Neues Nachrichtendienstgesetz

8. März 2013

Alter Wein in neuen Schläuchen

Im Juni 2007 legte der Bundesrat einen Entwurf zur Verschärfung des Staatsschutzgesetzes vor (BWIS II). grundrechte.ch hat diesen Gesetzesentwurf in der Vernehmlassungsantwort scharf kritisiert und auch einen öffentlichen Aufruf dagegen lanciert, welcher von über 500 Personen unterzeichnet wurde.

Allgemein stiessen die Vorschläge des Bundesrats auf breite Kritik. In der Folge haben der Ständerat am 3. März 2009 und der Nationalrat am 27. März 2009 die Rückweisung an den Bundesrat beschlossen.

4 Jahre nach der Rückweisung resp. 5½ Jahre nach der ersten Präsentation bringt der Bundesrat jetzt genau das Gleiche, was im Jahr 2009 zurückgewiesen wurde, einfach unter dem Titel «Nachrichtendienstgesetz» statt «BWIS II».

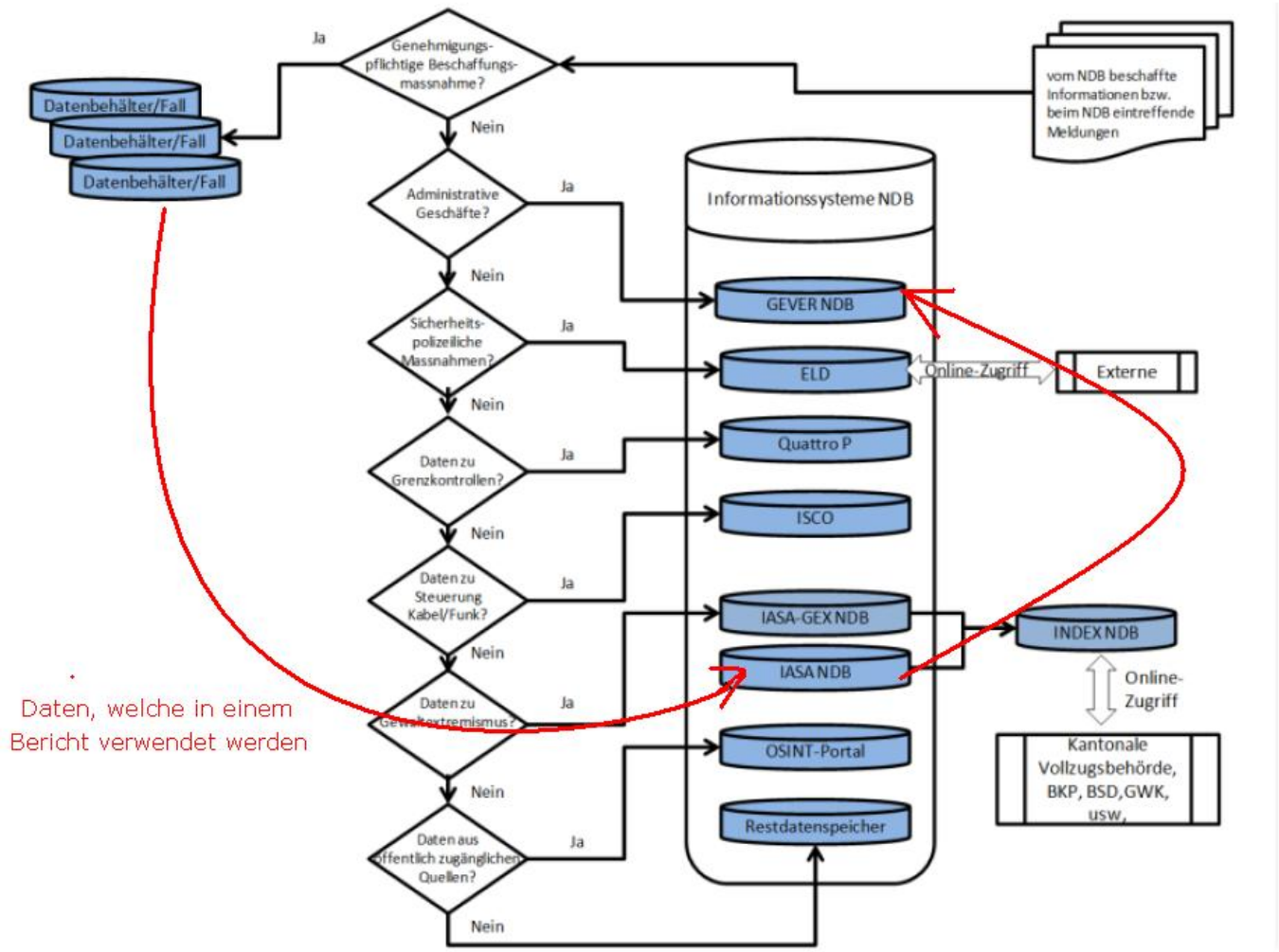
Namentlich die «besonderen Mittel der Informationsbeschaffung» wurden unverändert übernommen, sie heissen neu «genehmigungspflichtige Beschaffungsmassnahmen»:

- die Überwachung von Post, Telefon, E-Mail und Internet innerhalb der Schweiz
- das Beobachten und Abhören von Personen an nicht allgemein zugänglichen Orten (also in Wohnungen, Büros, Autos) - auch mittels technischer Überwachungsgeräte (Wanzen, Richtmikrofone, Videokameras, Fluggeräte etc.)
- das geheime Durchsuchen von privaten Datenbarbeitungssystemen / Computern, was entweder den geheimen Einbruch der Staatsschützer in private Wohnungen oder Büros oder das Versenden von sogenannten Trojanern voraussetzt (gezielte Einschleusung von Spionage-Software)

Neu unter den «genehmigungspflichtigen Beschaffungsmassnahmen» ist die Kabelaufklärung. Wie bei der Funkaufklärung soll bei der Kabelaufklärung der Fernmeldeverkehr aller Teilnehmer aufgezeichnet und ausgewertet werden. Im Gegensatz zur Funkaufklärung, welche ausschliesslich Signalquellen im Ausland abdeckt, betrifft die Kabelaufklärung ausnahmslos schweizerische Fernmeldeanbieter, welche auch zur Mitarbeit verpflichtet werden können. Erkenntnisse aus «genehmigungspflichtigen Beschaffungsmassnahmen» sollen explizit als Beweise in Strafverfahren verwendet werden können.

Gemäss Bericht des Bundesrats ist mit etwa 10 genehmigungspflichtigen Informationsbeschaffungen pro Jahr zu rechnen, wofür 16 neue Stellen (ohne Bundesverwaltungsgericht als Genehmigungsbehörde) benötigt werden. Wer die ausufernde Sammelwut des Staatsschutzes in den letzten Jahr(zehnt)en beobachtet hat, kann über diese offensichtliche Untertreibung nur lachen.

«Data Management by Chaos»



Die Datenhaltung im neuen Datenbanksystem, welches ISIS ablösen soll, spottet jeder Beschreibung. Zwar werden alle neuen Informationen, sowohl Inlands- als auch Auslandsdaten, nach einem vorgegebenen Muster einer bestimmten Datenbank zugewiesen. Sobald Daten aber erfasst sind, können sie frei in alle anderen Datenbanken kopiert werden und unterliegen dann den Zugriffs- Qualitäts- und Löschregeln der neuen Datenbank.

Der Nachrichtendienst soll auch zur Wahrung wesentlicher Landesinteressen in besonderen Lagen, wie dem Schutz kritischer Infrastrukturen und des Finanz- und Wirtschaftsplatzes oder bei Entführungen von Schweizer Bürgerinnen und Bürgern im Ausland, eingesetzt werden. Wie eine Organisation, welche nicht einmal die eigenen File- und Mailserver bewachen kann, kritische Infrastrukturen in der Schweiz schützen soll, bleiben der Bundesrat und der Nachrichtendienstchef Markus Seiler schuldig.

Microsoft hat mit der Publikation des «MS 2012 Law Enforcement Requests Report» erstmals offengelegt, aus welchen Ländern und wie oft staatliche Behörden Auskünfte über Nutzer von Internet-Angeboten erbaten. Die Schweiz erscheint in diesem Bericht lediglich im Zusammenhang mit der Internet-Telefonie Skype, nicht aber mit anderen Microsoft-Diensten, z.

