Allmächtiger Staat, rechtlose Bürger

23. November 2015

erweiterte Fassung des in plädoyer 06/2015 erschienen Artikels

von Viktor Györffy und Christof Hugentobler

Geheimdienst · Das Parlament hat im September ein neues Nachrichtendienstgesetz beschlossen. Damit erhält der Geheimdienst viele neue Kompetenzen. Das Gesetz verletzt die verfassungsmässigen Grundrechte der Bevölkerung.

Das neue Nachrichtendienstgesetz (NDG) soll Gesetzesgrundlage für die Aktivitäten des Geheimdienstes schaffen. Kernstück ist die Neuausrichtung der Informationsbeschaffung.

Dabei ist eine Reihe schwerer Eingriffe in die Grundrechte vorgesehen. Tangiert sind etwa das Recht auf Achtung des Intim-, Privat- und Familienlebens, das Recht auf Schutz vor Missbrauch der persönlichen Daten und die informationelle Selbstbestimmung. Je nachdem, wer betroffen ist, können auch weitere Rechte tangiert sein, etwa die Rechte von Journalisten, insbesondere auf Quellenschutz, sowie das Berufsgeheimnis von Ärzten, Rechtsanwälten und Geistlichen. Viele der vorgesehenen Massnahmen zielen auf die Überwachung von Kommunikation über elektronische Kanäle bzw. auf das Abfischen elektronischer Daten. Ein Aspekt der Grundrechtseingriffe besteht darin, dass diese geeignet sind, das eigene Verhalten so zu verändern, dass man von seinen Grundrechten nurmehr beschränkt Gebrauch macht, sich also beispielsweise in der Kommunikation einschränkt und über gewisse Themen nicht mehr informiert («Chilling effect»).

Aus grundrechtlicher Perspektive stechen besonders die genehmigungspflichtigen Beschaffungsmassnahmen (Art. 26) hervor, welche den harten Kern der Überwachungsmassnahmen beinhalten:

- Überwachung des Post-und Fernmeldeverkehrs nach dem BÜPF
- Einsatz von Ortungsgeräten (GPS) zur Feststellung des Standorts und der Bewegungen von Personen oder Sachen
- Einsatz von technischen Überwachungsgeräten wie Wanzen und Kameras im privaten Bereich
-

Einsatz von Staatstrojanern zur Informationsbeschaffung

- Cyberangriffe zur Abwehr von Cyberangriffen auf kritische Infrastrukturen

- Durchsuchen von Räumlichkeiten, Fahrzeugen oder Behältnissen zur Beschaffung von Gegenständen oder Informationen.

Derartige Überwachungsmassnahmen sind nach geltendem Recht - soweit sie überhaupt zulässig sind - den Strafverfolgungsbehörden vorbehalten. Neu soll auch der Geheimdienst auf sie zugreifen dürfen. Im Strafverfahren setzen solche Massnahmen einen hinreichenden Tatverdacht auf eine genügend schwere Straftat voraus und unterstehen strafprozessualen Garantien. Die betroffene Person wird früher oder später aktiv ins Strafverfahren involviert und kann ihren Standpunkt darlegen. All dies fehlt im Geheimdienstbereich. Als Basis geheimdienstlicher Tätigkeit reichen vage Vermutungen und dubiose Quellen. Es bedarf keines Verdachts auf Begehung einer Straftat. Wirksame Verfahrensrechte hat die betroffene Person nicht.

Ein immer grösserer Teil des Lebens und der Kommunikation läuft über digitale Kanäle oder bildet sich in der digitalen Welt ab. Mit der Überwachung der entsprechenden Daten kann eruiert werden, worüber wer wann mit wem kommuniziert und worüber man sich informiert. Mit der Überwachung mobiler Geräte können Bewegungsprofile erstellt werden. Weil wir immer mehr Datenspuren hinterlassen und die Daten immer ausgeklügelter ausgewertet werden können, ist die Eingriffswirkung solcher Massnahmen im Verlauf der letzten Jahre enorm gestiegen und wird in Zukunft wohl weiter zunehmen.

