

**Was weiß der Staat von uns?**

Autoren: Gábor Paál und Simone Hamm

**Ansage:**

Was weiß der Staat von uns?

Von Gábor Paál und Simone Hamm

**Cut 1: Mann von der Einwanderungsbehörde**

What's the purpose of your journey?

How long do you want to stay in the U.S.A.?

In which hotel are you going to stay?

**Übersetzer 4**

Was wollen Sie in den USA?

Wie lange wollen Sie in den USA bleiben?

In welchem Hotel werden Sie wohnen?

**Sprecherin:**

Nach dem 11. September 2001 haben sich die Vereinigten Staaten verändert. Die Angst vor weiteren Terroranschlägen ist groß. Der Anschlag auf die Bostoner Marathonläufer 2013 hat die Nervosität noch gesteigert. Jeder, der schon einmal in die USA geflogen ist, kann sie am Einwanderungsschalter spüren – wie hier in einer nachgestellten Szene.

**Cut 2: Mann von der Einwanderungsbehörde**

In which hotel are you going to stay?

How long do want to stay?

How much money do you have with you?

**Übersetzer 4**

In welchem Hotel werden Sie wohnen?

Wie lange wollen Sie bleiben?

Wie viel Geld haben Sie dabei?

**Sprecherin:**

Jede Fluglinie hat von jedem ihrer Passagiere 34 Datensätze weitergegeben; darunter die Telefonnummer, die Kreditkartennummer, auch der Wunsch nach einem vegetarischen Essen oder einem Fischmenü. Und die Mitarbeiter der Einwanderungsbehörde können – ohne Angabe von Gründen – jeden abweisen. Und diese Situation des Passagiers am Flughafen ist nur ein kleiner Ausschnitt der Gesamtsituation in den USA.

**Cut 3: Edward Snowden**

I sitting ... personal e-mail.

**Übersetzer 2:**

Ich hatte die Befugnis, von meinem sicheren Schreibtisch aus, jeden, wirklich jeden auszuspähen, dich, deinen Steuerberater, bis hin zu einem Bundesrichter, ja sogar den Präsidenten. Jeden, dessen private E-Mail-Adresse ich gehabt hätte.

**Sprecherin:**

Bis der Whistleblower Edward Snowden die Praktiken der NSA ans Licht brachte, war in der öffentlichen Diskussion die staatliche Überwachung – zumindest in Demokratien – in den Hintergrund getreten. Datenschützer lenkten die Aufmerksamkeit mehr auf die aus ihrer Sicht eigentlichen Datenkraken: die großen Internetfirmen, die Suchmaschinen und sozialen Netzwerke. Durch all die Daten, die Nutzer dort freiwillig von sich preisgeben, seien Datenschutz und Privatsphäre viel stärker gefährdet als durch die Aktivitäten des Staates. Doch die NSA-Affäre hat deutlich gemacht, wie private und staatliche Datensammelei miteinander verwoben sind. Die NSA bedient sich schließlich vor allem bei US-Konzernen wie Google, Microsoft, Facebook oder Apple. Sie greift auf die dort gespeicherten Nutzerdaten zu, sie späht Banken- und Kreditkartentransaktionen aus, sie überwacht die Telefonverbindungen von US-Bürgern und Ausländern. Wer hat mit wem wie lange telefoniert? Wer ist mit wem auf Facebook befreundet? Wer sucht was bei Google? Diese Eingriffe in die Privatsphäre werden mit „Sicherheit“ und „Kampf gegen den Terrorismus“ begründet. Die meisten Amerikaner nehmen sie achselzuckend in Kauf.

*Atmosphären-Wechsel auf Estland***Sprecher:**

Wie anders dagegen die Situation in Estland. Auch der estnische Staat weiß theoretisch eine Menge über seine Bürger. Kaum ein anderes Land der Welt ist so umfassend in allen Bereichen digitalisiert. In den staatlichen Datenbanken lagern etliche Informationen über die Bevölkerung. Der Unterschied liegt darin, wie der Staat damit umgeht. Anders als in den USA hat in dem kleinen Ostsee-Staat längst jeder Bürger einen elektronischen Ausweis. Fast alles ist damit verknüpft. Im Alltag braucht man keinen Führerschein mehr und keine Krankenversicherungs-Karte. Vom Busticket über die Steuererklärung bis zum Gesundheitswesen – alles läuft über den elektronischen Ausweis – die „E-ID“. Sergej Voronetski zum Beispiel ist Sportarzt. Er hat viele Patienten mit chronischen Erkrankungen. Wenn die ein Rezept brauchen, müssen sie nicht extra zu ihm kommen. Sergej kann das Rezept im Internet ausstellen und auf den Namen des Patienten hinterlegen. Dieser muss dann nur noch mit seinem elektronischen Personalausweis zur Apotheke gehen.

