

Das Panoptikum des digitalen Zeitalters

Über den NSA-Skandal und seine Bedeutung für Luxemburg

„Wir leben in einer Zeit, in der wir von Infrastruktur umgeben sind, die uns zu hintergehen versucht.“⁴¹ Fefe

In den letzten Monaten waren Begriffe wie NSA, PRISM, Tempora und Anhängsel vermehrt in der nationalen und internationalen Presse zu lesen. Was steht hinter diesen Begriffen und in welchem Zusammenhang wird Luxemburg erwähnt? Welche Technik wird bei der all-übergreifenden Überwachung benutzt? Welche Gegenmaßnahmen kann man hier anwenden? Dies sind nur einige der vielen Fragen, die man sich bei diesem Thema stellen kann.

Die NSA (National Security Agency) ist einer der vielen Geheimdienste der Vereinigten Staaten von Amerika. Es ist der größte Auslandsgeheimdienst des Landes und zum Teil vergleichbar mit unserem Geheimdienst, dem SREL (Service de Renseignement de l'État Luxembourg). Die Aufgabe der NSA ist, wie es der Name schon andeutet, für die „nationale Sicherheit“ zu sorgen. Nun wurde in den letzten Monaten durch die Enthüllungen von Edward Snowden bekannt, dass die NSA eine Weltüberwachung betreibt und damit quasi jede Person überwacht, ob US-Amerikaner oder nicht. Dieses Programm wird PRISM genannt und ist nur ein kleiner Teil des gesamten Panoptikums. Die NSA fängt nicht nur die Daten in Echtzeit ab und speichert sie, sondern sie hat auch versucht, Implementierungen von Verschlüsselungsmethoden bewusst zu beeinflussen, so dass es für sie einfacher ist, verschlüsselte Kommunikation zu durchbrechen und mitzulesen. Außerdem steht sie in engem Kontakt mit anderen

Geheimdiensten, vor allem mit dem *Government Communications Headquarters* (GCHQ) des Vereinigten Königreichs. Auch große Unternehmen wie Facebook, Google, Apple, Microsoft und Co. ermöglichen – freiwillig oder gezwungen – diese Überwachung.

Nun stellt sich die Frage, warum die US-amerikanische und britische Regierung dies tun. Terrorbekämpfung wird als Deckmantel für die Überwachung genutzt. Für den Laien mag dies als Rechtfertigung genügen, jedoch wird den meisten nicht bewusst, was dafür geopfert wird. Unsere Freiheiten, die unsere Vorfahren hart erkämpft haben, werden auf einmal vom Tisch gefegt. Rechte, die in der Allgemeinen Erklärung der Menschenrechte festgehalten wurden, gelten auf einmal nicht mehr. Und dies, um eine „nationale Sicherheit“ zu gewährleisten.

Je mehr der Staat über uns weiß, desto mehr kann er uns beeinflussen und dies widerspricht dem demokratischen Grundgedanken. Das Recht auf freie Meinungsäußerung ist eines der höchsten Güter die der Mensch sich gegeben hat. In einer Welt, die an die der Bücher *1984* von George Orwell oder *Brave New World* von Aldous Huxley erinnert, wird dem Mensch die Privatsphäre genommen, die fundamental für das Zusammenleben in einer Gesellschaft ist. Ein latentes Angstgefühl macht sich breit. Auch führt eine Massenüberwachung dazu, dass das Vertrauen innerhalb der Gesellschaft zerstört wird. Jeder weiß von sich selbst, dass er ein guter Mensch ist. Durch die Massenüberwachung kommt es dazu, dass wir uns Fragen stellen, warum z. B. mein Nachbar überwacht wird. Hat dieser etwas zu verbergen? Ist er ein Schwerverbrecher? Diesen psychologischen

Sam Grüneisen
Dennis Fink
Jan Guth

Je mehr der Staat über uns weiß, desto mehr kann er uns beeinflussen und dies widerspricht dem demokratischen Grundgedanken.



