Staatliche Überwachungsmass-nahmen im digitalen Zeitalter

Ein Rundflug über NDG, BÜPF und Staatstrojaner

Dr. iur. Daniel Hürlimann

Nachrichtendienstgesetz (NDG)

- Durch die Bundesversammlung in der Herbstsession 2015 verabschiedet
- Referendumsfrist läuft bis zum 14. Januar 2016
- Unterschriftensammlung läuft: www.nachrichtendienstgesetz.ch
- Botschaft: «Der Gesetzesentwurf soll keine Weiterentwicklung der bestehenden Rechtsgrundlagen darstellen.»
- Aufbau des Gesetzes:
  - 1. Kapitel: Allgemeine Bestimmungen und Grundsätze der Informationsbeschaffung
  - 2. Kapitel: Aufgaben und Zusammenarbeit des NDB
  - 3. Kapitel: Informationsbeschaffung
  - 4. Kapitel: Datenbearbeitung und Archivierung
  - 5. Kapitel: Dienstleistungen
  - 6. Kapitel: Politische Steuerung, Kontrolle sowie Rechtsschutz

NDG-Kapitel zur Informationsbeschaffung

1. Abschnitt: Genehmigungsfreie Beschaffungsmassnahmen
2. Abschnitt: Legendierungen und Tarnidentitäten
3. Abschnitt: Auskunfts- und Meldepflichten
4. Abschnitt: Genehmigungspflichtige Beschaffungsmassnahmen
5. Abschnitt: Zusammenarbeit und Quellenschutz
6. Abschnitt: Beschaffung von Informationen über Vorgänge im Ausland
7. Abschnitt: **Kabelaufklärung**

Art. 39 Abs. 1 NDG (Kabelaufklärung)
«Der NDB kann den durchführenden Dienst damit beauftragen, zur Beschaffung von Informationen über sicherheitspolitisch bedeutsame Vorgänge im Ausland sowie zur Wahrung weiterer wichtiger Landesinteressen grenzüberschreitende Signale aus leitungsgebundenen Netzen zu erfassen.»

Kabelaufklärung (Art. 39 ff. NDG)

«grenzüberschreitende Signale aus leitungsgebundenen Netzen erfassen»

→?!

Mit der Kabelaufklärung will der Nachrichtendienst des Bundes die Telekommunikationsverbindungen, welche von der Schweiz ins Ausland führen, nach definierten Stichworten durchsuchen. Da die meiste Internetkommunikation der Schweizer Bevölkerung über ausländische Server und Netzwerke führt, sind alle von dieser Überwachung betroffen.

Betroffene Grundrechte

Kabelüberwachung = verdachtsunabhängige Massenüberwachung
- Recht auf Schutz der Privatsphäre
- freie Meinungsäusserung
- Unschuldsvermutung

Art. 36 Abs. 3 BV: «Einschränkungen von Grundrechten müssen verhältnismässig sein.»
Botschaft des Bundesrates: «Aus dem Ausland ist bekannt, dass die Kabelaufklärung rein technisch machbar ist. Erst mit der Analyse der Datenströme durch die Schweiz lässt sich aber feststellen, ob mit der Kabelaufklärung auch in der Schweiz hinreichend nützliche Informationen gewonnen werden können.»

Menschenrechtskommissar des Europarats

COMMISSIONER FOR HUMAN RIGHTS

COMMISSAIRE AUX DROITS DE L'HOMME

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Ref: CommHR/CL-MB/sf 068-2015

Monsieur Ueli MAURER
Conseiller fédéral
Chef du Département fédéral de la défense,
de la protection de la population et des sports

Strasbourg, le 23 septembre 2015

Monsieur le Conseiller fédéral,

[…]

L'exploration du réseau câblé par le Service du Renseignement telle que prévue à l'article 38 du projet de loi et dont l'usage pourrait conduire à une collecte massive de données pose également des questions d'un point de vue du droit au respect de la vie privée. Cette méthode est à même de créer un climat social où toute personne serait perçue comme étant potentiellement suspecte.

[…]

Désireux de continuer un dialogue constructif avec vous, je vous prie d'agréer, Monsieur le Conseiller fédéral, l'expression de ma haute considération.

Nils Muižnieks

Antwort des VBS-Vorstehers

Monsieur le Commissaire,

Votre lettre du 23 septembre dernier concernant la nouvelle loi sur le renseignement m'est bien parvenue et a retenu toute mon attention.