**Cut 4: Voronetski**

Das bedeutet in ganz Estland kann der Patient die Arznei kaufen, ohne Probleme.

**Sprecher:**

Gerade bei älteren Patienten ist dieses Verfahren beliebt, sagt Voronetski:

---

**Cut 5: Voronetski**

Ältere akzeptieren alles, sehr schnell, sie brauchen nicht mehr so viel Papier und können auch durch Internet und E-Books kontrollieren, welche Arzneien brauchen sie zusätzlich zum Beispiel.

**Sprecher:**

Der Arzt kann aber noch mehr: Sämtliche Befunde eines Patienten sind in der zentralen staatlichen Gesundheitsdatenbank gespeichert. Kein Patient muss mehr mit seinem Röntgenbild von Arzt zu Arzt laufen oder darum bitten, dass Ärztin A einen Bericht an Ärztin B schickt – denn jeder behandelnde Arzt hat Zugriff auf die Daten seiner Patienten. Sergej Voronetski ruft im Internet eine Kernspin-Aufnahme auf. Sie zeigt das Knie eines Patienten:

**Cut 6: Voronetski**

Der Patient hat mich angerufen, dass diese Aufnahme schon gemacht wurde, und ich kann das angucken und untersuchen. Und ich habe festgestellt, dass er Probleme mit seinem Miniskus hat, eine Miniskuszerrung – hier kann man das sehen – und dieser Patient braucht meinen Termin nicht, sie braucht jetzt nur eine Operation, einen OP-Termin.

**Sprecher:**

Von jedem Esten sind auf diese Weise jede Menge persönlicher Informationen in den staatlichen Datenbanken hinterlegt. Mit dem elektronischen Ausweis machen die Esten ihre Steuererklärung, erledigen Bankgeschäfte und können online wählen. Insgesamt sind es mehr als 160 staatliche Dienstleistungen, für die der Ausweis gut ist. Einer seiner größten Verfechter ist Staatspräsident Toomas Hendrik Ilves. Er sieht das System auch als eine Maßnahme zum Bürokratieabbau:

**Cut 7: Ilves**

You can ... government's job.

**Übersetzer 3:**

Sie können eine Firma in Estland in 10 bis 15 Minuten registrieren. Dabei verlangen unsere Ämter die gleichen Informationen wie andere Länder auch: Die Namen der Geschäftsführung. Den Nachweis, dass Sie keine Vorstrafen haben und keine Steuern schuldig sind. Der Unterschied ist, in anderen Ländern brauchen Sie für die Registrierung drei Wochen, vielleicht sogar Monate. Denn dort müssen Sie zu den einzelnen Ämtern gehen und sich die einzelnen Bescheinigungen auf Papier aushändigen lassen. In Estland, wo wir das alles elektronisch machen, geht das in zehn Minuten. Denn wir haben auch ein Gesetz, wonach der Staat Sie nicht nach Informationen fragen darf, die er bereits hat. Nehmen wir also an, Sie wollen ein Unternehmen anmelden, dann legen Sie einfach ihren elektronischen Ausweis vor, das System sucht sich dann die notwendigen Informationen in den verschiedenen Behörden zusammen. Sie müssen deshalb nicht den Nachweis bringen, dass keiner in ihrer Geschäftsleitung Steuerschulden hat. Sondern das ist der Job des Staates.

**Sprecher:**

In den Ohren vieler deutscher Bürgerrechtlicher und Netzaktivisten läuten bei all diesen Beispielen die Alarmglocken. Online-Wahlen lehnt selbst die netzaufgeschlossene Piratenpartei ab. Zu unsicher. Krankenakten in einer zentralen Gesundheitsdatenbank? Nur mal angenommen, der deutsche Innenminister würde eine solche „Bundes-Cloud“ vorschlagen, also eine Bundes-Datenwolke, bei der alle Informationen eines Bürgers mit einem digitalen Ausweis-Schlüssel verknüpft sind – die Proteste wären groß, nicht nur in der Netzgemeinschaft. Wie gelassen dagegen klingt der estnische Netzaktivist Siim Tuisk.

