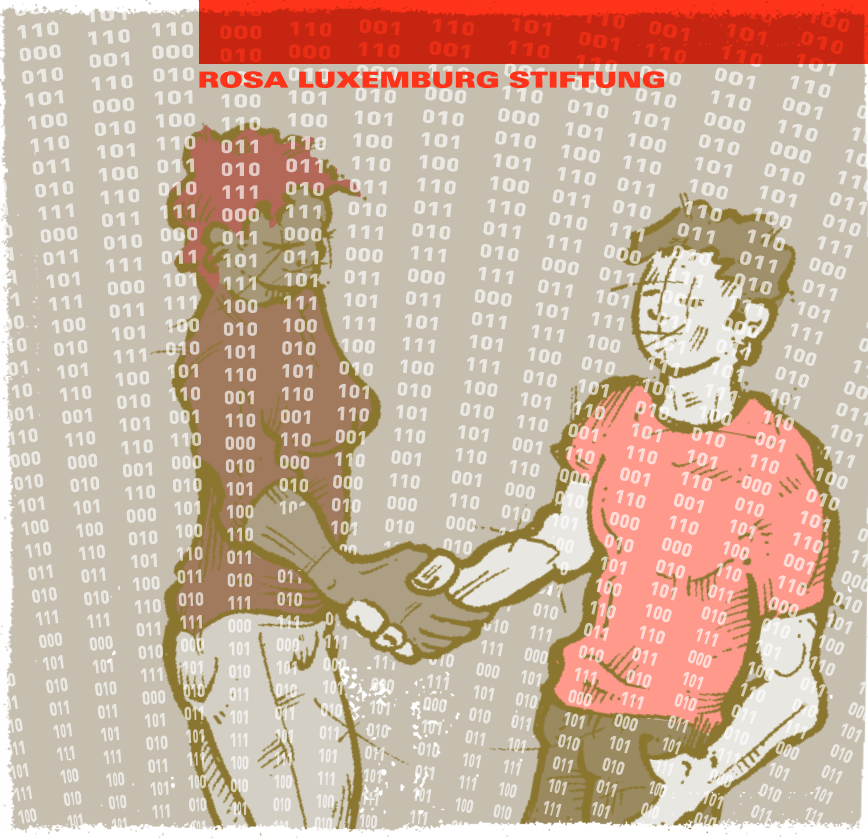
ROSA LUXEMBURG STIFTUNG



OFFENES GEHEIMNIS

Mythen und Fakten zu Überwachung und digitaler Selbstverteidigung

luxemburg argumente

Die ersten Enthüllungen durch den ehemaligen NSA-Systemadministrator Edward Snowden im Juni 2013 liegen nun eine Weile zurück. Seither ist deutlich geworden, wie tief auch die deutschen Behörden, angefangen mit dem Bundesnachrichtendienst (BND) bis hin zum Bundeskanzleramt, in die Affäre verstrickt sind. Die totale Massenüberwachung, Sabotage und gezielte Industriespionage sind amtlich.

Anstatt dem entgegenzusteuern, weitete die Bundesregierung die Möglichkeiten der Überwachung aus: Die Geheimdienste wurden aufgerüstet und mit mehr Befugnissen ausgestattet, etwa durch die Verfassungsschutzreform und das IT-Sicherheitsgesetz. Und um auch den Strafverfolgungsbehörden Überwachung zu erleichtern, wurde in einem Schnellverfahren die Vorratsdatenspeicherung neu aufgelegt und um einen Paragrafen erweitert, der das Arbeiten mit geleaktem Material unter Strafe stellt – ein Anti-Whistleblower-Paragraf.

Seit Sommer 2013 macht die Bevölkerung weltweit von verschlüsselter Kommunikation verstärkt Gebrauch, da Verschlüsselung einen effektiven Schutz vor Massenüberwachung darstellt. Die Geheimdienste antworteten prompt mit einer PR-Kampagne, die Terroranschläge nutzt, um ein staatliches Recht auf anlasslose Überwachung gegen das Recht der BürgerInnen auf informationelle Selbstbestimmung durch Verschlüsselung in Stellung zu bringen.

Die Industrie lässt sich von dem Geheimdienstskandal nicht weiter beeindrucken und treibt die Entwicklung und Vermarktung des sogenannten Internets der Dinge voran. Alles soll vernetzt sein und über das Internet kommunizieren können – nicht nur Computer, Telefone und Uhren, sondern auch Kühlschränke, Autos und Industrieanlagen. Obwohl die Sicherheitskonzepte, die diesen Entwicklungen zugrunde liegen, durch die bekannt gewordenen NSA-Aktivitäten erschüttert worden sind, entwickelt und verkauft die Industrie unbeirrt weiter. Wir, die EndverbraucherInnen, die BürgerInnen, stehen vor einem Internet-Trümmerhaufen: unsicher, fast vollkommen kommerzialisiert, von Spionage durchsetzt.

Was tun? In dieser Broschüre werden Ängste und Folgen, die im Zusammenhang mit diesem Spionageskandal stehen, diskutiert und Handlungsperspektiven aufgezeigt. Denn es gibt vieles, was wir tun können, um uns vor Überwachung zu schützen und das Internet als Freiraum wieder zurückzuerobern.

INHALT

MYTHEN UND FAKTEN ZU ÜBERWACHUNG UND DIGITALER SELBSTVERTEIDIGUNG

1

«ICH HAB NICHTS ZU VERBERGEN, DENN ICH TUE NICHTS VERBOTENES.»

Was ist dran?

Massenüberwachung erfasst alle – unabhängig von der Frage, ob jemand sich etwas hat zuschulden kommen lassen oder nicht. Dabei geht es nicht um das konkrete Individuum, sondern um die Kontrolle und Manipulation der gesamten Bevölkerung. Das Recht auf Privatsphäre ist aber eine Grundvoraussetzung für die Wahrnehmung anderer Rechte, etwa des Rechts auf Meinungs- und Informationsfreiheit, Versammlungsfreiheit oder des Rechts auf Freiheit von Diskriminierung. Anlasslose Massenüberwachung stellt deshalb einen
2 fundamentalen Angriff auf die Grundlangen demokratischer Gesellschaften dar.

Durch Edward Snowden sind die Spionagepraktiken des US-amerikanischen Geheimdienstes NSA und seiner Kooperationspartner teilweise an das Licht der Öffentlichkeit gelangt. Dabei ist bekannt geworden, dass das Ausmaß und die Reichweite der Massenüberwachung digitaler Kommunikation viel umfassender und größer sind, als selbst kritische DatenschützerInnen angenommen hatten: Nahezu überall auf der Welt werden Verbindungsdaten, Telefondaten, E-Mail-Verkehr und Banktransaktionen genauso wie Bewegungsprofile, die sich aus dem Herumtragen eines Mobiltelefons ergeben, anlasslos erfasst, gespeichert und analysiert.