Le 25 septembre 2015, le Conseil national et le Conseil des Etats ont adopté la loi à une large majorité. Les travaux législatifs se sont déroulés sur une période de quatre ans environ. Le Parlement, le public et les médias se sont intéressés de près à la question. La loi crée un équilibre judicieux entre, d'une part, des activités et moyens supplémentaires et, d'autre part, de nouveaux contrôles internes, indépendants et parlementaires. La liberté de la majorité de la population sera garantie tout en assurant la sécurité du pays. La loi ne donne pas un blanc-seing au Service de renseignement de la Confédération. En effet, une procédure d'autorisation sera toujours exigée pour s'introduire dans la sphère privée d'individus. La Suisse restera ainsi un havre de liberté et de sécurité.

Aujourd'hui, c'est avec fierté que je peux annoncer que la Suisse a créé une base légale moderne et tournée vers l'avenir pour son service de renseignement.

Veuillez agréer, Monsieur le Commissaire, l'expression de ma haute considération.

Ueli Maurer
Conseiller fédéral

Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF)

Aufbau des Gesetzes heute:
1. Abschnitt: Geltungsbereich und Organisation
2. Abschnitt: Überwachung ausserhalb von Strafverfahren
3. Abschnitt: Überwachung des Postverkehrs
4. Abschnitt: Überwachung des Fernmeldeverkehrs
5. Abschnitt: Gebühren und Entschädigungen

Aufbau des Gesetzes gemäss Entwurf:
1. Abschnitt: Allgemeine Bestimmungen
2. Abschnitt: Informatiksystem zur Verarbeitung von Daten im Rahmen der Überwachung des Fernmeldeverkehrs
3. Abschnitt: Aufgaben des Dienstes
4. Abschnitt: Pflichten bei der Überwachung des Postverkehrs
5. Abschnitt: Auskünfte im Zusammenhang mit der Überwachung des Fernmeldeverkehrs
6. Abschnitt: Pflichten bei der Überwachung des Fernmeldeverkehrs
7. Abschnitt: Sicherstellung der Auskunfts- und Überwachungsbereitschaft der Anbieterinnen von Fernmeldediensten
8. Abschnitt: Notsuche und Fahndung nach verurteilten Personen
9. Abschnitt: Kosten und Gebühren
10. Abschnitt: Strafbestimmungen
11. Abschnitt: Aufsicht und Rechtsschutz

Überwachung des Fernmeldeverkehrs

Art. 15 Abs. 3 BÜPF:
«Die Anbieterinnen sind verpflichtet, die für die Teilnehmeridentifikation notwendigen Daten sowie die Verkehrs- und Rechnungsdaten während sechs Monaten aufzubewahren.»

→ ?!

www.digitale-gesellschaft.ch/vds.html

Urteil des EuGH vom 8. April 2014

Vorratsdatenspeicherung verletzt die Grundrechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten, weil

- sie sich generell auf sämtliche Personen und elektronischen Kommunikationsmittel erstreckt
- der Zugang zu den Daten zu wenig genau geregelt ist
- die Speicherdauer von mindestens sechs Monaten unabhängig vom etwaigen Nutzen der Daten für das verfolgte Ziel gilt
- Richtlinie sieht keine Massnahmen zum Schutz vor unberechtigtem Zugang und unberechtigter Nutzung vor
- Richtlinie schreibt keine Speicherung der Daten im Unionsgebiet vor

Deshalb: EU-Richtlinie über die Vorratsspeicherung von Daten für ungültig erklärt.

Weitere Urteile

- 2009: Rumänien
- 2010: Deutschland
- 2011: Tschechien
- 2014: Österreich
- 2015: Niederlande, Bulgarien

→ Sämtliche Verfassungsgerichte, welche eine zur Schweiz vergleichbare Regelung zu prüfen hatten, haben die Vorratsdatenspeicherung als unrechtmässigen Eingriff in die Grundrechte eingestuft und sie aufgehoben.

…und die Schweiz?

Vorschlag Bundesrat (Februar 2013): Verdoppelung der Speicherdauer von 6 auf 12 Monate

Ständerat (März 2014): einverstanden

Nationalrat (Juni 2015): einverstanden

Ständeratskommission (November 2015): vielleicht doch nicht

Ständerat (gestern): keine Verdoppelung der Speicherdauer

Ständerat nun doch gegen längere Vorratsdatenspeicherung

www.inside-it.ch/articles/42305

Die Telefonranddaten sollen nicht länger aufbewahrt werden, als bisher. Der Ständerat hat sich am Montag dafür ausgesprochen, bei der geltenden Frist von sechs Monaten zu bleiben. Damit kam er auf einen früheren Entscheid zurück.

Randdaten geben Auskunft darüber, wer wann mit wem wie lange telefoniert hat oder wer wann an wen einen Brief geschickt hat. Heute werden diese Daten sechs Monate lang aufbewahrt. Der Bundesrat wollte im Rahmen der Revision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) die Frist für die Aufbewahrung der Randdaten verlängern. Der Nationalrat zeigte sich damit einverstanden.