B. Hotmail. Im Jahr 2012 lag die Schweiz in absoluten Zahlen mit 74 Anfragen hinter Grossbritannien (1,268), USA (1,154), Deutschland (686), Frankreich (402), Taiwan (316), Australien(195), Luxemburg (98) und Italien (96) an neunter Stelle. Gemessen an Anfragen pro eine Million Einwohner liegt die Schweiz mit 9.3 hinter Luxemburg (196), Grossbritannien (20.1), Taiwan (13.6) und Malta (12.3) gar an fünfter Stelle, noch vor Australien (8.9), Deutschland (8.4), Island (6.5) und Frankreich (6.3). Eine Aufschlüsselung nach anfragenden Behörden fehlt leider. Diese 74 Fälle wären aber sicher Kandidaten für eine Überwachung mittels Trojaner gewesen, falls dies bereits zugelassen wäre.

Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) äusserte sich kritisch zum Einsatz von Staatstrojanern. Dass der Nachrichtendienst in fremde Computer eindringen dürfe, schaffe eine gefährliche Ausgangslage. «Es ist rechtsstaatlich nicht vertretbar, dass der Nachrichtendienst Computer auch manipulieren darf», so Thür.

Das ausufernde Sammeln von Telefondaten durch den amerikanischen Geheimdienst NSA ist schon seit vielen Jahren ein kontroverses Thema. Bereits nach dem Terroranschlag vom 11. September 2001 erfasste die NSA die Verbindungsdaten sämtlicher Telefongespräche in den USA. Dies wurde erst fünf Jahre später bekannt. US-Medien berichteten danach über das Thema regelmässig und auch im Kongress und von Bürgerrechtlern wurde es ausführlich diskutiert.

Mitte Mai 2013 setzte sich der Systemadministrator Edward Snowden, welcher von «Booz Allen Hamilton» angestellt war und für die NSA auf Hawaii gearbeitet hatte, mit brisanten Unterlagen im Gepäck nach Hong Kong ab, wo er britische und amerikanische Medien kontaktierte. Am 5. Juni 2013 enthüllte der «Guardian», dass ein Gericht eine Verfügung der NSA bestätigt habe, welche den Telefonanbieter «Verizon» verpflichtet, detaillierte Informationen über alle Telefonate innerhalb der USA und zwischen den USA und dem Ausland an die Behörde weiterzugeben. Weltweit war die Empörung gross, vor allem, nachdem kurz darauf bekannt wurde, dass alle grossen Telefonanbieter der USA jeden Tag sämtliche Verbindungsdaten an die NSA abliefern müssen. Die NSA stellt jeweils Verfügungen aus, welche drei Monate gültig sind, und alle Telefongesellschaften unterliegen einer absoluten Schweigepflicht.

Während Präsident Barack Obama und NSA-Direktor James Clapper beschwichtigten, die Veröffentlichung der Sammelwut der NSA kritisierten und das wahre Ausmass herunterspielten, veröffentlichte die «Washington Post» am 7. Juni 2013 ein zweites Dokument von Edward Snowden, eine PowerPoint Präsentation von «Prism». Unter dem Codenamen «Prism» besteht ein Programm, welches der NSA Einsicht in die Daten von Internetdienstleistern ermöglicht. Die NSA kann E-Mails mitlesen, Videos studieren und Gespräche auf Skype mithören. Ob dies heimlich geschieht oder mit dem Wissen der Unternehmen, darüber wird gestritten. Jedenfalls begann es im September 2007 bei Microsoft, einer Firma, die gerade eine Werbekampagne mit dem Slogan bestreitet, wonach «Ihre Privatsphäre unsere Priorität» ist. 2008 folgte Yahoo, 2009 Google, Facebook und Paltalk, ein Dienst für Video-Chats. Seit drei Jahren bedient sich die Behörde bei Youtube, seit zwei bei Skype und AOL, seit einem Jahr ist auch Apple erfasst. Angeblich soll aber nur der Internetverkehr von Personen, welche keinen Wohnsitz in den USA haben, aufgezeichnet werden. Die Wahrscheinlichkeit, dass US-Bürger nicht erfasst werden, liegt bei 51 % (bei Würfeln hatte man lediglich 50 % ...). Zudem ist es ein merkwürdiges Grundrechteverständnis, wenn nur Landsleute von Behördenwillkür geschützt sind.