Die Daten lassen weitreichende Schlüsse zu

Die Überwachung des Post- und Fernmeldeverkehrs umfasst auch die Vorratsdaten, die laut BÜPF während sechs Monaten zu speichern sind. Dabei handelt es sich nicht um Kommunikationsinhalte, sondern Metadaten. Auch diese lassen weitreichende Schlüsse zu. Sie zeigen Verbindungen zwischen Personen auf, können Hinweise auf den Inhalt der ausgetauschten Daten geben und sind oft mit Standortdaten versehen. Überdies lassen sich die Vorratsdaten mit weiteren Daten verknüpfen, etwa solchen, die aus einem sichergestellten Gerät ausgelesen oder vom Provider herausverlangt werden.

Nicht zu unterschätzen sind auch die Möglichkeiten der computergestützten Analyse von Daten. Der Europäische Gerichtshof (EuGH) hat die EU-Richtlinie, die den Mitgliedsländern die Vorratsdatenspeicherung für die Strafverfolgung vorgeschrieben hat, mit Entscheid vom 8. April 2014 für ungültig erklärt, da sie mit der Charta der Grundrechte der EU nicht vereinbar ist. Dabei bemängelte der EuGH u.a., dass es keine wie immer geartete Einschränkung des Personenkreises gebe, deren Daten gespeichert werden sollte. Als unzulässig erachtet wurde also insofern der Grundrechtseingriff, der daraus resultiert, dass mit der Vorratsdatenspeicherung anlasslos Daten praktisch aller Personen gespeichert werden. Nebst dem EuGH haben auch verschiedene nationale Verfassungsgerichte die Vorratsdatenspeicherung als grundrechtswidrig erachtet, so insbesondere in Deutschland, Österreich, den Niederlanden, Rumänien und Tschechien.

Die Vorratsdatenspeicherung kann auch in der Schweiz nicht als grundrechtskonform erachtet werden. Die EU-Grundrechtecharta entspricht inhaltlich der Europäischen Menschenrechtskonvention. Zudem sind verschiedene nationale Regelungen, die von Verfassungsgerichten aufgehoben worden sind, inhaltlich und von den prozessualen Garantien mit der schweizerischen Regelung vergleichbar.

Die Entwicklung geht in der Schweiz in eine andere Richtung: Die BÜPF-Revision, die zurzeit bei den eidgenössischen Räten hängig ist, sieht eine Ausdehnung der Vorratsdatenspeicherung vor. Es wären mehr IT-Unternehmen und Personen sowie viel mehr Daten von der Speicherungspflicht betroffen. Alle Daten müssten zwölf Monate aufbewahrt werden. Mit der BÜPF-Revision soll auch dem IMSI-Catcher eine gesetzliche Grundlage gegeben werden. Dieses Gerät gibt sich als Mobilfunkantenne aus und zieht alle Mobilgeräte in einem bestimmten Umkreis auf sich. Damit kann festgestellt werden, welche Mobilgeräte sich in diesem Umkreis befinden. Im Ergebnis kommt dies in etwa auf dasselbe heraus, wie wenn eine massenhafte Personenkontrolle in einem bestimmten Gebiet vorgenommen werden könnte.

Staatstrojaner: Besonders schwerer Eingriff

Währenddem für die Verwendung der Vorratsdaten durch die Behörden im Strafprozess immerhin ein konkreter Tatverdacht notwendig ist, sollen die Daten vom Geheimdienst auf schwammiger Grundlage rein präventiv genutzt werden können, was umso weniger als grundrechtskonform erachtet werden kann. Besonders problematisch ist der Einsatz des Staatstrojaners. Er kann die Fülle an Daten, die ein Computer, ein Kopierer oder ein Smartphone enthält, direkt erschliessen, quasi als Kombination einer verdeckten Hausdurchsuchung und einer Wanze. Dies stellt einen äusserst schweren Grundrechtseingriff dar.