Eine Massenüberwachung unterscheidet sich grundsätzlich von der spezifischen Überwachung einer bestimmten Person. Sie ist nicht nur technisch, sondern auch konzeptionell anders angelegt und stellt eine der wichtigsten Grundlagen der demokratischen Gesellschaften auf den Kopf, die *Unschuldsvermutung:* Nicht mehr ein Verdacht rechtfertigt eine Überwachung, sondern die Überwachung rechtfertigt einen Verdacht. Nicht mehr die oder der von einem Gericht Verurteilte

ist schuldig, sondern potenziell schuldig ist jede Bürgerin beziehungsweise jeder Bürger.

Bei der Massenüberwachung gibt es *keinen Anlass* zur Überwachung. Stattdessen wird eine gesamte Bevölkerung oder Bevölkerungsgruppe überwacht. Die erfassten Daten werden nach bestimmten Verhaltens- oder Situationsmustern oder nach spezifischen Merkmalen («Raster») durchsucht. Treten bestimmte Kombinationen aus Merkmal, Verhalten und Situation auf, ergibt sich daraus ein Verdacht. Als verdächtige Person markiert zu sein kann zu weiteren Überwachungen und zur Aufnahme auf eine der unterschiedlichen Terrorismus-Verdächtigenlisten führen, die Geheimdienste und Strafverfolgungsbehörden in den USA derzeit führen, und sehr unangenehm werden: Verstärkte Kontrollen an den Grenzen, Flughäfen, Bahnhöfen oder bei Demonstrationen bis hin zum Reiseverbot können die Folge sein.

Diese Massenüberwachung findet statt, obwohl sie gesetzlich bislang noch in allen westlichen Demokratien *verboten* ist. Um die jeweiligen nationalen oder auch einzelne technische Beschränkungen zu umgehen, hat sich unter den westlichen Geheimdiensten eine sehr intensive Zusammenarbeit entwickelt. Will der eine Geheimdienst die Bevölkerung seines Landes ausspionieren, ist aber gesetzlich angehalten, dies nicht zu tun, kann er sich diese Spionagedaten von anderen Geheimdiensten zur Verfügung stellen lassen. Alle Sicherheitsdienste profitieren so gleichermaßen von den in den westlichen Demokratien üblichen rechtlichen Regelungen, bei denen die eigenen BürgerInnen vor Überwachung geschützt werden, AusländerInnen jedoch keinen Schutz vor Spionage genießen und weitgehend abgehört werden können. Durch eine enge Kooperation kann jeder Geheimdienst die Überwachung seiner eigenen BürgerInnen organisieren, ohne selbst in der aktiven Spionage gegen die eigene Bevölkerung nachweislich tätig zu sein.

Anlasslose Massenüberwachung ist als Praxis neu – ein Traum der Geheimdienste war sie jedoch schon immer. Der Grund, warum sie nun Realität ist, ist leider sehr banal: Die Sicherheitsbehörden überwachen, weil sie überwachen können. Es ist leichter und billiger, eine Massenüberwachung durchzuführen,

als zuerst bestimmte Zielpersonen zu definieren und diese dann einzeln und spezifisch zu überwachen (siehe auch Argument 4). Dabei verzichten die Geheimdienste aber nicht auf ihre bisherigen Methoden: Eine sehr detaillierte und weit ins Privateste der Person hineinreichende Überwachung von Verdächtigen findet nach wie vor statt. Nur ergibt sich der konkrete Verdacht, der diese intensive Überwachung auslöst, nicht mehr notwendigerweise aus einer Handlung dieser Person, sondern meistens aus der Massenüberwachung und der daraus entstandenen verdächtigen Muster. Dass so eine weitaus größere Anzahl von Menschen als verdächtig eingestuft wird, erscheint logisch. Und deshalb verwundert es nicht, dass auf den Überwachungslisten mindestens 1,2 Millionen Menschen stehen, die im Detail von der NSA verfolgt werden.

Das heißt in der Praxis: *Jede beliebige Person kann ins Visier der Ermittlungsbehörden geraten,* wenn sie zur falschen Zeit am falschen Ort war, den falschen Beruf hat, im falschen Netzwerk eingeloggt war, die falsche Software benutzt hat oder einfach nur Pech hatte. Im Ergebnis ist die Auswahl der Verdächtigen rassistisch und diskriminierend: Arabischstämmige Männer geraten beispielsweise wesentlich schneller ins Raster der NSA und auf eine Verdächtigenliste als weiße US-amerikanische Männer.

Wer einmal durch die Massenüberwachung erfasst und als verdächtig markiert worden ist, wird nicht darüber informiert, kann sich nicht dazu äußern oder verteidigen und hat auch keinen Einfluss darauf, je wieder aus der Datenbank der Verdächtigen entfernt zu werden. Solche Verdächtigungen können auch Anlass sein, festgenommen und verhört zu werden.

Ein absurdes Beispiel für eine aus Massenüberwachung abgeleitete falsche Verdächtigung liefert der Fall von zwei aus Großbritannien anreisenden TouristInnen, die in Los Angeles Urlaub machen wollten. Emily Bunting und Leigh Van Bryan hatten sich Wochen vor ihrer Abreise auf Twitter über ihre Reise ausgetauscht. In einem Kommentar hatte Van Bryan sinngemäß geschrieben, dass er «in Amerika die Sau rauslassen» wolle. In britischer Alltagssprache heißt das «destroy America». Die Überwachungssoftware und auch die eingesetzten Polizeibe-

amtInnen nahmen diesen Spruch wörtlich und behandelten die beiden bei ihrer Ankunft in Los Angeles, als wären sie TerroristInnen, die die USA zerstören wollen: Abtransport in einem Käfig und stundenlange Verhöre.

Besonders drastisch war der Fall des kanadischen Staatsbürgers Maher Arar, der völlig grundlos bei einem Zwischenstopp auf einem US-amerikanischen Flughafen nicht nur festgenommen, sondern auch entführt und gefoltert wurde. Wie viele solcher falschen Verdächtigungen es gibt, ist nicht bekannt. Der Fall von Maher Arar wurde publik, weil er in einem langjährigen Prozess seine Unschuld beweisen konnte. Einen solchen Prozess zu führen ist für viele Betroffene allein schon aus finanziellen Gründen nicht möglich. Daher ist von einer hohen Dunkelziffer auszugehen.