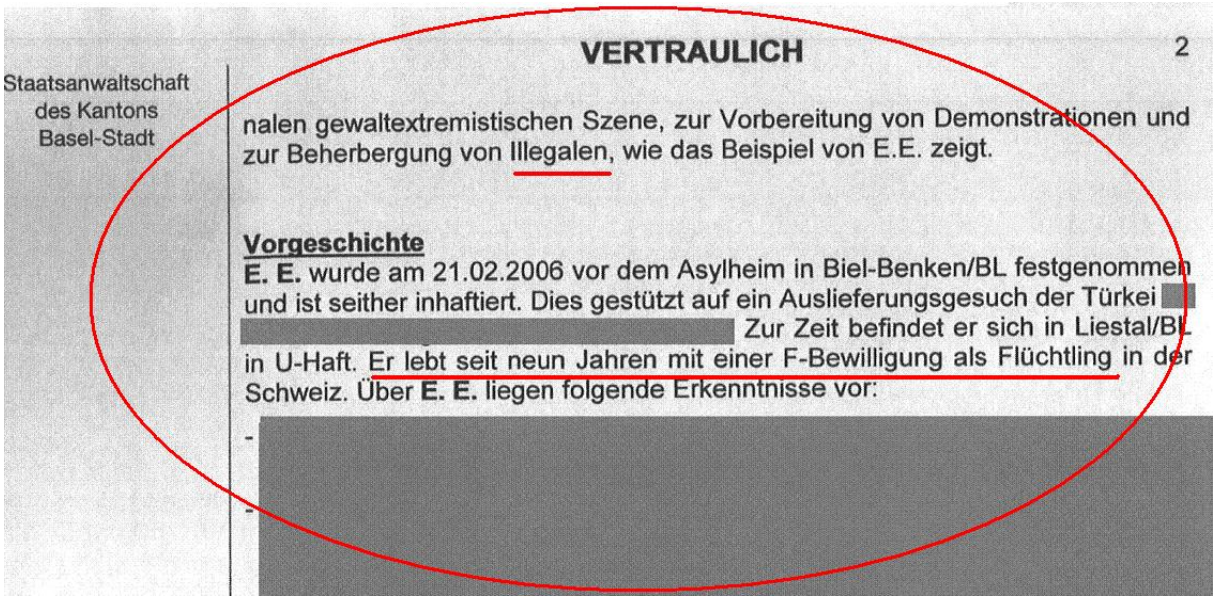
Am 7. Juni 2013 durfte dann wieder der «Guardian» über «Boundless Informant» berichten. «Boundless Informant» (zu deutsch: grenzenloser Informant) ist ein Computersystem, welches aus einer Fülle nachrichtendienstlicher Daten mit Hilfe von Data Mining signifikante Zusammenhänge herausfiltert, etwa die Bewegung einer einzelnen, z. B. terrorverdächtigen

Person aus einer Fülle von E-Mails und Telefonmetadaten von Millionen von Menschen. «Boundless Informant» gibt fast in Echtzeit Antworten auf Fragen wie «welche Abhördichte haben wir im Land X?».

Der britische Geheimdienst zapft seit eineinhalb Jahren mit «Tempora» im grossen Stil Telefon- und Internetkabel an und gibt die Informationen an die US-Behörde NSA weiter. Im Mai 2012 waren 300 Analysten von GCHQ und 250 von NSA mit der Auswertung beschäftigt. Insgesamt 850,000 Mitarbeiter der NSA und privater Firmen haben Zugriff auf die Datenbanken des GCHQ. Bis zu 46 Kabel mit einer Bandbreite von je 10 Gigabit pro Sekunde können gleichzeitig erfasst werden. Die NSA hackte im grossen Stil Netzwerke von Universitäten und Telefongesellschaften in Hong Kong und China. Am 23. Juni 2013 reiste Edward Snowden aus Hong Kong «auf einer sicheren Route» ab, um in Ecuador um Asyl nachzusuchen.