Dazu kommt: Ein Trojaner manipuliert das Gerät, in das er sich einschleust. Er kann damit auch sich selbst manipulieren und die Spuren seiner Tätigkeit verändern. Im Unterschied zu einer Hausdurchsuchung ist es so technisch nicht möglich, ein verlässliches Dokument darüber zu erstellen, was der Trojaner eigentlich gemacht hat. Rechtsstaatlich ist sein Einsatz damit unhaltbar.

Zudem muss für die Platzierung des Trojaners im Zielgerät eine Sicherheitslücke gefunden werden. Damit sind weitere unschöne Aspekte des Staatstrojaners verbunden. Das zeigt der Fall Hacking Team, eines Unternehmens, das Überwachungssoftware vertrieb und seinerseits gehackt wurde. Die aufgedeckten Daten zeigten, dass das Hacking Team die Sicherheitslücken und die Software für deren Ausnutzung für teures Geld auf dem Schwarzmarkt einkaufen musste. Die Kantonspolizei Zürich bezog ihren Staatstrojaner vom Hacking Team und dürfte so mit Staatsgeldern Hacker alimentiert haben, die Sicherheitslücken nicht an die Hersteller der Software meldeten, sondern die Information dem Meistbietenden verkauften. Der Trojaner hatte zudem eine Hintertüre für das Hacking Team eingebaut, von der die Kantonspolizei wohl nichts wusste.

Die genehmigungsfreien Beschaffungsmassnahmen werden in Art. 13 ff. aufgeführt. Gemäss Art. 15 können «menschliche Quellen» eingesetzt werden. Dabei handelt es sich um den Einsatz von V-Leuten, die als Spitzel gegen Bezahlung im entsprechenden Milieu tätig werden. Die Erstellung von Legenden und Tarnidentitäten kann vom Vorsteher des VBS angeordnet werden. Dass der Einsatz von V-Leuten problematisch und deren Nutzen mehr als fragwürdig ist, zeigt ein Blick nach Deutschland.

Öffentliche und allgemein zugängliche Orte können gemäss Art. 14 NDG durch luftgestützte

Geräte wie Drohnen oder auch durch weltraumgestützte Geräte wie Satelliten überwacht werden. Beobachtungen in Bereichen der Privatsphäre sind zwar unzulässig, da die Massnahme keiner Genehmigungserteilung durch ein Gericht unterliegt. Der Gesetzgeber toleriert jedoch solche Aufnahmen, wenn sie aus technischen Gründen nicht verhindert werden können. Dass diese Aufnahmen zu vernichten sind, ändert nichts an der Tatsache, dass ein Eingriff in die Privatsphäre bereits stattgefunden hat. Der Einwand in der bundesrätlichen Botschaft, dass auch Blicke aus den Fenstern von Verkehrsflugzeugen private Bereiche treffen können, mutet reichlich naiv an.