CONFIDENTIAL//NOFORN//20291123	
TIER A Comprehensive Cooperation	Australia Canada New Zealand United Kingdom
TIER B Focused Cooperation	Austria Belgium Czech Republic Denmark Germany Greece
	Iceland Italy Japan Luxemburg Netherlands Norway Poland Portugal South Korea Spain Sweden Switzerland Turkey

Die spanische Zeitung *El Mundo* veröffentlichte am 30. Oktober 2013 ein Dokument aus dem Fundus Edward Snowdens mit dem Titel „Sharing computer network operations cryptologic information with foreign partners“

Faktor darf man nicht unterschätzen, denn dadurch entsteht eine allgemeine Paranoia in der Gesellschaft. Jeder Mensch hat Geheimnisse und die Vertreter der Argumentation „Wer nichts zu verbergen hat, hat auch nichts zu fürchten!“, sind sich des Ausmaßes der Bedrohung nicht bewusst.

Luxemburg: Ziel oder Mittäter?

Für die Verantwortlichen in den Regierungsstellen und Nachrichtendiensten sind US-amerikanische Bürger und alle anderen Weltbewohner bei weitem nicht gleichzustellen. Dies hat jeder spätestens am Tag verstanden, an dem die US-Regierung die Abgeordneten zweiter Wahl Mr. Murphy und Mr. Meeks nach Deutschland schickte, um ein „No-Spy“-Abkommen auszuhandeln. Die USA gedenken aber nicht es zu unterschreiben, denn es soll kein Präzedenzfall geschaffen werden. Die Sorge ist zu groß, dass auch andere Länder die gleichen Forderungen wie Deutschland stellen könnten: eine Hinhaltenaktik, die sich bis jetzt immer bewährt hat.

Doch warum soll Luxemburg nun als Mittäter angesehen werden? In einem von Edward Snowden geleakten NSA-Dokument wird Luxemburg als „Tier B“-Land aufgelistet, mit dem angeblich eine engere Kooperation besteht. Was dies nun genau zu bedeuten hat, wissen wahrscheinlich nur die betroffenen Geheimdienste. Doch es lässt sich vieles erahnen. Wir wissen, dass die USA massenweise Daten abschöpfen und das verdachtsunabhängig. Da sich eine lupenreine Diktatur durch totale Überwachung aber nur schwer im Alleingang durchsetzen lässt, lassen CIA und NSA auch Geheimdienste anderer Länder für sich arbeiten. Durch den „Tier B“-Rang Luxemburgs dürften wohl einige Datensätze von Luxemburger Bürgern den Weg in die Datenbanken der NSA finden. Denken wir da nur mal an Skype – der VoIP-Dienst schlechthin und dies weltweit. Skype ist ansässig in Luxemburg und es wäre überaus naiv zu glauben, dass SREL und Co. die Telefonate und/oder Metadaten nicht rausrücken würden (cf. Kasten).

Aus vergangenen Erfahrungen kann man der Untersuchung des Dossiers der nationalen Datenschutzkommission (CNPD) nicht das nötige Vertrauen entgegenbringen, um ernsthaft zu glauben, dass es keinen Spionagedatenaustausch mit den USA gab.

Dass die US-amerikanische Botschaft in Berlin jedmögliche Sensoren auf ihrem Dach installiert hat, um im deutschen Regierungsviertel so viel wie möglich abzuhören, ist mittlerweile bekannt. Nun kann man sich doch fragen, weshalb die Botschaft in Luxemburg nicht in einem Regierungsviertel ist? Sind wir vielleicht ohne es zu ahnen, von der US-Regierung zum einundfünfzigsten Bundesstaat befördert worden und fallen somit nicht mehr unter die weltweite, sondern nur noch die landesinterne Überwachung? Nein, sicher nicht! Doch der Standpunkt der Botschaft ist dennoch sehr günstig gelegen, denn viele wichtige europäische Institutionen liegen im direkten Blickfeld der Botschaft, ohne größere Hindernisse. Für Richtantennen eine hervorragende Voraussetzung. Nun wollen wir jedoch hier nichts unterstellen, sondern nur die geopolitische Lage verdeutlichen. Es gibt allerdings eine Botschaft, die nahe dem Staatministerium und anderen wichtigen Regierungsgebäuden liegt: die des Vereinigten Königreichs. Von der Hausnummer 5 auf dem Boulevard Joseph II bis hin zum Staatsminister sind es grob geschätzt 40 Meter Luftlinie. Eine ideale Distanz zum „Abschnorcheln“ von Daten?