**Cut 8: Tuisk**

The Germans have ... has been done.

**Übersetzer 1:**

Gerade von den Deutschen kommen solche Bedenken oft. Aber wenn man sich ansieht, wie das estnische ID-Karten-System verknüpft ist mit 160 Diensten, dann macht es Sinn. Es stimmt schon, es ist eigentlich irre, wie viele Informationen der Staat über einen hat. Andererseits sind die Esten hier sehr liberal, sie sehen die Probleme noch nicht, die mit Big Data aufkommen, um zu erkennen, was der Staat damit anstellen kann. Ich kenne aber kein Beispiel, dass unser Staat die Daten missbraucht hätte. [Ich will nicht ausschließen, dass es Missbrauchsmöglichkeiten gibt, aber ich kenne keinen Fall, wo das passiert wäre.]

*Atmosphärenwechsel USA***Sprecherin:**

In den USA, dem Mutterland der Internetindustrie, zahlt man die Miete, den Arzt, das Karatewochenende oder den Geigenunterricht noch mit Schecks. Rezepte muss man beim Arzt abholen oder sich faxen lassen. [Und ohne das alte, meist handgeschriebene Rezept gibt es keine Medikamente.] Natürlich sind US-Amerikaner auch im Internet aktiv. Doch wissen sie genau: Ob sie Mails schreiben oder googeln, im Zweifel bleibt nichts geheim. Mag sein, dass viele US-Bürger ihrem Staat vertrauen. Sicher ist aber: Der Staat vertraut seinen Bürgern nicht. Und erst recht nicht Ausländern, die in den USA leben.

**Cut 9: Peter Lüders**

Ich kam mit meinem Assistenten am Schalter an. Er kriegte seinen Boarding-Pass. Bei mir haben die ja nur gesagt, sorry unser Computer funktioniert nicht mehr richtig. Sie können jetzt leider keinen Boarding-Pass mehr bekommen. Die links und rechts von mir kriegten alle ihren Boarding-Pass, nur ich nicht:

**Sprecher**

Peter Lüders ist Fotograf und Vielflieger. Er lebt in New York. Er will wissen, warum man ihn am Flughafen aufhält und er bangen muss, ob er überhaupt mitfliegen darf.

**Cut 10: Peter Lüders**

---

Da haben sie mir dann gesagt, dass ich mehrere Level 2-Warnings hätte in meiner Polizeiakten. Und da meinte ich, was ist denn ein Level 2-Warning?

**Sprecherin**

Ein Level-Two-Warning bedeutet: Warnstufe 2. Eine Stufe über Warnstufe 1. Warnstufe 1 bekommt jemand, der der Polizei so verdächtig erscheint, dass sie es für notwendig hält, ihn nach seinem Ausweis zu fragen. Ob sich der Verdacht erhärtet oder in Luft auflöst, spielt dann keine Rolle mehr. „Warnstufe 1“ steht von nun an in den Akten. Bei einer Verdachtskontrolle in einer kritischeren Situation erhöht sich die Warnstufe auf 2. Peter Lüders ahnt, wie er dazu gekommen ist: Er war zuvor von New York den Hudson hinauf nach Saratoga gefahren, eine dreistündige Zugfahrt. Doch in Hudson Valley endet sie für ihn.

**Cut 11: Peter Lüders**

Nach ungefähr der Hälfte der Fahrt hält der Zug plötzlich an und der Schaffner stürmt mit zwei Polizisten herein und ruft: „That's the guy, that's the guy!“ Und die packen mich und schmeißen mich gegen die Wand, legen mir Handschellen an und sie zerren mich raus und zerren mich an allen Leuten vorbei. Ich wurde ins Polizeiauto gesteckt. Und ich hab natürlich gesagt, was wollen Sie, Sie müssen mir sagen warum.

**Sprecherin:**

Die Polizisten müssen nicht sagen, warum sie den Zug gestoppt haben, nicht, warum sie Peter Lüders in Handschellen abgeführt haben und auch nicht, warum sie ihn in das Polizeiauto bugsiiert haben. [Allenfalls hätten sie Lüders, einen Deutschen, darauf aufmerksam machen müssen, dass er seine Botschaft hätte anrufen dürfen.]