Dass eine permanente Überwachung Effekte auf die Psyche der überwachten Menschen hat und vor allem ihr Vertrauen in die Demokratie und die Organe des Staates erheblich beeinträchtigt, liegt nahe. Die Selbsteinschätzung, man habe nichts zu verbergen oder man tue nichts Verbotenes, ist bereits eine erste Reaktion auf das unerträgliche Wissen, permanent überwacht zu werden. Mit der von ÜberwachungskritikerInnen vorhergesagten *Selbstkontrolle* der Menschen geht die faktische Abschaffung der Meinungsfreiheit einher: Man überprüft sein eigenes Handeln und die mögliche Interpretation dieses Handelns bereits selbst und nimmt damit die Kontrolle der Behörden vorweg. Daraus entsteht das Gefühl, selbst nicht Ziel der Sicherheitsbehörden werden zu können, weil man sich ja nichts zuschulden hat kommen lassen.

Die Effekte von permanenter Überwachung gehen aber noch weiter. Das zeigt ein beeindruckendes dokumentarisches Rechercheprojekt am Beispiel der US-amerikanischen Kleinstadt Bridgeview, einem Vorort von Chicago: Die Bevölkerung von Bridgeview, die hauptsächlich aus arabischstämmigen US-amerikanischen Familien besteht, hat seit den frühen 1990er Jahren das Gefühl, ständig vom FBI überwacht zu werden, und dieser Eindruck – so können die FilmemacherInnen Assia Boundaoui und Alex Bushe nachweisen – ist nicht unbegründet. Das FBI hat diese Stadt im Rahmen einer der größten Counter-Terror-Pro-

SELBSTBESTIMMTE ANEIGNUNG (VON TECHNOLOGIE)
IST GLEICHSAM EIN AKT DES WIDERSTANDS

gramme intensiv überwacht. In ihrem Dokumentarfilm «The feeling of being watched» (Veröffentlichung angekündigt für 2016) zeichnen sie nach, wie sich das Leben, das Denken und Handeln von BürgerInnen verändert, die seit 30 Jahren unter den Bedingungen ständiger Überwachung leben: Das Vertrauen der Betroffenen in demokratische Institutionen ist durch die Überwachungserfahrung stark beschädigt. Aber auch Verhaltensänderungen im Privaten werden sichtbar: Telefonate werden nur noch im Rahmen des absolut Notwendigen geführt, mehrdeutige Begriffe oder Redewendungen werden gar nicht mehr benutzt und es ist vollkommen normal, alle Fenster, auch tagsüber, mit einem blickdichten Sichtschutz zu verhängen.

2

«GOOGLE, FACEBOOK UND CO SIND NOCH VIEL SCHLIMMER!»

Was ist dran?

Die IT-Dienstleister monopolisieren riesige Datenmengen. Sie nutzen sie, um Profite zu machen, und treiben damit die Kommerzialisierung des Internets voran. Das stimmt. Bislang ist aber kein Fall bekannt geworden, in dem IT-Dienstleister gezielt einzelne InternetnutzerInnen ausgespäht oder gehackt oder anderweitig angegriffen hätten. Das unterscheidet sie von den Geheimdiensten.

Google, Facebook, Microsoft, Twitter, Yahoo und Apple sind die weltweit am meisten genutzten Anbieter von Onlinediensten und allesamt US-basierte Internetunternehmen. Das bringt sie in eine besondere Lage: Alle US-amerikanischen Unternehmen sind *gesetzlich dazu verpflichtet,* nicht nur mit der NSA auf Anordnung zusammenzuarbeiten, sondern über diese Verpflichtung zur Zusammenarbeit auch nie in irgendeiner Form Auskunft zu geben. Diese Anordnung heißt «National Security Letter». Weil Dienstleister wie Google, Facebook, Microsoft, Apple, Twitter und Yahoo, aber auch Dropbox oder Internetprovider wie Verizon für ihre Dienste und darüber hinaus Nutzerdaten erfassen und verwalten – wenn sie beispielsweise E-Mail-Services oder Speicherplatz zur Verfügung stellen –, stehen diese Daten der NSA also zur Verfügung.

Durch Edward Snowden wissen wir, dass von der gesetzlichen Möglichkeit, Unternehmen zur Zusammenarbeit zu zwingen, auch intensiv Gebrauch gemacht wird. Wie oft welche Unternehmen in welchem Umfang der NSA bisher Zugang gewährt haben, ist allerdings nicht bekannt, wohl aber, dass einige Unternehmen mit der NSA freiwillig zusammenarbeiten, andere wiederum auch gegen ihren Willen von der NSA über die gesetzlichen Regelungen hinaus ausgespäht oder gehackt worden sind.

Die Politik der großen IT-Unternehmen ist seit den Snowden-Veröffentlichungen ein wenig positionierter geworden. Mit dazu beigetragen hat sicher die große Unzufriedenheit vor allem bei GeschäftskundInnen, die vielfach auch einen Wechsel des Anbieters zur Folge hatte. So haben Apple und Google an einigen Punkten *Verschlüsselungen* mit in ihr Standardangebot aufgenommen oder dies angekündigt, die direkt von KommunikationspartnerIn zu KommunikationspartnerIn realisiert werden. Diese sogenannte Ende-zu-Ende-Verschlüsselung setzt darauf, dass Anbieter, die keine Daten einsehen können, auch nicht gezwungen werden können, solche Daten weiterzugeben. Allerdings findet dieses Prinzip nur an sehr wenigen, kleinen Punkten Anwendung: Apple hat eine solche Verschlüsselung in seinen Messenger-Dienst iMessage eingebaut und Google arbeitet derzeit an einer E-Mail-Verschlüsselungsoption.

Auch deutsche Unternehmen haben auf die Situation reagiert: So bieten nicht nur besonders datenschutzsensible E-Mail-Dienstleister wie Mailbox.org und Posteo.de eine Verschlüsselungsoption für ihre Webmail-Dienste an, sondern auch weit verbreitete Anbieter wie United Internet AG, besser bekannt mit ihren Produkten Web.de und Gmx.de.

Zusätzlich scheinen sich auch die Ansprüche der NutzerInnen geändert zu haben, insbesondere im Hinblick auf die Möglichkeit, die eigenen Daten löschen zu können. In den neueren Google-Produkten wie Google-Timeline etwa, mit der Google abspeichert, wann man sich wo aufgehalten hat, gibt es die Möglichkeit, diese Daten selbst wieder zu löschen. Allerdings: Wer seine Daten *nicht* selbst löscht, der riskiert, dass sie von Geheimdiensten oder Behörden bei den Anbietern eingesehen werden.

