunikation soll unabhängig von der verwendeten Technologie umfassend überwachbar werden. Die Ausdehnung des Geltungsbereichs würde im Ergebnis sehr viele Anbieter treffen. Die Botschaft geht von heute rund 50 neu auf bis zu 200 Unternehmen aus. Effektiv würden aber unübersehbar viele Firmen und Privatpersonen erfasst.

Längere Speicherung der Vorratsdaten

Der Bundesrat schlägt in seinem Entwurf weiter vor, die Aufbewahrungsfrist für die sogenannten Randdaten (Vorratsdaten) von sechs auf zwölf Monate zu verlängern. Dazu muss man wissen: Viele europäische Staaten praktizieren bis heute diese Vorratsdatenspeicherung nicht. EU-Staaten sind zwar aufgrund einer entsprechenden Richtlinie verpflichtet, sie einzuführen. In Deutschland, Rumänien und Tschechien hoben die Verfassungsgerichte die jeweiligen Gesetze jedoch auf. Auch der Europäische Gerichtshof befasst sich zurzeit mit dieser EU-Richtlinie. Der Generalanwalt hat in diesem

Verfahren ein Gutachten vorgelegt, wonach die Vorratsdatenspeicherung grundrechtswidrig ist. Die Vorratsdaten umfassen keine Kommunikationsinhalte, sondern Metadaten. Diese lassen weitreichende Schlüsse zu. Sie zeigen Verbindungen zwischen Personen auf, können Hinweise auf den Inhalt der ausgetauschten Daten geben und sind sehr oft mit Standortdaten versehen. Überdies lassen sich die Vorratsdaten mit weiteren Beweismitteln und Daten verknüpfen, etwa solchen, die aus einem sichergestellten Gerät ausgelesen oder von einem Provider herausverlangt werden. Nicht zu unterschätzen sind auch die Möglichkeiten der computergestützten Analyse von Daten.

Bedarf der Strafverfolger nicht belegt

Angesichts der im Raum stehenden grundsätzlichen Bedenken gegenüber der Vorratsdatenspeicherung wäre vom Bundesrat überzeugend zu begründen, weshalb die Dauer der Aufbewahrung auf zwölf Monate ausgedehnt werden soll. In der Botschaft wird bloss ausgeführt, die Erfahrungen der Strafverfolgungsbehörden hätten gezeigt, dass die geltende Aufbewahrungsfrist von sechs Monaten zu kurz bemessen sei. Oft sei diese Frist bereits abgelaufen, wenn die Behörde in der Lage sei, eine Überwachung anzuordnen. Ein Blick in die vom Dienst Überwachung Post- und Fernmeldeverkehr geführten Statistiken bestätigt dies

jedoch nicht, im Gegenteil: Die Strafverfolgungsbehörden benötigen in den meisten Fällen nur kürzlich angefallene Daten. Hinzu kommt, dass in der Schweiz kein aussagekräftiges statistisches Material zur Verfügung steht, das die Effektivität der Vorratsdatenspeicherung in der Strafverfolgung belegt. In Deutschland liegen Untersuchungen des Max-Planck-Instituts für internationales Strafrecht vor. In einem Gutachten von 2011 gelangt das Institut zum Schluss, dass sich kein Zusammenhang zwischen Vorratsdatenspeicherung und Aufklärungsquote belegen lässt. Die Verlängerung der Aufbewahrungsfrist erscheint somit zur wirksamen Bekämpfung der Kriminalität nicht notwendig. Die rechtlichen Auseinandersetzungen um die Vorratsdatenspeicherung in der EU zeigen, dass die Überlegungen in eine ganz andere Richtung gehen müssten: Die (langfristige) Speicherung der Metadaten aller Personen müsste aufgegeben und durch ein anderes, mit den Grundrechten verträgliches Verfahren ersetzt werden, bei dem die Strafverfolgungsbehörden primär zeitnahe Daten anfordern.

Ausdehnung der Überwachung

Neu soll der Einsatz besonderer technischer Geräte angeordnet werden können, um Gespräche mitzuhören oder aufzunehmen oder eine Person oder Sache zu identifizieren oder deren Standort zu ermitteln (neuer Artikel 269bis StPO). Dabei geht es laut Botschaft namentlich um den Einsatz von Überwachungsgeräten wie IMSI-Catchern. Ein IMSI-Catcher schiebt sich im Handynetz zwischen die Mobiltelefone in der Umgebung und das eigentliche Mobilfunknetz. Er ermöglicht die sofortige Identifizierung der Netzteilnehmer, die Erstellung eines Bewegungsprofils und das Mithören von Handyanrufen.