Globaler und lokaler Datenschutz

Schriftsteller aus aller Welt beschriften den Weg, eine weltweite Petition mit dem Titel „Writers against Mass-Surveillance“ zu starten. Die zentrale Forderung ist die Umsetzung eines globalen Datenschutzes, der über die nationalen Grenzen hinausgeht. Doch ist dies der entscheidende Schritt in der Schlacht gegen die Neugierigen oder stellt es ein Ideal dar, das wahrscheinlich weltweit kaum durchgesetzt werden könnte?

Ein globaler Datenschutz würde von mehr als 190 Ländern verlangen, gemeinsam ein Ziel zu erreichen. Doch wenn dies schon beim Umweltschutz nicht klappt, warum sollte die Weltgemeinschaft hierbei erfolgreich sein?

„Le Gouvernement soutiendra les initiatives au niveau de l'Union européenne en vue de la mise en place d'une convention anti-espionnage avec ses partenaires politiques et économiques“, schreibt die neue Regierung in ihrem Koalitionsprogramm.² Unter dem Titel „Demokratische Erneuerung“, kündigt die Koalition an, dass sie ein „No-Spy-Abkommen“ auf europäischer Ebene unterstützen möchte. Doch

ist dies der richtige Weg? Und scheren sich die Geheimdienste überhaupt um solche Gesetze, wenn sie sich doch bereits jetzt schon über unzählige andere Paragraphen hinwegsetzen?

Würden wir mit einem nationalen (lokalen) fundierten Datenschutz den richtigen Weg beschreiten? Die Autoren dieses Artikels stehen hinter dieser Auffassung! Man muss sich darüber im Klaren sein, dass die Forderung nach mehr „Datenschutz“ auch andere Prinzipien beinhaltet, wie bspw. Netzneutralität, die Freiheit der Informationen, OpenData und noch andere, die sicherstellen, dass das Internet ein freies und kreatives Netz bleiben kann. Ein in der Verfassung verankerter Datenschutz, kombiniert mit strengen nationalen Gesetzen, würde nicht nur die Datensätze der Bürger verteidigen oder den Wirtschaftsstandort attraktiver machen, sondern der betreffende Staat würde auch als Vorbild angesehen werden. Diese pädagogische Rolle des Vorbilds ist fast ebenso wichtig wie die des Schutzes der Daten.

Revolution oder Revolte?

Wie geht man gegen einen Feind vor, der über unendlich große Ressourcen verfügt und sich über Gesetze hinwegsetzt? Ziviler Ungehorsam stellt eine Möglichkeit dar. Proteste, Mahnmale und Aktivismus helfen und können Hoffnungsträger sein. Es liegt ein Hauch von Revolution in der Luft. Ägypten, Tunesien und die Ukraine machen es vor.

Doch auch die Technologie kann man gegen den Staat und deren Spitzeldienste benutzen. Hierbei spielt Kryptografie eine gewichtige Rolle. Wer dem Joch der globalen Massenüberwachung entfliehen will, der kann sich so genannten „Cryptopartys“ anschließen. Hier lernt der Bürger z. B. den Umgang mit Verschlüsselungssoftware und wie man anonym im Internet surfen kann. Auch gibt es nun vermehrt Organisationen, die Dienste zur anonymen Kommunikation bereitstellen. Lokal gibt es zum Beispiel den Tochterverein des Chaos Computer Clubs Lëtzebuerg namens Frënn vun der Ënn, der weltweit Tor-Server betreibt. Tor ist eine Software, die jedem erlaubt, anonym im Internet zu surfen.