So ist im November 2015 bekannt geworden, dass gerade die Daten von Google-Timeline von Strafverfolgungsbehörden genutzt werden, um alte Fälle wieder neu aufzurollen, denn *Google-Timeline speichert alle Bewegungsdaten seit 2009 standardmäßig.*

Das zeigt ganz gut, wie die Politik der großen IT-Dienstleister momentan aussieht: Einerseits wollen sie das Vertrauen der KundInnen wiedergewinnen und sich von den Geheimdiensten nicht auf der Nase herumtanzen lassen, andererseits wollen sie das profitable Geschäft mit den Nutzerdaten auch nicht aufgeben.

Das Problem daran: Wer viele Daten hat, dem können auch viele Daten entwendet werden. *Datensparsamkeit,* wie sie deutsche DatenschützerInnen seit Jahren fordern, war bislang weder für US-amerikanische oder deutsche Internetunternehmen noch für InternetnutzerInnen ein Qualitätsmerkmal.

In der Tat würden viele Internetdienste heute anders aussehen, wenn mit personenbezogenen Daten entsprechend sorgsam umgegangen werden würde, wie es in der Welt vor der Verbreitung des Internets qua Gesetz erforderlich war. Soziale Netzwerke, angepasste Suchergebnisse und personalisierte Kaufempfehlungen, wie sie heute üblich sind, würde es so vermutlich gar nicht geben, oder sie hätten technisch ganz anders realisiert werden müssen. Durch das Auffliegen der NSA-Aktivitäten ist klar geworden, wie hoch der Preis ist, den wir zahlen, wenn bei der Weiterentwicklung des Internets Vermarktungsinteressen im Vordergrund stehen. Wenn Google zum Beispiel personalisierte Werbung anbietet, soll sie die NutzerInnen nicht «stören», sondern als passende Empfehlung daherkommen. Das kann sie aber nur, wenn sie ihre AdressatInnen gut kennt. Deshalb werden bei Anbietern wie Google alle E-Mails im Volltext untersucht und in Profilen zusammengefasst. Nur so weiß Google, ob etwa ein Nutzer, der nach «Golf» sucht, eher auf Werbung für Sport oder Autos anspringt. Diese technische Realisierung stellte in der Werbebranche eine regelrechte Revolution dar – und führte zu gläsernen KundInnen und BürgerInnen.

Es geht aber auch anders. Es gibt E-Mail-Provider, die sehr sorgsam mit den Daten ihrer KundInnen umgehen, die keine Werbung in jede versendete E-Mail einfügen, die die Inhalte der E-Mails nicht durchforsten und die keinen Profit mit den Kundendaten machen. Dass sich auf dieser Basis sogar funktionierende Geschäftsmodelle gründen lassen, die es in den Punkten Service, Sicherheit und Professionalität mit den großen werbebasierten Anbietern aufnehmen können, stellen Internetdienstleister wie Posteo.de, Mailbox.org und andere unter Beweis. Dort zahlen KundInnen einen kleinen monatlichen Betrag für die Nutzung einer E-Mail-Adresse, anstatt (zusätzlich) mit ihren Daten zu bezahlen.

Allerdings gilt auch hier: Jedes Mehr an Sicherheit «kostet» ein wenig mehr an Geld, Aufwand oder Komfort. Auch wenn es nur um einen Klick geht, der beim Einrichten eines E-Mail-Kontos zu beachten ist. Aber das ist das *Grundprinzip von Sicherheit:* Sicherheit erschwert, verhindert und blockiert, denn sie soll Dritte abwehren und ausschließen. Das ist in der Regel auch mit mehr Aufwand für die verbunden, die etwas sichern wollen. Wenn mein Fahrrad nicht gestohlen werden soll, muss ich es anschließen. Jedes Schloss, das ich an meinem Fahrrad befestige, schützt es besser, macht mir aber auch mehr Mühe im alltäglichen Gebrauch.

Wer glaubt, auf Dienste wie Facebook, Google oder Dropbox nicht verzichten zu können, sollte sich in diesen Netzwerken umsichtig verhalten und auf den Schutz seiner Daten achten. Zum Beispiel sollte allen Facebook-NutzerInnen bewusst sein, dass Strafverfolgungsbehörden vollen Zugriff auf die dort hinterlassenen Daten haben und dass es Analysesoftware gibt, die sehr detailliert Auskunft geben kann, welche Kommunikations- und Beziehungsprofile sich aus einem Facebook-Konto ableiten lassen. Solche Software ist nicht sonderlich aufwendig und teuer und steht jeder durchschnittlichen Detektei zur Verfügung. Auch das, was ich in angeblich geschlossenen Facebook-Gruppen poste, kann Gegenstand von Gerichtsverfahren werden und gegen mich verwendet werden. Das haben verschiedene – vor allem arbeitsgerichtliche – Verfahren in der Vergangenheit gezeigt. Darum: *Organisierungsprozesse haben auf Facebook nichts zu suchen,* Fotos von FreundInnen, Bekannten oder Ge-

nossInnen sollten nur mit deren ausdrücklicher Erlaubnis in sozialen Netzwerken veröffentlicht werden.

3

«DIE GEHEIMDIENSTE SAMMELN NUR METADATEN.»

Was ist dran?

Metadaten sind Verbindungs- und Bewegungsdaten: Wer hat wann mit wem gesprochen, wer ist wann wo langgelaufen. Das entspricht in der analogen Welt der herkömmlichen Beschattung. Wer sagt, es sind «nur» Metadaten, der sagt, es ist «nur» eine Observation.

Metainformationsdaten, kurz Metadaten oder auch Verkehrsdaten genannt, sind Informationen *über* Daten. In der Internet- und Telefonkommunikation gehören dazu unter anderem Verbindungs-, Kunden- und Geodaten. Während die eigentlichen Inhalte eines Gesprächs oder einer E-Mail als Inhaltsdaten bezeichnet werden, beziehen sich Metadaten zum Beispiel auf die Teilnehmenden an einem Gespräch, Ort, Zeit und Dauer des Gesprächs, die genutzte Hard- und Software, die IP-Adressen oder Telefonnummern und dazugehörige Telefon- oder Internetverträge sowie eventuelle Bewegungen während, vor und nach dem Gespräch.

Metadaten geben ziemlich viel Auskunft über uns und sind sehr leicht zu erfassen. Da die Daten auch sehr einfach zu verarbeiten sind, weil es sich zumeist um gut dokumentierbare, zähl- und sortierbare Ereignisse handelt, sind sie auch vergleichsweise leicht auszuwerten. Aus Geodaten können ohne komplizierte Analyseverfahren, quasi mit einem Klick, *Bewegungsprofile* erstellt werden. Ohne großen technischen Aufwand kann aufgrund von Metadaten zum Beispiel festgestellt werden, welche Personen mit Mobiltelefon sich zu einem bestimmten Zeitpunkt in einem bestimmten Gebiet aufgehalten haben, wohin sie gegangen sind und wer mit wem in diesem Zeitraum kommuniziert hat.