Der Einsatz solcher Geräte ist nicht grundrechtsverträglich. Klar wird dies, wenn man sich eine gesetzliche Norm vorstellt, die es der Polizei erlauben würde, auf einen Schlag die Identität aller Personen, die sich in einem bestimmten Gebiet aufhalten, zu kontrollieren und alle Namen zu protokollieren. Nachdem heute fast jede Person ein Handy auf sich trägt, läuft der Einsatz des IMSI-Catchers auf eine solche flächendeckende Personenkontrolle in einem bestimmten Umkreis hinaus - ohne dass es die Betroffenen merken.

Neu vorgesehen ist in der StPO (neuer Art. 269ter) auch der Einsatz von sogenannten Staatstrojanern durch die Strafverfolgungsbehörden. Dabei handelt es sich um Informatikprogramme zur Überwachung des Fernmeldeverkehrs. Eingesetzt würden diese Trojaner im Rahmen des bereits heute weit gefassten Deliktskataloges für Überwachungsmassnahmen. Die Polizei schleust dabei unbemerkt einen Trojaner auf Computer, Tablet, Smartphone, Festnetztelefon oder andere Datenverarbeitungssysteme. Zum Einsatz kommen soll diese Methode namentlich, wenn Kommunikation anders nicht abgehört werden könnte, weil sie verschlüsselt erfolgt oder über ein tragbares Gerät, das verschiedene Übertragungskanäle nutzt, etwa mehrere SIM-Karten.

Der Einsatz eines Trojaners ist ein äusserst schwerwiegender Eingriff. Er setzt voraus, dass sich die Polizei heimlich physisch oder über das Netz Zugriff zum betroffenen Gerät verschafft und einen massgeschneiderten Trojaner platziert. Die Einschränkung auf den vorgesehenen Zweck - etwa den Mitschnitt eines Chats oder eines Skype-Telefonats - liesse sich nicht gewährleisten. Um zu beurteilen, was konkret überwacht werden soll, müssten die Ein- und Ausgabegeräte wie Tastatur, Bildschirm, Mikrofon und Kamera ständig überwacht werden. Zapft man Kamera und Mikrofon an, werden sie zur Wanze, die Überwachung weitet sich automatisch auf den umliegenden Raum aus.

Die Botschaft führt aus, der Trojaner müsse so konfiguriert werden, dass er nur die Beschaffung von Fernmeldeverkehrsdaten ermöglicht, sodass kein Zugang zu sämtlichen Daten besteht, die im betreffenden Computer enthalten sind. Damit soll die Online-Durchsuchung dieses

Computers ausgeschlossen werden. Das ist in der Realität gar nicht umsetzbar. Ein Trojaner kann so programmiert werden, dass er alle Daten auf einem Gerät einsieht, und er kann während des Einsatzes verändert werden. Grundsätzlich ist das intendiert: Die Botschaft legt dar, dass sich die laufende Überwachung gegebenenfalls auf andere Arten von Daten ausweiten könne. Dabei besteht ein grosses Missbrauchspotenzial. Kommt hinzu: Der Trojaner kann das Beweismittel - das Gerät oder die Daten darauf - manipulieren. Damit wird eine verlässliche Dokumentation des Einsatzes und die Überprüfbarkeit der Daten unterminiert.

Keine überzeugenden Argumente

Bereits die heute vorgesehenen Überwachungsmassnahmen sehen eine Reihe schwerer Eingriffe in die Grundrechte vor. Tangiert sind etwa das Recht auf Achtung des Intim-, Privat- und Familienlebens und das Recht auf Schutz vor Missbrauch der persönlichen Daten und die informationelle Selbstbestimmung. Die weit verbreitete Nutzung elektronischer Kommunikationsgeräte ermöglicht schon nach geltendem Recht sehr weitgehende Überwachungen. Diese Grundrechtseingriffe würden durch die Büpf-Revision deutlich verstärkt.

Gewichtige Gründe für eine Ausweitung der Überwachung sind nicht festzustellen.Nicht zugkräftig ist insbesondere das Argument, die Möglichkeiten elektronischer Kommunikation würden auch von Kriminellen genutzt. Kriminelle sitzen mitunter auch in einem Restaurant oder auf einer Parkbank und tauschen sich aus. Mit derselben Argumentation könnte man die flächendeckende Überwachung von Restaurants und Parks fordern. So betrachtet entspringt der Revisionsvorschlag nicht einer Notwendigkeit, sondern dem Gedanken der Machbarkeit: Die Daten fallen an, also sichert man sich den Zugriff darauf.