Und was die NSA kann, muss der NDB auch können, haben sich in der Schweiz ein paar Schlapphüte gedacht. Mit dem neuen Nachrichtendienstgesetz sollen die Befugnisse der schweizerischen Geheimdienste stark erweitert werden: Telefonüberwachung mit Zugriffsmöglichkeit auf die bei den Telefonanbietern gespeicherten Randdaten, «Kabelaufklärung», bei welcher der gesamte Internetverkehr eines Kupfer- oder Glaskabels nach Schlüsselwörtern durchsucht wird, Trojaner installieren, um verschlüsselte Daten mitlesen zu können, und so weiter. Analog zur NSA sollen aber nur Internetteilnehmer aus dem Ausland ohne Grund und ohne richterliche Bewilligung bespitzelt werden, wobei die Trefferwahrscheinlichkeit auch bei knappen 51 % liegen dürfte, ein «Prism» nach Schweizer Art quasi. Als Begründung für die neuen Massnahmen darf auch der 11. September 2001 herhalten. Mit der «Funkaufklärung» gibt es in der Schweiz bereits ein Pendant zu «Boundless Informant».

Dass der NDB heute noch unter dem Regime des BWIS gleich unsinnige Daten sammelt wie vor Ende der 80iger-Jahre, beweist der Artikel «Zwei gewalttätige SeniorInnen» aus der WOZ Nr. 25/2013 vom 20. Juni 2013. Neben Belanglosigkeiten enthalten die Fichen aber auch haarsträubende Fehler. Sollten dem NDB noch verdeckte Ermittlungen zugestanden werden, würde die Sammelwut noch mehr ausufern. Vor diesem Hintergrund erscheint die Forderung der CVP, den NDB «Krawallanten präventiv überwachen» zu lassen, als schlechter Witz.



VERTRAULICH 2

Staatsanwaltschaft des Kantons Basel-Stadt

nalen gewaltextremistischen Szene, zur Vorbereitung von Demonstrationen und zur Beherbergung von Illegalen, wie das Beispiel von E.E. zeigt.

Vorgeschichte

E. E. wurde am 21.02.2006 vor dem Asylheim in Biel-Benken/BL festgenommen und ist seither inhaftiert. Dies gestützt auf ein Auslieferungsgesuch der Türkei [redacted] Zur Zeit befindet er sich in Liestal/BL in U-Haft. Er lebt seit neun Jahren mit einer F-Bewilligung als Flüchtling in der Schweiz. Über **E. E.** liegen folgende Erkenntnisse vor:

- [redacted]
-

*Detailansicht Seite 2 der Fiche Demo «Freiheit für Erdogan!»: Zur Beherbergung von **Illegalen**, wie das Beispiel E. E. zeigt ... Er lebt seit neun Jahren mit einer **F-Bewilligung**... Wer den Unterschied zwischen illegal und F-Bewilligung nicht kennt, sollte auch keine Fichen verfassen*

dürfen!

grundrechte.ch lehnt das Nachrichtendienstgesetz entschieden ab und hat sich in der Vernehmlassungsantwort entsprechend geäussert.

Am 23. Oktober 2013 hat der Bundesrat vom Ergebnis des Vernehmlassungsverfahrens über das Nachrichtendienstgesetz Kenntnis genommen und das VBS mit der Ausarbeitung einer Botschaft zuhanden des Parlaments beauftragt. Trotz aller Kritik, welche nach den Enthüllungen von Edward Snowden laut wurde, hält der Bundesrat an allen Schnüffel-Kompetenzen des NDG fest.

Nachrichtendienstgesetz – Bundesrat legt weiteres Vorgehen fest

Ergebnisbericht Vernehmlassung NDG

Medienmitteilung VBS

Gesetzgeber muss Anti-Terror-Datei nachbessern

BGE Einsicht in Staatsschutzakte

BGE Badenfahrt

Über Wanzen, Lecks und Terroristen

«Etliche Spione sind in der Schweiz tätig»

Bericht zum Vorentwurf

Nachrichtendienstgesetz (NDG)

Rechtsvergleich und internationales Recht

MS 2012 Law Enforcement Requests Report

RaBe-Info: Nachrichtendienstgesetz (mp3)

Datenkraken in den USA und in der Schweiz

Zwei gewalttätige SeniorInnen

Fiche Demo «Freiheit für Erdogan!»

Krawallanten präventiv überwachen

Stellungnahme zum neuen Nachrichtendienst-Gesetz

Vernehmlassungsantwort zum neuen Nachrichtendienstgesetz