

Okay, Deal!

Ich soll meinen Kalender online in den USA hosten lassen, damit er sich einfacher zwischen Smartphone und Laptop synchronisiert?

Na gut ...

Ich soll mein Wohnzimmer abhören lassen, damit ich mit meinem Fernseher sprechen kann?

Moment mal!

Ja, George Orwell hat vieles vorhergesehen ... Aber nicht, dass wir uns die panoptischen Teleschirme auch noch freiwillig kaufen würden!

... und erst recht nicht, dass sie die Daten auch noch abhören würden.

Wie so viele andere Dienste ist auch die Spracherkennung in die Cloud gewandert. Der Algorithmus verbessert sich täglich, so dass die Geräte uns immer besser verstehen. Neue Funktionen können ohne Updates eingebaut werden, und auf dem Gerät selbst werden Speicherplatz und kostbare Akkulaufzeit gespart. Gleichzeitig lernen die Großrechner in der Cloud immer mehr von und über uns, damit wir eine möglichst persönliche Behandlung erfahren.

Wenn die Spracherkennung aber in der Cloud liegt, dann geben wir die hinter einem Service stehenden Abläufe aus der Hand.

Wenn wir zum Beispiel eine Internet-Suche mit den Worten „OK Google“ einleiten, oder per Sprachbefehl den Sender an unserem Fernseher wechseln, oder über den Amazon Echo-Lautsprecher eine Bestellung tätigen, dann sprechen wir nicht mit unserem Gerät, sondern mit einer Serverfarm irgendwo da draußen in den Weiten des Internets.

Und wenn unser Smartphone dann die SMS an Mutti schreibt, einen Termin in unseren Kalender einträgt oder unsere Frage be-

antwortet, dann ist es genau diese Serverfarm, die unser Gerät fernsteuert.

Eine Serverfarm in den Händen eines Konzerns, der die Mikrofon-Mitschnitte der Welt sammelt, analysiert und speichert.

Machen Sie sich da regelmäßig Gedanken drüber? Haben Sie sich überhaupt schon einmal Gedanken darüber gemacht?

Ganz wichtig ist für diese Konzerne: Damit sich die Investitionen in den Elektronik-Wachstumsmarkt auch lohnen, müssen unsere lieben Kunden und Kundinnen möglichst früh mit der Technik vertraut gemacht werden. Denn was schon im Kinderzimmer normal war, ist später umso selbstverständlicher.

Mit der Barbie fängt man „Bob der Baumeister“ und Playmobil an die Kunden mitspielen. Dabei ist der Wind weht – in Europa wird befürchteten Datenschutzbedenken kommen.

erschienen in der *FifF-Kommunikation*,
herausgegeben von *FifF e.V.* - ISSN 0938-3476
www.fiff.de

Mit WLAN, Mikrofon und Lautsprecher ermöglicht die neue „Hello Barbie“ schon unseren Kindern, sich mit einer Serverfarm irgendwo da draußen in den Weiten des Internets zu unterhalten. Sie bringt eine datenschutzrechtlich äußerst fragwürdige Technik ohne erkennbaren sinnvollen Anwendungszweck direkt in unsere Kinderzimmer.

Damit Gespräche überhaupt möglich werden, merkt „Hello Barbie“ sich, was unsere Kinder ihr erzählen. Später kann sie im Gespräch darauf zurückgreifen, und dadurch eine echte Freundin imitieren. Die lieben Eltern sorgen sich, was ihre Kinder der Puppe, pardon, Serverfarm so alles über sich erzählen? Kein Problem! Selbstverständlich lässt Mattel Sie an den gesammelten Daten teilhaben: In einer täglichen oder wöchentlichen E-Mail erhalten Sie das Protokoll der Sorgen, Träume und Geheimnisse, die Ihr Kind seiner besten Freundin, der Serverfarm von Mattel und Toytalk, anvertraut.

Und deshalb: Herzlichen Glückwunsch zum BigBrotherAward in der Kategorie *Technik*, „Hello Barbie“, Mattel und Toytalk.



Rolf Gössner

Kategorie *Behörden und Verwaltung* – Laudatio

Der BigBrotherAward 2015 in der Kategorie *Behörden und Verwaltung* geht an den Bundesnachrichtendienst (BND), vertreten durch seinen Präsidenten Gerhard Schindler (FDP).