**Cut 12: Peter Lüders**

Ich war da eingeklemmt, die Hände waren hinterm Rücken. Die Handschellen werden einem angelegt, da wird der eine Arm verdreht. Das ist extrem unangenehm. Er ging mir langsam die Luft raus. Ich dachte, ich bin jetzt wie so ein Kleinkind oder ein Hund auf der Rückbank und erstickte dann gleich. Ich hatte die Hände in Handschellen und konnte auch nicht winken und ich habe dann versucht, Gesten zu machen oder so, aber die guckten gar nicht rüber. Und dann habe ich eben immer mit dem Kopf gegen das Fenster geknallt, und die dachten nur, ich versuche jetzt durch das Fenster auszubrechen. Und kamen dann mit gezogenen Pistolen auf mich zugerannt und schrien alle, bis ich ihnen klarmachen konnte, dass ich kurz vorm Ersticken war.

**Sprecherin:**

Nach einiger Zeit, die Peter Lüders endlos erscheint, fahren die Polizisten mit ihm los und bringen ihn in ein Gefängnis.

**Cut 13: Peter Lüders**

Der Chef der Homeland Security kam aus Albany angefahren, ein älterer, farbiger Polizist, der aussah wie Morgan Freeman und der einzige ein bisschen schlauere der

Jungs dort zu sein schien. [Die Polizisten dort wollten ihm aber eindeutig beweisen, dass sie einen echten Terroristen gefangen hatten.] Da haben sie mir dann das erste Mal erzählt warum. Ich habe telefoniert, auf Deutsch. Eine Frau, die im Zug sitzt, hat angeblich gehört, wie ich am Mobiltelefon arabisch gesprochen hätte und dem mehrfach das Wort Bombe sagte. Der Schaffner, [dem sie das erzählt hatte,] ist daraufhin selber in Panik geraten, weil er dachte, sein geliebter Zug wird gleich die Luft fliegen und hat dann die örtliche Polizei angerufen. Die dachten, jetzt hätten sie endlich mal einen Terroristen.

**Sprecherin:**

Der Chef der Homeland Security weist die Polizisten an, Peter Lüders freizulassen. Die Reisende im Zug habe sicher überreagiert. Doch obwohl unschuldig, trägt Lüders von nun an den Makel eines Verdächtigen, steht mit einem Level-2-Warning in den Polizeiakten. Und deshalb wurde ihm am Flughafen die Bordkarte nicht ausgehändigt. Zumindest ist das der Zusammenhang, den er vermutet. Offiziell gibt ihm niemand eine Begründung. Möglicherweise hat der Staat ja noch andere Motive, ihn als Terrorverdächtigen einzustufen? Vielleicht ist er auch schon im Visier der NSA?

**Cut 14: James Bamford**

Basically it's like a giant firehouse, instead of water communications coming out ... have to use a shotgun approach.

**Übersetzer 2:**

Das Internet ist wie ein gigantisches Feuerwehrhaus. Nur dass aus den Schläuchen Kommunikation kommt statt Wasser. Und die NSA filtert die Kommunikation nach Telefonnummern, E-Mails und jeder Satz, jedes Wort, dass man bei Google eingegeben hat. Das ist wie mit Kanonen auf Spatzen schießen.

**Sprecherin:**

James Bamford war der erste, der ein Buch über die NSA geschrieben hat. Er ist Gastdozent in Berkeley und schreibt für die New York Times. Und warnt vor der bedenkenlosen Nutzung des Internets. Google zum Beispiel hat Daten von Milliarden von Nutzern. Jede Suchanfrage wird aufgezeichnet. Ein wesentlicher Unterschied zum vielzitierten „Big Brother“ in Orwells Zukunftsroman „1984“, meint Bamford. Der Big Brother habe nur gewusst, was jemand laut ausgesprochen habe. Doch wer all die Nutzeranfragen bei Google kennt, kennt auch die Gedanken, Wünsche und Hoffnungen, die unausgesprochen bleiben. Der ehemalige Google-Chef Eric Schmidt hat inzwischen in den Aufsichtsrat gewechselt, ist aber noch immer der oberste Repräsentant des Konzerns. Zusammen mit dem Google-Vordenker Jared Cohen hat er das Buch "Die Vernetzung der Welt" geschrieben. Eine Privatsphäre, so Eric Schmidt, werde es nicht mehr geben. Nicht auf der Straße und nicht im Netz.