Solche Metadaten entstehen überall dort, wo mithilfe von technischen Geräten kommuniziert wird beziehungsweise Daten transferiert werden. Sie können auch an all diesen Stellen erfasst werden. Beispielsweise können Geheimdienste den In-

ternetverkehr an bestimmten Leitungsknotenpunkten überwachen und alle darin vorkommenden Metadaten analysieren. Gäbe es alternativ dazu bereits gespeicherte Metadaten, könnten Geheimdienste und Strafverfolgungsbehörden einfach auf diese zurückgreifen, um sich ein Bild davon zu machen, wer wann wo gewesen ist und was getan hat.

Als die Bundesregierung im Jahr 2007 zum ersten Mal ein Gesetz zur *Vorratsdatenspeicherung* beschlossen hatte, wurde darin beispielsweise festgelegt, dass solche Metadaten sechs Monate lang von den jeweiligen Internetdienstleistern aufbewahrt werden müssen, für den Fall, dass sie noch einmal von Strafverfolgungsbehörden gebraucht werden. Schnell wurde klar, dass es sich dabei um eine Grundlage zur Totalüberwachung handelt. Denn wo Daten erhoben werden, können sie auch analysiert oder überwacht werden. Durch die starke Gegenbewegung und eine damit einhergehende Verfassungsbeschwerde wurde das Gesetz im Jahr 2010 für verfassungswidrig erklärt und vorerst zurückgenommen.

Am 16. Oktober 2015 hat die Große Koalition eine neue Variante, das Gesetz zur «Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten», im Schnellverfahren beschlossen, seit Dezember 2015 ist es in Kraft. Es legt für alle Anbieter von Internet- und Telekommunikationsdienstleistungen fest, dass sie

– Standortdaten der TeilnehmerInnen aller Mobiltelefonate bei Beginn des Telefonats und bei Beginn der mobilen Internetnutzung für vier Wochen speichern müssen;
– Rufnummern, Zeit und Dauer aller Telefonate, aber auch Rufnummern, Sende- und Empfangszeit aller SMS-Nachrichten für zehn Wochen speichern müssen und
– die IP-Adressen aller InternetnutzerInnen sowie Zeit und Dauer der Internetnutzung ebenfalls für zehn Wochen speichern müssen.

Die Daten sind im Inland zu speichern und nach Ablauf der vorgeschriebenen Frist zu löschen. Es bedarf keiner richterlichen Anordnung zur Herausgabe der Daten an Stellen der Strafverfolgung oder Gefahrenabwehr. Das bedeutet für die Praxis: Die Überwachung des E-Mail- und Telefonverkehrs wird zu einem Standardinstrument in der Strafverfolgung, von dem ohne wei-

tere gesetzliche oder richterliche Genehmigungen Gebrauch gemacht werden kann.

Wie weitgehend dieser Eingriff in die Privatsphäre jeder und jedes Einzelnen ist, hat der Grünen-Abgeordnete Malte Spitz im Jahr 2009 im Rahmen des Bürgerprotests gegen das Vorratsdatenspeichergesetz eindrucksvoll demonstriert: Er stellte die Verbindungsdaten seines Handys (kein Smartphone) für eine Visualisierung zur Verfügung. Sie zeigt, wie aussagekräftig ein Bewegungsprofil ist. Fast entsteht beim Betrachten der Eindruck, es sei gar nicht mehr nötig, jetzt noch alle Gesprächsinhalte zu kennen, um ein Personenprofil von dem Abgeordneten erstellen zu können (→ Beispiel Handy-Bewegungsprofil: **www.zeit.de/datenschutz/malte-spitz-vorratsdaten**).

Noch viel weiterreichender, als es das jetzige Gesetz vorsieht, wird die *massenhafte Speicherung von Metadaten* in der Bundesrepublik bereits *durch den BND* betrieben. Im Oktober 2014 konnte durch den NSA-Untersuchungsausschuss bewiesen werden, dass der BND in Datenbanken wie dem Verkehrsanalysesystem, abgekürzt VerAS, massenhaft Metadaten auch von deutschen BürgerInnen speichert – und zwar weitreichender als dies durch die NSA geschieht. Denn es werden nicht nur die Kommunikationsdaten von einer Person erfasst, sondern zusätzlich noch die ihrer KommunikationspartnerInnen und wiederum die von deren KommunikationspartnerInnen und von deren KommunikationspartnerInnen etc. Während der US-amerikanische Geheimdienst die Kommunikationsbeziehungen nur bis in die dritte Ebene erfasst, sammelt der BND gleich zwei Ebenen mehr. Das bedeutet zum Beispiel, dass neben der Kommunikation eines Verdächtigen auch die des Lebensgefährten der Mutter der Freundin des Anwalts des Verdächtigen durchsucht werden kann.

Besonders drastisch brachte der ehemalige NSA- und CIA-Chef Michael Hayden die Bedeutung von Metadaten auf den Punkt. Im Rahmen einer Podiumsdiskussion erklärte er im April 2015: «Wir töten Menschen auf der Basis von Metadaten!»[1] Die-

1 Eine Dokumentation der Podiumsdiskussion ist im Internet unter: https://youtube.com/watch?v=kV2HDM86XgI zu finden.

se Aussage war keine Zuspitzung, sondern eine Beschreibung dafür, wie die Zielpersonen bei sogenannten gezielten Tötungen durch Drohneneinsätze erfasst werden. Aufgrund von Verbindungsdaten werden diese Personen geortet und schließlich auch umgebracht.

Das Entscheidende an Metadaten ist, dass sie *nicht verschlüsselt werden können.* Ich kann beispielsweise den Inhalt meiner E-Mail mit einer Verschlüsselungssoftware verschlüsseln, aber an wen ich wann von welchem Computer und welcher IP-Adresse aus mit welchem E-Mail-Programm und zu welcher Uhrzeit die E-Mail geschickt habe, lässt sich nicht verschlüsseln. Ich kann mein Telefongespräch mit Verschlüsselungssoftware vor fremden Ohren schützen, aber mit wem ich wann wie lang von wo aus und mit welcher Hard- und Software telefoniert habe, kann durch Verschlüsselung nicht geschützt werden. Deshalb benötigen Metadaten einen besonderen rechtlichen Schutz. Mit dem neuen Gesetz zur Vorratsdatenspeicherung hat die Bundesregierung jedoch genau das Gegenteil getan.