Der deutsche Auslandsgeheimdienst erhält den Negativpreis für eine ganze Palette von Skandalen sowie Datenschutz- und Bürgerrechtsverstößen, die wir im Rahmen dieser Preisverleihung allerdings nur ausschnittsweise behandeln können. Unter anderem wird dem BND der Preis zuerkannt,

1. weil er aufs Engste in den menschenrechtswidrigen NSA-Überwachungsverbund verflochten ist und damit in den globalen Massenüberwachungsskandal;
2. weil er mit der sog. strategischen Überwachung der grenzüberschreitenden Telekommunikation und insbesondere mit seiner gesamten Auslandsaufklärung via Funk, Satellit oder Kabel weitgehend im rechtsfreien Raum operiert – nach Auffassung renommierter Verfassungsrechtler sogar schlicht verfassungswidrig;
3. weil der BND täglich über 220 Millionen Telekommunikationsdatensätze sammelt, speichert, auswertet und davon





Millionen an ausländische Partnerdienste übermittelt. Darunter sind auch grundrechtlich geschützte Daten von Bundesbürgern, deren Weitergabe gesetzlich untersagt ist; außerdem, so Ex-NSA-Mitarbeiter Thomas Drake, soll der BND sensible Informationen für den menschenrechtswidrigen Drohnenkrieg der USA geliefert haben, und damit für das gezielte Töten von Terrorverdächtigen.

4. Nicht zuletzt erhält der BND den BigBrotherAward für seine Informationsblockade und dreisten Vertuschungen geheimdienstlicher Praktiken gegenüber dem NSA-Untersuchungsausschuss des Bundestags, der sich mit aufklärungsunwilligen BND-Zeugen und überwiegend geschwärtzten, lückenhaften oder anderweitig manipulierten Akten des BND herumschlagen muss – frei nach der Zeugenaussage des Nachrichtendienst-Beauftragten im Bundeskanzleramt, Klaus-Dieter Fritsche (CSU), das „Staatswohl“ sei nun mal weit wichtiger als parlamentarische Aufklärung und Kontrolle.



Dr. Rolf Gössner, Foto: Bernd Sieker, CC by 4.0

I. Ausufernde Praktiken: Illegaler Datentransfer BND – NSA – BND

Nur eine der preiswürdigen Verfahrenspraktiken möchte ich ein wenig ausführen, um die damit verbundene Problematik deutlich zu machen: Seit 2004 zapfte der BND – mit Hilfe der Telekom und an allen Kontrollgremien vorbei – einen wichtigen Internetknoten (DE-CIX) in Frankfurt an und belieferte aus dieser sprudelnden Quelle die NSA jahrelang mit gewaltigen Datenmengen (Operation „Eikon“).

Der Frankfurter Netzknoten ist der größte Glasfaser-Knotenpunkt und Datenumschlagort der Welt – ein gefundenes Fressen für den BND, um etwa Daten zur grenzüberschreitenden anlasslosen „strategischen Fernmeldekontrolle“ abzusaugen, auf der Suche nach Hinweisen auf Terrorismus, Waffenhandel und Ausländerschleusung. Auch die grundrechtlich besonders geschützte Alltagskommunikation von Bundesbürgern fiel dabei gewissermaßen als „Beifang“ ab, deren Metadaten der Auslandsgeheimdienst eigentlich weder speichern noch an Auslandsdienste übermitteln darf. Deshalb hätte er sie herausfiltern müssen. Doch der eigens konstruierte Filter (DAFIS) funktionierte nur unzulänglich, so dass auch viele geschützte Daten illegal an die NSA übermittelt wurden.

Unter Auslandsgeheimdiensten ist der Datentransfer ohnehin keine Einbahnstraße, sondern ein Geschäft auf Gegenseitigkeit, das mit Vorliebe im Datenringtausch abgewickelt wird. Und der funktioniert so: Weil ein Auslandsdienst die eigene Bevölkerung nicht überwachen darf (deshalb heißt er ja AUSLANDS-Geheimdienst), bespitzelt er eben die Bevölkerung anderer Länder und tauscht dann die gewonnenen Daten mit den jeweiligen Partnerbehörden. Diese gängige Praxis beschert dann auch dem BND illegal Erkenntnisse über die bundesdeutsche Bevölkerung. Insgesamt gesehen müssen wir also von schwerwiegenden Grundrechtseingriffen in das Telekommunikationsgeheimnis, die Privatsphäre und die Informationelle Selbstbestimmung von Millionen ahnungsloser Menschen ausgehen.