**Zitat/Übersetzer 5: (Eric Schmidt)**

Das Sicherheitsargument wird immer schwerer wiegen als private Anliegen. Die Hardliner müssen nur auf ein schockierendes Ereignis warten, um die politische

---

Unterstützung für ihre Projekte zu finden und sich über Bedenkenträger hinwegzusetzen. [Die Betreiber umfangreicher Datenbanken werden früher oder später gegen die gesetzlichen Einschränkungen verstoßen.

**Sprecherin:**

Auch Google verfügt über eine umfangreiche Datenbank. Dennoch könnten sich die Nutzer der Suchmaschine sicher fühlen, beteuert Eric Schmidt.

**Cut 15: Eric Schmidt**

In America, which I know very well, we won't respond to a friendly request from the government unless it is accompanied by a court order.

**Übersetzer 5:**

In Amerika, das ich ja nun gut kenne, wird Google nicht auf eine freundliche Anfrage der Regierung reagieren und Daten einfach so freigeben, sondern nur, wenn das von einem Gericht angeordnet worden ist.

**Sprecherin:**

Die Regierung braucht gar nicht freundlich anzufragen.] Seit 1978 gibt es den Foreign Intelligence Surveillance Court, ein Gericht, speziell dafür da, die Auslandsgeheimdienste – also auch die NSA – zu kontrollieren. Es besteht aus 11 Bundesrichtern, die diese Kontrollfunktion abwechselnd und nur nebenberuflich ausüben. Sie entscheiden darüber, ob abgehört werden darf oder nicht.

**Cut 16: Bamford**

The NSA ... of a nightmare.

**Übersetzer 2:**

Die NSA betont, dass das alles richterlich geprüft worden sei. Was sie nicht sagen, ist, dass dieses Gericht ein Traum von Franz Kafka sein könnte. Das Gericht tagt im Verborgenen. Niemand weiß wo. Es findet unter Ausschluss der betroffenen Personen statt. Es gibt keine Möglichkeit, sich zu verteidigen. Es gibt keine Aufzeichnungen von den Entscheidungen dieses Gerichtes. Niemand weiß, was dort passiert. Niemals erfährt man etwas von den Urteilen. Es ist ein Albtraum.

*Atmosphärenwechsel – Estland***Cut 17: Ilves**

There is ... doesn't work.

**Übersetzer 3:**

So etwas wie Vertrauen gibt es im Cyberspace nicht. Ich meine, heute kann jeder in meinen E-Mail-Briefkasten schauen, wahrscheinlich passiert das auch. Da gibt es keine Sicherheit. Doch die Grundlage für jede echte Internetgesellschaft ist, dass Ihre Identität verlässlich ist, dass Ihr Gegenüber sicher sein kann, dass Sie der sind, für

---

den Sie sich ausgeben. Und dazu brauchen Sie ein System, das mindestens so sicher ist wie unseres.

**Sprecher:**

Der estnische Präsident Toomas Hendrik Ilves ist vermutlich das einzige Staatsoberhaupt der Welt, das schon als 13-Jähriger in den 1960er-Jahren erste Erfahrungen mit Computerprogrammen gemacht hat. [Aufgewachsen ist er in den USA, als Sohn estnischer Exilanten. 1993 wurde er Botschafter Estlands für die USA, Kanada und Mexiko. Doch schon in dieser Funktion forcierte er, von Washington aus, die Digitalisierung seines Landes.] Dass ausländische Geheimdienste seine E-Mails lesen oder sein Handy ausspionieren – das war ihm schon vor der NSA-Affäre klar. Manchmal würde er aus Spaß gerade E-Mails mit banalem Inhalt besonders gut verschlüsseln, um dem russischen Geheimdienst etwas zu tun zu geben, sagt Ilves.

**Cut 18: Ilves**

What's ... my card.

**Übersetzer 3:**

Oder nehmen Sie Bezahl-Systeme wie Paypal oder Kreditkarten. Wenn ich damit im Internet bezahle, muss ich eine sogenannte „Prüfnummer“ eingeben. Die besteht aus drei Ziffern, da denke ich, was soll das? Haben Sie in sowas Vertrauen? – Ich nicht. Die einzigen Daten, bei denen ich mich darauf verlasse, dass sie sicher sind, sind gerade diejenigen, die ich mit meinem elektronischen Personalausweis eingebe und mit unserem System verschlüssele.