Wenn wir Metadaten nicht rechtlich schützen können, bleibt nur der Ausweg, technische Kommunikationswege zu erfinden, die ohne oder mit wenigen Metadaten auskommen. Während heutzutage beispielsweise eine E-Mail sehr viel und genau dokumentiert, wer sie wann von welcher IP-Adresse mit welchem Betriebssystem und E-Mail-Programm an wen geschickt hat, wäre es technisch denkbar, Kommunikationsformen zu entwickeln, die weniger Metadaten «produzieren», die erfasst werden können, also sparsamer mit Metadaten umgehen.

Wo das nicht möglich ist, können Verschleierungstechniken helfen, Anonymität und Privatsphäre wiederherzustellen. Nach diesem Prinzip funktioniert beispielsweise der Tor-Browser, der die Herkunft des Web-Surfenden durch eine Vielzahl von Weiterleitungen derart verschleiert, dass darüber die Anonymität des Nutzers oder der Nutzerin faktisch wiederhergestellt werden kann.

KOLLEKTIVE SELBSTVERTEIDIGUNG ✵ ZUSAMMEN KÄMPFEN, STATT ALLEINE GOOGELN!

4

«DASS GEHEIMDIENSTE ÜBERWACHEN, IST DOCH NICHTS NEUES!»

Was ist dran?

Im Kern ist keine von den jetzt bekannten Praxen der Geheimdienste neu. Sie überwachen, spionieren, manipulieren, sabotieren und greifen einzelne Ziele an. Neu ist aber das Ausmaß: Wenn früher Hunderte betroffen waren, sind es heute Milliarden. Und neu ist auch der geringe Aufwand: Wenn früher Hunderte GeheimdienstlerInnen wenige Menschen beschatteten, überwachen heute wenige GeheimdienstlerInnen Millionen Menschen.

Geheimdienste spionieren im Geheimen. In westlichen Demokratien sind sie dabei an Gesetze gebunden und Kontrollverfahren unterworfen. Diese doppelte Bindung unterscheidet – so lehrt es die politische Bildung – einen demokratischen von einem undemokratischen Staat. In Letzterem setzen sich Geheimdienstinstitutionen selbstständig Regeln und werden nicht kontrolliert. In der Vergangenheit wurden immer wieder Fälle bekannt, in denen Geheimdienste demokratischer Staaten ihre Befugnisse weit überschritten und *illegale* Abhörpraktiken angewendet haben.

In Deutschland gibt es im Wesentlichen drei Geheimdienste:
- den Bundesnachrichtendienst (BND), der vor allem für die internationale Spionage und deren Abwehr zuständig ist,
- den Verfassungsschutz, der für die Überwachung der bundesdeutschen BürgerInnen zuständig ist, um Demokratiegefährdungen zu identifizieren, und sowohl in den einzelnen Bundesländern, aber auch als Bundesbehörde existiert, und
- den zur Bundeswehr gehörigen Militärischen Abschirmdienst (MAD).

Der erste große *Abhörskandal* in Deutschland wurde 1963 durch den damaligen Verfassungsschutzmitarbeiter Werner Pätsch aufgedeckt. Ähnlich wie Edward Snowden konnte er den Gewissenskonflikt nicht mehr ertragen, mit illegalen Methoden Menschen im Rahmen seiner Geheimdiensttätigkeit auszuspionieren. Schon damals wurde durch Pätsch bekannt, dass der

deutsche Verfassungsschutz eng mit dem britischen und amerikanischen Geheimdienst in Deutschland zusammenarbeitet und sich von diesen Informationen über deutsche BürgerInnen beschaffen lässt, deren Überwachung für den Verfassungsschutz illegal war. Als Konsequenz aus dieser Affäre wurden die Rechte des Verfassungsschutzes kurzerhand ausgeweitet, sodass die illegale Beschaffung der Abhördaten über befreundete Geheimdienste nicht mehr nötig war, weil der Inlandsgeheimdienst jetzt *legal* seine BürgerInnen ausspionieren durfte.

Ein ganz ähnlich gelagerter Skandal beschäftigt den NSA-Untersuchungsausschuss heute: Inwieweit hat der BND mit der NSA über das zulässige Maß hinaus zusammengearbeitet? Wurden dabei Grundrechte deutscher StaatsbürgerInnen verletzt? Damals wie heute ist zu befürchten, dass die Öffentlichkeit nicht über das vermutlich illegale Treiben deutscher Geheimdienste aufgeklärt wird, solange nicht couragierte GeheimdienstmitarbeiterInnen, die ihrem Gewissen mehr als ihrer Karriere verpflichtet sind, den Mut finden, über diese Praktiken aufzuklären.

Neben dem deutlichen Überschreiten der Grenzen rechtlich zulässiger Überwachung werden aber noch weitere Probleme durch die aktuelle NSA-Überwachungsaffäre offensichtlich. Denn das, was in Argument 1 schon aus einer individuellen Perspektive beschrieben wurde, hat auch eine systemische Dimension:

(1) Noch nie war Massenüberwachung technisch so unkompliziert und so preiswert wie heutzutage. Solange die meisten Verbindungen im Internet unverschlüsselt sind, ist das Mitlesen und Speichern ein Leichtes. Die einzigen Kosten entstehen beim Speichern, wenn diese ganzen Massendaten gesammelt und für spätere Analysezwecke vorgehalten werden sollen. Eines der größten bekannten Datenzentren, das die NSA für die Speicherung der durch Massenüberwachung erfassten E-Mails nutzt, ist das Utah Data Center. Allein seine Errichtung kostete 1,7 Milliarden US-Dollar. Das gesamte Gelände ist etwa 93.000 Quadratmeter groß, das entspricht einer Fläche von etwas mehr als 13 Fußballfeldern. Wie groß die Datenmengen sind, die dort gespeichert werden, ist nicht genau bekannt, fest

steht allerdings, dass diese Anlage Kapazitäten zur Speicherung des E-Mail-Verkehrs der Weltbevölkerung vorhält.

(2) Noch nie war es so schwer, sich vor gezielten Überwachungsmaßnahmen zu schützen, es ist technisch fast unmöglich. Obwohl das Recht auf Privatsphäre im Grundgesetz verbrieft ist, bleibt vollkommen unklar, wie dieses Recht wahrgenommen werden kann.