II. Geheimdienstliches Aufrüstungsprogramm

Doch trotz dieser ausufernden, illegalen und unkontrollierbaren Praxis wird der BND nicht etwa rechtsstaatlich gezügelt, sondern künftig noch weiter digital aufrüstet und für das Massenüberwachungsgeschäft tauglich gemacht – für insgesamt 300 Mio. Euro, von denen bereits fast 35 Mio. bewilligt sind. Auch für dieses geheime Aufrüstungsprogramm mit dem Tarnnamen „Strategische Initiative Technik“ (SIT) und für weitere Nachrüstungsprojekte wird der BND mit dem BigBrotherAward 2015 ausgezeichnet – vor allem dafür:

- dass er künftig soziale Netzwerke, Blogs und Web-Foren systematisch, flächendeckend und anlasslos ausforschen soll – und zwar sowohl die Metadaten als auch die Inhalte;
- und dass der BND mit Hilfe von Sicherheitslecks und „Nachschlüsseln“ in fremde Computersysteme einbrechen und Verschlüsselungen knacken soll, um speziell solche Bürger, Firmen und Netzwerke gezielt auszuforschen, die sich besonders gegen Cyberattacken schützen wollen – wobei wohl viele treuherzig dem guten Rat des Bundesinnenministers gefolgt sein dürften, sich angesichts des NSA-Überwachungsskandals doch bitteschön per Verschlüsselung selbst zu schützen. Ein Tipp, der sich angesichts solcher BND-Pläne rasch als ziemlich perfide herausstellen könnte.

Beispiel: BND-Ausforschung sozialer Netzwerke

Demnächst soll der BND einen höchst fragwürdigen Freibrief erhalten, nämlich die Lizenz oder Ermächtigung zur anlasslosen Ausforschung sozialer Netzwerke wie Facebook, Flickr, YouTube oder Twitter, aber auch von Blogs und Internet-Foren. Die aufgefundenen Netzwerkdaten und Inhalte sowie das gespeicherte Kommunikationsverhalten der Nutzer können damit jederzeit automatisiert durchrastert, zu Persönlichkeits- und Bewegungsprofilen verdichtet oder biometrisch ausgewertet werden; auch Rückschlüsse auf soziale und politische Kontakte werden möglich. Deshalb greift diese Internet-Durchleuchtung besonders stark in Grundrechte der Betroffenen ein.

Die Behauptung der Bundesregierung, dies betreffe doch nur das Ausland, ist entweder naiv oder ganz bewusst irreführend und unzutreffend: Zum einen gelten Grund- und Menschen-

rechte auch im Ausland; zum anderen sind Server von sozialen Netzwerken quer über die Welt verteilt, so dass der innerdeutsche Datenverkehr auch über andere Länder fließt und danach als ausländisch gilt; so geraten auch bundesdeutsche Nutzer leicht ins BND-Visier.

Die globale Ausforschung sozialer Kommunikationsräume, in denen Infos, Meinungen, Bilder und andere sensible Daten ausgetauscht werden, soll dazu dienen, Stimmungen, Auffälligkeiten, Wirtschaftstrends, politische Proteste und Beziehungsgeflechte in bestimmten Ländern und Krisenregionen präventiv herauszufiltern und zu analysieren. Soziale Netzwerke wecken geheimdienstliche Gelüste auch deshalb, weil sie sich weltweit zu Mobilisierungsforen für Protestbewegungen entwickelt haben – wie etwa während des „Arabischen Frühlings“. Deshalb sollen sie nun – ab 2015 – nach NSA-Vorbild auch unter die Echtzeit-Kontrolle des BND gestellt werden; ihre Auswertung ist für die Bundesregierung, den so genannten Verfassungsschutz oder die Bundeswehr von Interesse, um etwa Krisen, geopolitische und militärstrategische Probleme und politische Akteure frühzeitig zu erkennen.

Verfechter solcher modernen Massenüberwachungsmethoden behaupten, nur so könne man Terroranschläge verhindern oder Organisierte Kriminalität bekämpfen, was auch schon passiert sein soll – eine Behauptung, die schon aus Geheimhaltungsgründen nie wirklich überprüfbar war.