Einschneidende Massnahmen, wie sie im NDG vorgesehen sind, sollten - wenn überhaupt - Domäne der Strafverfolgungsbehörden bleiben. Dafür spricht, dass dort strafprozessuale Garantien bestehen, die dem Gewicht der mit den Überwachungsmassnahmen verbundenen Grundrechtseingriffen entsprechen. Hinzu kommt, dass diverse Formen von Betätigungen, die im Fokus des Geheimdienstes stehen, bereits vom Strafrecht erfasst sind. Zu erwähnen sind dabei insbesondere strafbare Vorbereitungshandlungen (Art. 260bis StGB) sowie Beteiligung an bzw. Unterstützung einer kriminellen Organisation (Art. 260ter StGB). Mit dem NDG würde der Geheimdienst zu einer parallelen Vorfeldermittlungsbehörde, die teilweise dieselben Kompetenzen hätte wie die Strafverfolgungsbehörden - aber mit viel tieferen Eingriffshürden. Strafverfolger wie der St. Galler Staatsanwalt Thomas Hansjakob kritisieren das neue Gesetz, weil die Erkenntnisse des NDG in einem Strafprozess möglicherweise nicht verwendet werden können. Es kann zu Beweisverwertungsverboten kommen oder dazu, dass der Geheimdienst die ihm vorliegenden Informationen nicht offenlegt. Das dies nicht nur rein theoretische Bedenken sind, illustriert der Fall des mutmasslichen sog. Rütlibombers. Dessen Verhaftung beruhte offenbar auf geheimdienstlichen Quellen, u.a. auf Aussagen einer Person, die der Inlandgeheimdienst (DAP) unter Zusicherung der Anonymität befragt hatte. Die Person hatte sich zunächst bei einem Polizisten gemeldet und soll angegeben haben, für den als Rütlibomber Verdächtigten auf einer Baustelle Zündkapseln und Sprengstoff beschafft zu haben. Der DAP weigerte sich in der Folge standhaft, Unterlagen im Zusammenhang mit der Einvernahme herauszugeben oder die Identität der Person offen zu legen. Das Verfahren gegen den mutmasslichen Rütlibomber wurde schliesslich eingestellt. Wer die Person war, die der DAP befragt hatte, ob sich diese allenfalls in irgend einem Zusammenhang strafbar gemacht hatte und wie das Verfahren gegen den als Rütlibomber Verdächtigten verlaufen wäre, wenn die andere Person im Strafverfahren ausgesagt hätte, bleibt offen.

Kontrollgremien haben wenig Wirkung

Befürworter des NDG verweisen auf die im Gesetz vorgesehene Kontrolle durch Richter und Aufsichtsgremien. Bevor man sich damit das rechtsstaatliche Gewissen beruhigen lässt, lohnt es sich, darüber nachzudenken, was diese Kontrollinstanzen zu leisten vermögen.

Als Strassburg die Schweiz zur Einführung des Haftrichters zwang, wurden damit grosse Erwartungen verbunden. Die Praxis war ernüchternd. Ein Angeschuldigter im Strafverfahren kann sich glücklich schätzen, wenn er auf ein Zwangsmassnahmengericht trifft, das sich auf eine wirkliche Prüfung der Verhältnismässigkeit einlässt und nicht einfach wie in jedem Standardfall mechanisch Untersuchungshaft anordnet.

Bei geheimdienstlichen Zwangsmassnahmen wird man noch viel weniger von der richterlichen Überprüfung erwarten können. Sie findet ohne den Betroffenen statt. Geheimdienstliche Massnahmen gründen nicht auf einem konkreten Tatverdacht. Es geht vielmehr darum, Massnahmen bewilligt zu erhalten, um Hinweisen und Vermutungen nachgehen zu können. Der Richter kann seine Abwägung nicht auf Fakten abstützen, sondern nur entscheiden, ob die Vorbringen des Nachrichtendienstes schwer genug wiegen, um die beantragte Massnahme

bewilligen zu können. Der Nachrichtendienst muss seinen Antrag also nur geschickt genug begründen und ausreichend mit Behauptungen aufladen. Beweise wird er nicht vorbringen müssen. Eine richterliche Überprüfung aber, die nicht über die formelle Ebene hinauskommt und deren Ergebnis einzig davon abhängt, wie geschickt sich die antragstellende Behörde gebärdet, ist von geringem Wert.

Im NDG ist ein Ausbau der für den NDB zuständigen Kontrollgremien vorgesehen. Dass die Kontrolle des Geheimdienstes eine dornenvolle Sache ist, weiss man seit dem Fichenskandal. Einen Eindruck der Schwierigkeiten vermittelt der Bericht der Geschäftsprüfungsdelegation der Eidgenössischen Räte (GPDel) vom 21. Juni 2010, der zahlreiche Ungereimtheiten im DAP aufdeckte.