Zur Zielperson kann man schnell erklärt werden. Fällt durch einen der Filter oder Raster der Massenüberwachung eine Person auf – weil sie beispielsweise mit jemandem E-Mails ausgetauscht hat, der oder die sich irgendwo auffällig bewegt oder geäußert hat, oder weil die Person selbst eine Journalistin oder ein Wissenschaftler ist –, wird diese Person unter Umständen für eine persönliche Verfolgung bestimmt. Da auch dafür die Kosten verhältnismäßig gering sind, werden ziemlich viele Personen heutzutage persönlich überwacht. Eine der durch Edward Snowden geleakten Daten beinhaltet eine Zielpersonenliste der NSA, auf der allein 1,2 Millionen Personen erfasst sind. Um solche Zielpersonen zu überwachen, infiziert der Geheimdienst ihre Computer gezielt mit Schadsoftware, damit eine Überwachungssoftware über all ihre Tätigkeiten Auskunft geben kann. Ihre Telefone werden angezapft und ausgewertet, Bewegungsprofile erstellt, Banktransaktionen überwacht, Fotos gemacht. Technisch sind diese Überwachungsmöglichkeiten dermaßen ausgefeilt und treffen auf so viele nicht mehr vollständig abzusichernde Systeme, dass selbst ComputerexpertInnen nicht mehr in der Lage sind, ihren Computer vor einem solchen Zugriff zu schützen.

Als mit den Notstandsgesetzen in den 1970er Jahren in der Bundesrepublik auch die Möglichkeiten der Überwachung ausgeweitet wurden, gab es unter politisch Aktiven eine Diskussion und einen Umgang mit dieser Situation. Spaziergänge im Wald standen beispielsweise hoch im Kurs, um vertrauliche Gespräche zu führen und sich dabei effektiv vor Wanzen, Richtmikrofonen und mithörenden Menschen zu schützen. Aber was tun wir heute, wo selbst der Wald von Überwachungskameras durchsetzt ist? Zum Beispiel setzen JägerInnen Überwachungskameras zur Kontrolle des Wildbestands ein, oftmals werden

aber auch potenzielle Müllabladestellen oder andere Orte in der freien Natur aus unterschiedlichen Gründen videoüberwacht. Zu dieser Praxis gibt es weder eine Regulierung noch einen Überblick, wer sie wo anwendet. Von DatenschützerInnen ist dieser Missstand wiederholt kritisiert worden – bislang allerdings ohne positives Ergebnis.

(3) Noch nie war unsere Privatsphäre so leicht angreifbar und noch nie war es so schwer, persönliche Daten zu schützen, wie heute. Denn dank der Geheimdienste ist unsere Privatsphäre jetzt nicht nur durch Geheimdienste angreifbar. Durch systematische Sabotage und Manipulation haben sie das Internet unsicherer gemacht. Sie haben Sicherheitsstandards manipuliert, Sicherheitslücken sind durch Geheimdienste programmiert worden, Hintertüren auf Intervention der Geheimdienste in viele Geräte eingebaut worden. Nur eine Frage haben NSA & Co dabei nicht bedacht: Wer wird diese Lücke neben den Geheimdiensten noch nutzen?

5

«PRIVATSPHÄRE INTERESSIERT DOCH DIE LEUTE VON HEUTE NICHT MEHR. SIND DOCH ALLE BEI FACEBOOK!»

Was ist dran?

Nichts. Privatsphäre ist ein Recht, das allen zusteht. Auch wenn Facebook-NutzerInnen einen Teil ihrer privaten Kommunikation in die Öffentlichkeit verlagern, kann ihnen weder das Recht auf Privatsphäre noch ein Interesse daran abgesprochen werden. Und viele von ihnen machen von diesem Recht auch Gebrauch, wenn sie die Privatsphäre-Einstellungen bei Facebook nutzen.

Das Recht auf Privatsphäre zu erkämpfen war ein langer Prozess, und für den Erhalt dieses Rechts müssen wir uns auch heute noch engagieren. Wie bei anderen Bürgerrechten auch ist der Staat zwar diejenige Instanz, vor der dieses Recht einklagbar ist, gleichzeitig behält er sich aber vor, bestimmte Personengruppen von diesem Recht auszuschließen, zum Beispiel GefängnisinsassInnen, PatientInnen oder HeimbewohnerInnen.

Zu den Ausnahmen gehören auch Orte oder Situationen, die für die staatliche Sicherheit als bedrohlich angesehen werden: Demonstrationen, Staatsbesuche, Fußballspiele. Diese Orte, Ausnahmesituationen und ausgeschlossenen Personengruppen wurden durch viele Regierungen in den letzten Jahren stückweise ausgeweitet. So ist es heute beispielsweise in den USA und Großbritannien möglich, dass Beschuldigte per Gerichtsbeschluss und – wenn es sein muss – auch Beugehaft gezwungen werden, ihre Passwörter oder andere Verschlüsselungsdaten herauszugeben. Wenig ist über solche Gerichtsbeschlüsse bekannt, denn sie werden meistens nur öffentlich, wenn Beschuldigte den Mut aufbringen, dagegen gerichtlich vorzugehen.

Es gibt Berichte von Reisenden, die bei der Einreise in Länder wie Israel, die USA oder China ohne Beschuldigung genötigt wurden, ihre Facebook- und E-Mail-Konten offenzulegen. Auch während jeder anderen Flugreise ist das Recht auf die eigenen Daten zu großen Teilen außer Kraft gesetzt – Reisedatenweitergabe an Behörden, komplette Durchsuchungen des Gepäcks mit beliebigen Nachfragen und Leibesvisitationen gehören für Reisende heute zum Alltag.

Die Praktiken und Beschränkungen, die den von *Hartz IV Betroffenen* auferlegt werden, sind ein anschauliches Beispiel dafür, wie eine gesamte Personengruppe in ihren Rechten beschnitten wird. Viele der Hartz-IV-EmpfängerInnen nehmen die Auskunftspflichten, die sie gegenüber dem Amt haben, als demütigend und in die Privatsphäre unangenehm eindringend wahr. Ob es Nachweispflichten ihrer Wohnverhältnisse, Kontrollen durch das Amt oder Auskunftspflichten aller Art sind, die Privatsphäre der Betroffenen wird deutlich verletzt.

Zu den Einschränkungen des Rechts auf Privatsphäre gehört auch das bundesdeutsche *Meldegesetz.* Im Juni 2012 beschlossen, wurde den Einwohnermeldeämtern die Möglichkeit eingeräumt, persönliche Daten der BürgerInnen an Werbefirmen und Inkassounternehmen zu verkaufen. Zusätzlich wurden alle 5.200 bundesdeutschen Meldeämter vernetzt, außerdem müssen VermieterInnen seit 2015 beim Meldeamt wieder Ein- und Auszüge von MieterInnen bestätigen. Aufgrund der vielen,

deutlichen Proteste von Initiativen und Bündnissen wie «Meine Daten sind keine Ware!» wurde das Gesetz um eine Zustimmungspflicht modifiziert: BürgerInnen können bei ihrem jeweiligen Einwohnermeldeamt dem Weiterverkauf ihrer Daten nun widersprechen.