**Sprecher:**

Estland war 2005 das erste Land, das Online-Wahlen einführte. Zunächst bei den Kommunalwahlen, später auch bei den Parlamentswahlen. In Deutschland geht das noch lange nicht. Der bayerische Finanzminister Markus Söder hat in Bayern Online-Wahlen für 2018 angekündigt, steht damit in Deutschland allerdings allein auf weiter Flur. Selbst die sonst so netzaufgeschlossenen Piraten halten Online-Wahlen für zu unsicher. In Estland dagegen haben bei den letzten Wahlen jeweils etwa ein Viertel der Wahlberechtigten diese Möglichkeit genutzt.

**Cut 19: Ilves**

Okay, so this is ...

**Sprecher:**

Er mache das zum ersten Mal, sagt Priit Ennet, als er bei den Kommunalwahlen online seine Stimme abgibt. Er macht das von seinem Laptop im Büro aus. Gerade noch rechtzeitig: In einer halben Stunde schließt die digitale Wahlkabine.

**Cut 20: Ennet**

So let's see ...

**Übersetzer 4:**



---

Schauen wir mal, wie das geht. Ich nehme meinen elektronischen Personalausweis, der ähnelt ein bisschen einer Kreditkarte, und stecke ihn in meinen Kartenleser, den ich am Computer angeschlossen habe.

**Sprecher:**

Für Online-Wahlen hat der Staat eine eigene Seite eingerichtet.

**Cut 21: Ennet**

So now ... (*Tastentippen*)

**Übersetzer 4:**

Jetzt werde ich gebeten, mich zu identifizieren. Das kann ich mit meinem Ausweis oder meinem Handy machen. Ich klicke auf „Ausweis“. Jetzt werde ich nach meinem Pin-Code gefragt.

**Sprecher:**

Ein paar Klicks später findet Priit die Liste der Kandidaten, nach Parteien geordnet.

**Cut 22: Ennet**

Now ... taken into account.

**Übersetzer 4:**

Ich suche meinen Kandidaten oder meine Kandidatin und klicke ihn bzw. sie an. Jetzt steht da: Sie haben sich für diese Person von dieser Partei entschieden. Ich klicke den nächsten Button mit der Aufschrift: Wählen. Dann muss ich noch einmal meine Wahl bestätigen. Und jetzt werde ich nach meiner zweiten Pin gefragt ... Ich klicke nochmal „okay“. Und ich bekomme die Mitteilung: Ihr Stimme wird nun gezählt.

**Sprecher:**

[Priit könnte sich nun auch ein zweites Mal anmelden und erneut wählen. Die zweite Wahl würde die erste ungültig machen. Es zählt immer nur seine jeweils letzte abgegebene Stimme.] Zu den Sicherheitsvorkehrungen beim elektronischen Personalausweis gehört die doppelte Signatur. Deshalb auch die beiden Pin-Nummern: Mit der einen identifiziert man sich lediglich als Inhaber des Ausweises. Doch um die entsprechende Anwendung durchzuführen – in dem Fall die Online-Wahl – ist eine zweite Signatur und somit eine zweite Pin notwendig. Nach der Wahl sind die beiden Informationen – die Identität des Nutzers einerseits und wen er gewählt hat andererseits – nicht mehr miteinander verknüpft.

**[Cut 23: Priit Ennet**

The programmers ... in this form.

**Übersetzer 4:**

Die, die das System programmiert haben, sagen jedenfalls, dass es aufgrund der Verschlüsselung unmöglich ist herauszufinden, wer für wen gestimmt hat. Bisher

---

jedenfalls gab es noch keine Sicherheitsprobleme – wenn es dazu käme, wäre das wohl das Ende.]

**Sprecher:**

Zwar gab es in den vergangenen Jahren ein paar kleinere technische Pannen, aber es wurden keine gezielten Manipulationen bekannt. Zumindest würden diese auffallen, meint der Netzaktivist Siim Tuisk. Er hält die Online-Wahlen und den elektronischen Ausweis heute für eine gute Sache.

**Cut 24: Tuisk**

The activists ...

**Übersetzer 1:**

Wir Aktivisten haben zehn Jahre lang immer wieder mögliche Sicherheitsprobleme angesprochen. Jetzt werden sie berücksichtigt. Insofern bin ich schon im Großen und Ganzen zufrieden.