III. Wettrüsten im Infokrieg: Präventive Vormacht- und Herrschaftssicherung

Auf diese Weise will der BND offenbar sein Image als „Wurmfortsatz“ der NSA, wie ihn Ex-NSA-Mitarbeiter Thomas Drake despektierlich nannte, loswerden und sich vom Großen Bruder emanzipieren. Wir werden also Zeugen eines fatalen Wettrüstens im Informationskrieg der Geheimdienste – einem Informationskrieg, in dem es nicht zuletzt um geostrategisch-wirtschaftliche Interessen sowie um präventive Vormacht- und Herrschaftssicherung geht, bis hin zur Absicherung militärischer Operationen. Schließlich gilt es, Staat oder Staatengemeinschaften nicht allein vor Terror und Gewalt zu schützen, sondern auch gegen mögliche soziale Unruhen, militante Aufstände oder unkontrollierte Wanderungsbewegungen und drohende Rohstoffknappheit vorsorglich zu wappnen – Aufstandsbekämpfung und militärische Interventionen inbegriffen.

Solche hochgerüsteten, letztlich unkontrollierbaren Präventionsdienste wuchern im Schatten des demokratischen Rechtsstaats, bedrohen Menschen, politisch-soziale Bewegungen und deren Freiheitsrechte. Sie wittern in jedem Menschen, jedem kritischen Gedanken und abweichenden Verhalten eine potenzielle Bedrohung, die es zu überwachen gilt. Doch Menschen, die unter ständiger Überwachung stehen, sind niemals frei. Schon wer sich nur beobachtet fühlt, verändert sein Verhalten, wird unsicher, entwickelt Ängste, passt sich an – Wirkungen, die eine offene, freie demokratische Gesellschaft schädigen, wie das Bundesverfassungsgericht bereits vor über dreißig Jahren in seinem berühmten Volkszählungsurteil festgestellt hat.

IV. Kapitulation des Rechtsstaats vor staatlichem Unrecht

Trotz massiver Bedrohungen und Bürgerrechtsverstöße durch die Massenüberwachung von NSA, BND & Co. hat es die Bundesregierung sträflich unterlassen, Bürger und von Wirtschaftsspionage betroffene Betriebe vor deren Attacken zu schützen – obwohl es zu ihren verfassungsrechtlichen Aufgaben gehört, diesen Schutz zu gewährleisten. Angesichts der regierungsamtlichen Lethargie erstatteten Anfang 2014 die Internationale Liga für Menschenrechte, der ChaosComputerClub und Digitalcourage beim Generalbundesanwalt Strafanzeige gegen Bundesregierung und Geheimdienst-Verantwortliche: wegen massiver Verstrickung des BND in das globale Massenüberwachungssystem, wegen millionenfacher Verletzung des Menschenrechts auf Privatsphäre und wegen sträflich unterlassener Abwehrmaßnahmen. Tausende unterstützten diese Anzeige.

Bekanntlich hat der Generalbundesanwalt Mitte 2014 ein Strafereignisverfahren eingeleitet – aber nur wegen des unfreundlichen Spionage-Angriffs auf das Handy der Kanzlerin. Eine Entscheidung, die an der Gleichheit aller Menschen vor dem Gesetz zweifeln lässt: Denn auf ein Ermittlungsverfahren wegen der ungleich schwerer wiegenden massenhaften Ausspähung der ganzen Bevölkerung verzichtet er – kurioserweise mangels „zureichender Tatsachen“.

Das ist angesichts der Fülle an Belastungsbeweisen und -zeugen Realitätsverleugnung oder Willfährigkeit – jedenfalls hart an der Grenze zur Strafvereitelung im Amt. Diese Rechtsschutzverweigerung ist eine Kapitulation des Rechtsstaats vor staatlichem Unrecht.

Deshalb sehen wir uns in der Pflicht, mit diesem überfälligen BigBrotherAward den Blick der Öffentlichkeit erneut auf die Machenschaften des BND zu lenken und auf das Problem geheimer Institutionen in einer Demokratie. Das ist das Mindeste, was wir tun können, auch wenn es auf den ersten Blick effektiver scheint, die milliardenteure BND-Zentrale in Berlin einfach unter Wasser zu setzen, wie Anfang März dieses Jahres geschehen: Eine originelle Geheimoperation auf der bestgesicherten Baustelle der Nation. Wenn auch keine Dauerlösung, so lässt uns dieses „Watergate“ doch auf weitere undichte Stellen hoffen – auf der dringenden Suche nach einem Snowden im BND! Und vielleicht lässt uns die Flutung des BND erahnen, wie der Auslandsgeheimdienst dereinst in seinen eigenen Datenfluten zu ertrinken droht. In diesem Sinne: „Kopf hoch“, „Petri heil“ und herzlichen Glückwunsch zum BigBrotherAward 2015, Herr BND-Präsident Gerhard Schindler!



Foto: Matthias Hornung, CC by 4.0