Der Ständerat hatte zunächst ebenfalls Ja gesagt zu zwölf Monaten für die Telefonranddaten. Beim Postverkehr wollte er bei sechs Monaten bleiben. Am Montag hat er nun auf Antrag seiner Rechtskommission oppositionslos beschlossen, auch bei den Telefonranddaten bei sechs Monaten zu bleiben.

Der Kommissionssprecher Stefan Engler (CVP/GR) begründete die Kehrtwende mit dem drohenden Referendum. Die Vorratsdatenspeicherung sei ohnehin schon umstritten. Würde die Aufbewahrungsdauer auf zwölf Monate verlängert, könnte dies die Chancen eines Referendums erhöhen und die ganze Vorlage gefährden, gab er zu bedenken. (sda/hjm)

…und die Schweiz?

Beschwerde der Digitalen Gesellschaft (digitale-gesellschaft.ch), seit September 2014 hängig beim Bundesverwaltungsgericht

Volltext der Beschwerde abrufbar unter:
http://digiges.ch/Beschwerde_20140902.pdf

Gemäss Medienmitteilung des Digitalen Gesellschaft ist die Beschwerde seit März 2015 spruchreif.

Bundesverwaltungsgericht gibt keine Auskunft zum Urteilszeitpunkt.

Unabhängig vom Ergebnis Weiterzug ans BGer wahrscheinlich

Staatstrojaner

- Kantonspolizei Zürich kauft Staatstrojaner
- Staatstrojaner = Spionageprogramm, das gegen die gängigen Computer und Smartphones eingesetzt werden kann
- Kauf eines Staatstrojaners beinhaltet zwangsläufig auch Kauf geheimer Sicherheitslücken in Software wie Microsoft Word
- Gesetzliche Grundlage?

Art. 280 StPO

Die Staatsanwaltschaft kann technische Überwachungsgeräte einsetzen, um:

a. das nicht öffentlich gesprochene Wort abzuhören oder aufzuzeichnen;
b. Vorgänge an nicht öffentlichen oder nicht allgemein zugänglichen Orten zu beobachten oder aufzuzeichnen;
c. den Standort von Personen oder Sachen festzustellen.

Art. 280 lit. a StPO

Thomas Hansjakob: «Man könnte am ehesten versucht sein, den Einsatz von GovWare unter Art. 280 lit. a StPO zu subsumieren. Eingesetzt werden aber eben keine technischen Geräte, sondern es wird in ein Datenverarbeitungssystem des Beschuldigten eingegriffen. Dessen Software wird so manipuliert, dass das dem Beschuldigten gehörende technische Gerät dazu verwendet werden kann, seine Gespräche zu überwachen. Das ist offensichtlich von der Eingriffstiefe her etwas anderes als der Einsatz von Geräten der Strafverfolgungsbehörden, und es betrifft eben einen Eingriff nach Art. 143bis StGB, für welchen Art. 280 lit. a StPO meines Erachtens keine gesetzliche Grundlage liefern kann.
Dies führt zum (zugegebenermassen für den Praktiker unbefriedigenden) Ergebnis, dass die Überwachung der Internet-Telefonie mittels GovWare zurzeit mangels klarer gesetzlicher Grundlage nicht zulässig ist.»

www.hansjakob.ch/thomas/jusletter_einsatz_govware.pdf

Art. 280 lit. a StPO

Thomas Hansjakob: «Ich halte denn auch den vorgesehenen Weg des Bundesrates, die gesetzliche Grundlage mit der Revision des BÜPF zu schaffen, für richtig – in der VÜPF wäre eine solche Regelung unzulässig gewesen, weil von der Eingriffsschwere her eine Grundlage in einem formellen Gesetz erforderlich ist.
[…]
Fazit: Der Einsatz von GovWare zur verdeckten Beweiserhebung ist nach der geltenden Rechtslage in der Schweiz zurzeit noch nicht möglich. Die Revision des BÜPF und die damit verbundene Ergänzung der StPO sollen diese Lücke schliessen, wobei (wohl vorwiegend aus politisch-taktischen Gründen) die GovWare auch in Zukunft in der Schweiz nur dazu verwendet werden soll, Internet-Telefonie und verschlüsselten Mailverkehr überwachen zu können.»

www.hansjakob.ch/thomas/jusletter_einsatz_govware.pdf

Ergebnis

Falls BÜPF-Revision kommt, wird erst damit die gesetzliche Grundlage für Staatstrojaner geschaffen.

Der externe Standpunkt

Wer heute schon Trojaner einsetzt, verspottet unseren Rechtsstaat

Der polizeiliche Einsatz von Spionage-Software ist im geltenden Recht klar illegal. Daran würde auch ein neues Gesetz nichts ändern: Trojaner gehören nicht in die Hände des Staats, **meint Martin Steiger**

Danke für Ihre Aufmerksamkeit!

www.uni-zh.ch/dh