Erkenntnisse aus den vergangenen Monaten

Eine Erkenntnis ist, dass die Presse ein wichtiger Bestandteil unserer Demokratie ist. Sie darf nicht nur als Anhängsel angesehen, sondern muss zum vierten Pfeiler der Demokratie aufgewertet werden. Sie hat als Aufgabe, Missstände in der Legislative, Judikative und Exekutive aufzuzeigen. Auch müssen Whistleblower adäquat geschützt werden. Das Recht auf Anonymität für Informanten muss fest im Gesetz

verankert werden, weil sie unabdinglich ist, um solche Missstände aufzudecken.

Ein nicht zu unterschätzender Punkt ist die friedliche Präsenz auf der Straße in Form von Demonstrationen. Denn es reicht nicht, nur in sozialen Netzwerken zu teilen und zu liken, sondern die Bürger müssen aktiv werden und beispielsweise Petitionen oder Proteste organisieren. Deshalb gilt weiterhin: „Verbreite die Nachricht und geh auf die Straße!“ ♦

1 <https://blog.fefe.de/?ts=ac5169c5>

2 Koalitionsprogramm Regierung 2013 - <http://www.gouvernement.lu/3322796/Programme-gouvernemental.pdf> (Seite 10)

Auszüge aus der Aktennotiz von SREL-Direktor Patrice Heck an Premierminister Jean-Claude Juncker vom 24. Juni 2013*

„Le SRE n'a pas de système PRISM. Le SRE ne participe pas au système PRISM. Le SRE n'a jamais été destinataire direct et n'a jamais sollicité des données personnelles venant spécifiquement et directement de ce système; il n'a pas d'accès à la plateforme PRISM et n'a pas demandé un tel accès. Évidemment nous coopérons avec les services américains mais nous ignorons si les services américains se sont procurés des données personnelles et/ou autres informations qui nous auraient été transmises à partir du système PRISM.“

„les autorités US et UK avaient demandé en décembre 2010 à trouver un accord avec le gouvernement luxembourgeois pour solliciter son aval pour la mise en place à Luxembourg d'une plateforme d'interception des communications moyennant une technologie d'interceptions nouvelle. Après de longues et compliquées négociations le gouvernement avait fait parvenir à la société [blanc]** une lettre signée par le Premier Ministre invitant la société [blanc] à ne pas installer cette plateforme à Luxembourg mais à l'installer dans d'autres pays notamment ceux dont les ressortissants ou résidents étaient visés.“

„La Commission de contrôle parlementaire du SRE avait été informée de la problématique [blanc] à trois reprises :

- Le 29 juin 2007 où le Directeur du SRE explique le problème de l'impossibilité d'interception des communications générées par le logiciel [blanc] et l'augmentation des demandes de la part de services partenaires [...]

- Le 23 février 2010 où le Directeur du SRE (Mille) avait informé la Commission de ce que USA et UK étaient en train de développer une nouvelle technique d'interception en mettant la pression sur le Luxembourg pour mieux coopérer en ce sens.

- Le 1^{er} novembre 2011 où le SRE informe la Commission des pourparlers en cours avec USA, UK et [blanc].“

* aus: Annexes au Rapport de la Commission d'enquête sur le Service de Renseignement de l'Etat, 25.7.2013, Chambre des députés, N° 6565, S. 1024f. (veröffentlicht am 11.7.2013).

** Skype ist mit hoher Wahrscheinlichkeit das Softwareunternehmen, auf das in der Aktennotiz verwiesen wird. (Siehe I. Kurschat, „Abscheuliche Berichte“, d'Lëtzeburger Land, 12.7.2013.)