Gemäss dem Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit darf eine Person nur registriert werden, wenn in Bezug auf diese Person Hinweise für eine relevante Aktivität vorliegen, etwa für terroristische oder gewaltextremistische Betätigung. Der Geheimdienst hatte nun stattdessen über Jahre alle Personen, über die er Angaben erhielt, zunächst im damaligen Staatsschutzinformationssystem ISIS erfasst und die Prüfung, ob diese Person effektiv ins ISIS gehört, aufgeschoben. Die GPDel hatte bemerkt, dass der Geheimdienst mit diesen Überprüfungen stark im Hintertreffen war. Zudem war es Praxis, die Tausenden von ausländischen Personen, die im Rahmen der Fotopasskontrollen an der Grenze erfasst werden, ins ISIS einzutragen. Über Jahre hinweg versuchte der DAP, der GPDel den Eindruck zu vermitteln, die Überprüfung der Personen schreite voran. Irgendwann stellte die GPDel fest, dass dem überhaupt nicht so war. Hinzu kamen massive Probleme bei der Umstellung auf eine neue Version des Informationssystems. Schliesslich musste der Chef des DAP, Urs von Daeniken, der schon vor dem Fichenskandal im Geheimdienst tätig gewesen war, den Hut nehmen.

Im Bericht der GPDel sind auch einige Beispiele unrechtmässiger ISIS-Einträge erwähnt. So war Balthasar Glättli, heutiger Nationalrat der Grünen, als Bewilligungsinhaber einer friedlichen Palästina-Demo verzeichnet. Bei der Flüchtlingshelferin Anni Lanz vermutete der DAP aufgrund einer Anfrage eines ausländischen Nachrichtendienstes Verbindungen zu «extremistisch-islamistischen Gruppierungen», was zu einem Eintrag ins ISIS mitsamt Zusatzeintrag «Verdacht Schwarzer Block» führte. Fünf türkisch- bzw. kurdischstämmige Mitglieder des Grossen Rats des Kantons Basel-Stadt wurden registriert, nachdem ihr Wahlerfolg u.a. von einer Zeitung gefeiert wurde, die nach Einschätzung des DAP der PKK und ihren Nachfolgeorganisationen nahe stand. Dass die im Bericht erwähnten Fälle überhaupt bekannt wurden, war überwiegend reiner Zufall. All dies zeigt: Auf die Fähigkeiten zur Selbstbegrenzung des Geheimdiensts vertraut man besser nicht; der geheimdienstliche Datenhunger ist gross und überschiessend. Dasselbe hat sich ja auch im NSA-Skandal gezeigt.

Im NDG sind zusätzliche Aufsichtsgremien vorgesehen, darunter eine sogenannte unabhängige Aufsichtsbehörde (Art. 76 ff.). Sie wird vom Bundesrat gewählt und ist dem VBS zugeordnet, unter dessen Dach auch der Nachrichtendienst agiert. Bei der Unabhängigkeit ist damit ein Fragezeichen anzubringen. Auch wenn die Aufsichtsbehörde weitgehende Auskunfts- und Zugriffsrechte hat: Mehr als Schlaglichter in die Dunkelkammer Geheimdienst wird auch sie nicht werfen können.Den nächsten Fall Glättli oder Lanz würde sie nur finden können, wenn sie bereits weiss, dass sie diesen suchen muss.