*Zitate über getragenes Bett*

**Zitator:**

Angenommen, ich würde in den Vereinigten Staaten, Frankreich, Großbritannien, Russland oder China leben ...

**Sprecher:**

... schreibt der estnische Bürgerrechtler und IT-Experte Otto de Voogd in einem Blogbeitrag.

**Zitator:**

Ich würde die Vorstellung, dass mein Staat mir ein Verschlüsselungssystem anbietet, aber selbst keine Kopie des Schlüssels behält, in weniger als einer Mikrosekunde ins Reich der Fantasie verbannen. Es wäre undenkbar, dass eine Regierung in einem dieser Länder ihren Bürgern ein System zur Verfügung stellt, das nicht einmal der Staat selbst knacken könnte.

**Sprecher:**

Netzaktivisten, die ihre Regierung auf dem richtigen Weg sehen und für sie auch mal ein gutes Wort einlegen – so etwas findet man wohl in kaum einem anderen demokratischen Land der Welt. Warum also haben die Esten offenbar so viel Vertrauen in ihren Staat?

**Cut 25: Ilves**

I'am always ... digital illiterate level, the discussion.  
Entschuldigen Sie, aber in Deutschland, das ist Wahnsinn.

**Übersetzer 3:**

---

Ich bin immer perplex, wenn mir diese Frage gestellt wird. Ich finde die Diskussion in den meisten Staaten läuft auf dem Niveau von digitalen Analphabeten

**Sprecher:**

Toomas Hendrik Ilves ist nicht der Typ von Staatsoberhaupt, der seine Worte vorsichtig abwägt und sich hinter wohlfeilen blumigen Phrasen versteckt.

**Cut 26: Ilves**

The fact that ...

**Übersetzer 3:**

Die Tatsache, dass die NSA und andere jederzeit Ihren Mail-Account lesen können, hat nichts mit dem zu tun, was wir haben. Ich höre oft das Argument aus dem Ausland: So was wie ihr, das können wir nicht machen, wir haben Angst vor Big Brother. Ich Sorge mich aber nicht vor dem „Big Brother“, sondern vor Big Data. Davor, dass Unternehmen all die Daten, die sie von mir haben, gegen mich verwenden. Und auch die NSA hat ja auf die Daten bei Google und Facebook zurückgegriffen, die Menschen im Netz freiwillig von sich preisgegeben haben.

**Sprecher:**

Für den estnischen Präsidenten folgt daraus, dass man in der digitalen Gesellschaft nur die Wahl hat, entweder alle Geräte abzuschalten und gar nicht online zu kommunizieren, oder eben ein wirklich sicheres System zu entwickeln. Das estnische System hält er für sicher. Ilves vergleicht es mit dem von Lavabit – dem US-amerikanischen E-Mail-Service, den auch Edward Snowden genutzt hat. Selbst die NSA war nicht in der Lage, die Lavabit-Verschlüsselung zu knacken und hat deshalb den Betreiber unter Druck gesetzt.

**Cut 27: Ilves**

And so Lavabit was ...

**Übersetzer 3:**

Das war das Ende von Lavabit. Wir verwenden nun dieselbe Methode wie Lavabit, mit einem Unterschied: Sie hatten einen Verschlüsselungsstandard von 512 Bits. Unserer hat 2048 bits, ist also nochmal um zwei Sicherheitsstufen besser.

**Cut 28: Tuisk**

Basically ...

**Übersetzer 1:**

Man muss sagen, dass diese ganze E-Government-Idee nicht in der Regierung geboren wurde, sondern eher von den Internet-Freaks der Regierung verkauft wurde.

**Sprecher:**

... erklärt der Netzaktivist Siim Tuisk.

---

**Cut 29: Tuisk**

The Politicians ... and so on.

**Übersetzer 1:**

Die Politik hat das unterstützt, aber der Impuls kam von außen. Und die Menschen haben den Netzaktivisten dahinter vielleicht mehr vertraut als sie es normalerweise Politikern gegenüber tun. Vielleicht schwingt da auch ein Stück Stolz mit.

**Sprecher:**

Die Gefahr, dass der Staat seine Informationsmacht missbraucht, sieht Tuisk zwar, hält sie aber in Estland für derzeit gering. Schließlich sei das System so angelegt, dass niemand unbemerkt die Daten eines Bürgers einsehen kann.

**Cut 30: Tuisk**

The system ...