Rasterfahndung im Internet

Eine weitere Neuerung im Gesetz trägt die eher unverfänglich klingende Bezeichnung Kabelaufklärung (Art. 39 ff.). Vorgesehen ist die breite Erfassung und Auswertung

«grenzüberschreitender Signale aus leitungsgebundenen Netzen». Damit würde der Nachrichtendienst zu einer Mini-NSA. In einer Art permanenten Internetrasterfahndung könnten grenzüberschreitende Telekommunikationsverbindungen erfasst und nach Stichworten durchsucht werden. Gemäss Art. 39 Abs. 2 ist die Durchsuchung von landesinternen Verbindungen unzulässig. Nur: Es gibt kein landesinternes Internet. Internetkommunikation mit Schweizer Beteiligung läuft regelmässig auch über ausländische Server. Damit verliert die Unzulässigkeitserklärung der inländischen Kabelaufklärung ihre Bedeutung. Der Ansatz, möglichst alle Kommunikation mitzuschneiden, nach Suchbegriffen zu durchforsten und vom anfallenden Datenhaufen Ergebnisse mit landesinternem Hintergrund wieder zu entfernen, kann auch insoweit herzlich wenig zur Wahrung der Grundrechte der inländischen Personen beitragen, als deren Kommunikation eben doch erfasst wird und das Entfernen ja auch nicht geht, ohne sich damit zu befassen, von wem die Kommunikation stammt und für wen sie bestimmt war. Im Ergebnis resultiert eine fast flächendeckende Überwachung der elektronischen Kommunikation. Mit der Kabelaufklärung besteht die Möglichkeit, Suchfilter zu setzen, die automatisch sämtliche E-Mails, Suchanfragen oder Inhalte der Internettelefonie nach gewissen Begriffen durchforsten.

Die nachrichtendienstliche Datenerfassung und insbesondere die Kabelaufklärung müssen auch im Zusammenhang mit der internationalen Geheimdienstzusammenarbeit gesehen werden, bei der der Datenaustausch eine zentrale Rolle spielt. Inländische Datenbeschaffung dient nicht zuletzt dem Zweck, Material für die internationale Datenbörse zu haben. Damit lassen sich auch Beschränkungen zugunsten der inländischen Bevölkerung aushebeln. Die Bespitzelung der eigenen Bürger kann man sich schenken, wenn man diese einem Partnerdienst überlassen und dann die Daten austauschen kann.

Was fehlt im neuen Gesetz, ist ein wirksames Einsichtsrecht der betroffenen Personen. Es ist derart mit Einschränkungen versehen, dass es kaum zum Tragen kommen kann. Es ist für die Betroffenen essenziell zu wissen, ob, wie und aufgrund welchen Sachverhalts sie beim Nachrichtendienst verzeichnet sind. Ist jemand erfasst und kann dies nicht in Erfahrung gebracht werden, vergrössert dies den Eingriff in die Grundrechte noch einmal. Die betroffene Person wäre die einzige, die dem Eintrag etwas entgegensetzen und ihn korrigieren könnte. Das scheitert aber daran, dass niemand weiss, was über ihn gespeichert ist. Die vorgesehenen weitgehenden Einschränkungen des Einsichtsrechts (Art. 63 ff.) verletzen eindeutig die Grundrechte. Problematisch ist hierbei, dass der Nachrichtendienst selbst darüber entscheiden kann, ob ein überwiegendes Interesse gegen die Einsicht spricht, und dass die daran anschliessende Überprüfung des Entscheids durch den Datenschutzbeauftragten und das Verwaltungsgericht stattfindet, ohne dass die betroffene Person erfährt, was überprüft wird, und ohne dass sie eine Stellungnahme abgeben kann. Dieses Vorgehen verletzt insbesondere die Rechtsweggarantie und das mit den Grundrechten verbundene Recht auf wirksame Beschwerde.

Fazit: Die bestehenden gesetzlichen Grundlagen wären reformbedürftig - aber in eine andere Richtung: Die nachrichtendienstliche Tätigkeit ist klarer zu begrenzen. Insbesondere wäre ein wirksameres Einsichtsrecht in die Staatsschutzakten zu schaffen.

zum doppelseitigen Ausdrucken im Format A3

(für A4-Drucker Zoom auf 72% einstellen, aber es ergibt sich eine kleine Schrift)