**Übersetzer 1:**

Wenn irgendjemand in irgendeiner Behörde auf meine Daten zugreift, wird das automatisch registriert. Mit Ausnahme vielleicht von den Geheimdiensten. Aber wenn die Polizei oder das Landwirtschaftsministerium meine Daten aufrufen, werde ich darüber informiert.

*Zitate über Atmo*

**Zitator:**

Da wir über Estland reden, bin ich bereit, die Möglichkeit in Betracht zu ziehen, dass der Staat ehrlich zu uns ist.

**Sprecher:**

... schreibt der estnische Bürgerrechtler und IT-Experte Otto de Voogd.

**Zitator:**

Ich hoffe, dass es so ist und dass ich auf wundersame Weise in einem der besten Länder lebe, was die Privatsphäre und den Schutz unserer Bürgerrechte betrifft.

**Sprecher:**

Zugegeben, Estland hat, was Terroranschläge betrifft, weitaus weniger Sorgen als die USA.

*Atmowechsel USA*

**[Cut 31: Eric Schmidt**

It's very ... it's very hard to take out ...

**Übersetzer 5:**

---

Für eine Regierung ist es sehr einfach, in die Privatsphäre einzudringen. Und dagegen sollte man kämpfen. Ist erst mal ein System der Überwachung installiert – wird man es so leicht nicht wieder los.

**Sprecherin:**

... sagt Eric Schmidt von Google. Er weiß, wovon er spricht. Denn nicht nur befreundete Staatsoberhäupter werden ausgespäht. Auch Google und Microsoft wurden gezwungen, Informationen über Zehntausende von Kundenkonten herauszugeben. Aus Sorge, dass ihre Nutzer sich zurückziehen werden, haben AOL, Facebook, Google, LinkedIn, Microsoft und Yahoo einen offenen Brief an Präsident Obama geschrieben und folgende Leitforderungen aufgestellt.

**Zitator:**

Einschränkung der Macht der Regierung, Nutzerinformationen zu sammeln.  
Transparenz über das, was die Regierung abrufen.  
Respekt vor dem freien Fluss der Information.]

**Sprecher:**

Im Januar 2014 hat Präsident Obama eine Reform angekündigt und Mäßigung gelobt, zumindest was die Bespitzelung der eigenen Bevölkerung betrifft. Auch sollten in der Regel keine Regierungschefs befreundeter Staaten mehr abgehört werden. Telekommunikationsdaten würden weiterhin gesammelt, nur nicht direkt bei der NSA, die Speicherung solle privatisiert werden. Ein No-Spy-Abkommen wollen die USA aber nicht abschließen. Immer wieder beschwor Obama in seiner Rede die Gefahr, die von Terroristen ausgehe. Man könne gar nicht aufmerksam genug sein. Und wer nichts zu verbergen habe, dem könne man auch nichts anhaben. Edward Snowden widerspricht:

**Cut 32: Edward Snowden**

You don't ... „derive“ suspicion.

**Übersetzer 2:**

Du musst gar nichts falsch gemacht haben, du wirst einfach verdächtigt, weil jemand die falsche Nummer gewählt hat. Und die NSA untersucht deine Vergangenheit, findet jeden Freund heraus, mit dem du einmal diskutiert hast und attackiert dich auf dieser Basis. Eine Art „abgeleitete“ Verdächtigung.

**Sprecher:**

Die NSA überwache nicht nur die Person, die sie im Visier habe, erklärte NSA-Vizechef Chris Inglis vor US-Abgeordneten. Sondern sie durchleuchte auch deren Freunde und Facebook-Freunde. Und die Freunde dieser Freunde. Wenn jemand bei Facebook 150 Freunde hat, werden diese 150 Freunde unter die Lupe genommen und die 150 Freunde dieser Freunde, das sind schon 22.500 Personen. Und die Freunde der Freunde der Freunde, das sind 3.375.000 Menschen, deren Mails, Telefonate und Chats registriert werden. 3.375.000 Menschen, die abgehört werden können, weil ein einziger als verdächtig gilt.

© Westdeutscher Rundfunk Köln 2014

Dieses Manuskript einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des WDR unzulässig. Insbesondere darf das Manuskript weder vervielfältigt, verbreitet oder öffentlich wiedergegeben (z.B. gesendet oder öffentlich zugänglich gemacht) werden.

\* \* \* \* \*