Die Liste der Bedingungen, unter denen das Recht auf Privatsphäre und das Recht an den eigenen Daten ausgesetzt oder Personengruppen davon ausgeschlossen werden, ließe sich problemlos fortführen. Aber ebenso ließe sich an jedem einzelnen dieser Beispiele auch zeigen, wie umkämpft diese Einschnitte waren und sind.

Neben den rechtlichen Beschränkungen haben sich durch die Digitalisierung zudem neue technische Möglichkeiten ergeben, die Privatsphäre zu verletzen und zu beschneiden. Das Internet hat Einzug in Bereiche gehalten, die zuvor privat waren, Öffentliches und Privates haben sich zunehmend verflochten. Computer, Smartphones und das sogenannte Internet der Dinge sorgen dafür, dass eine Kommunikation mit der Arbeitswelt und mit der Öffentlichkeit auch von den privatesten Orten aus möglich ist. Dadurch wird immer etwas von dieser Öffentlichkeit auch an diese privaten Orte getragen. Gleichzeitig finden durch soziale Medien viele «private» Aktivitäten vermehrt in der Öffentlichkeit statt. Die Privatsphäre hat dadurch ihren Charakter verändert. Wir befinden uns mitten in einer Neubestimmung des Privaten und des Öffentlichen.

Denn gleichzeitig ermöglichen Digitalisierung und Internet neue Formen der *öffentlichen Teilhabe* und Mitbestimmung. Das beweisen Initiativen wie «Frag den Staat», die auf der Grundlage des Informationsfreiheitsgesetzes BürgerInnen die Möglichkeit geben, nicht nur privat einzelne Auskünfte über Regierungshandeln zu erhalten, indem sie Einsicht in bestimmte Behördendokumente verlangen, sondern diese auch der Öffentlichkeit zur Verfügung zu stellen, und so für mehr Transparenz und Einsicht in demokratische Prozesse sorgen.

Die Herausforderung besteht darin, diese Chance zur Offenheit mit einem aktualisierten Recht auf Privatsphäre zu verbinden, statt das eine gegen das andere in Stellung zu bringen. Auch

wenn Menschen einen Teil ihrer ehemals privaten Kommunikation in die Öffentlichkeit verlagern, haben sie dennoch ein Recht auf Privatsphäre und ein Recht, nicht überwacht zu werden. Ihnen dieses Recht abzusprechen ist gefährlich und folgt der gleichen Logik, die NichtwählerInnen das Wahlrecht absprechen will.

6

«COMPUTERSICHERHEIT IST VIEL ZU KOMPLIZIERT UND NUR WAS FÜR EXPERTINNEN – ICH HAB GAR KEINE ZEIT, MICH UM VERSCHLÜSSELUNG ZU KÜMMERN.»

Was ist dran?

Sicherheit ist mehr als Verschlüsselung, und viele Sicherheitsmaßnahmen sind technisch nicht anspruchsvoll. Aber alle Maßnahmen, die die Sicherheit verbessern, bedeuten zusätzliche Arbeit und benötigen zusätzliche Zeit. Und so wie ich eigentlich keine Zeit habe, Zahnseide zu benutzen, habe ich eigentlich auch keine Zeit, meine Cookies im Webbrowser zu löschen.

Wer sein Auto parkt, schließt es ab. Das geht ganz automatisch. Mittlerweile ist es nur ein kurzes Drücken auf die Fernbedienung, ein kurzes Piepen ertönt und das Auto ist zu. Mit wenigen Klicks für Sicherheit auch im digitalen Alltag zu sorgen ist heute an vielen Stellen bereits möglich. Das Konzept dahinter heißt «Security by Design», was so viel bedeutet wie «Sicherheit als Teil des Konzepts» oder auch «eingebaute Sicherheit». Geräte werden so konzipiert, dass eine sichere Nutzung und ein Schutz vor Angriffen vorgesehen sind. Das ist vergleichbar mit Sicherheitsanforderungen beim Hausbau: Ein altes Gebäude umzubauen, damit es aktuellen Sicherheitsanforderungen entspricht, kann unter Umständen teuer und aufwendig sein. Werden Sicherheitsfragen bereits bei der Planung mitberücksichtigt, sind diese beim Hausbau preiswerter und einfacher umzusetzen.

Dementsprechend ist eine digitale Architektur, die von vornherein Sicherheitsfragen und den Schutz der Privatsphäre mitbedenkt, viel effektiver in der Handhabung, auch wenn sie viel-

leicht schwerer zu konzipieren ist. Wenn zum Beispiel eine Kommunikationssoftware so erstellt wird, dass sie keine Protokolle der stattgefundenen Kommunikation erfasst, dann können auch keine Protokolle abhanden kommen oder müssen gegen ungewollte Einsichtnahme gesichert werden. Wenn Verbindungen qua Software nur verschlüsselt stattfinden, können sie nicht versehentlich unverschlüsselt bleiben. Einige der heute entwickelten Programme versuchen, «Security by Design» umzusetzen. Ob sich das als Standardanforderung durchsetzen wird, entscheiden am Ende auch die NutzerInnen: Wenn sie sich für Sicherheitsfragen nicht interessieren, Sicherheitsoptionen in ihrer Software nicht nutzen und bei ihrer Kaufentscheidung nicht berücksichtigen, wird dieses Konzept nicht zum Standard werden.

Dreh- und Angelpunkt bleiben auch in Bezug auf das Internet die NutzerInnen: Wer ein Internet will, das so weit wie möglich frei von Überwachung und Kontrolle, Weitergabe und Handel mit privaten Daten ist, muss sich dafür interessieren, muss sich das *Wissen darum aneignen.* Angesichts der rasanten Entwicklung der digitalen Welt dürfen wir uns nicht abhängen und auf unmündige KonsumentInnen reduzieren lassen. Wenn ich nicht weiß, welche sichere Software es gibt, werde ich sie auch nicht nutzen. Wenn ich nicht weiß, dass mein Computer eine Komplettverschlüsselung in zwei Klicks aktivieren kann, werde ich meine Daten nie verschlüsseln. Sich dieses Wissen anzueignen ist nicht leicht und individuell nicht zu bewältigen. Vielmehr kann eine solche Nutzersouveränität nur gemeinsam erarbeitet und kollektiv umgesetzt werden (siehe Abschnitt «Was tun?»).

Diese Fragen werden täglich dringender. Nicht nur weil fortgesetzt Informationen darüber an die Öffentlichkeit gelangen, mit welchen Techniken die NSA und andere Geheimdienste die Totalüberwachung organisieren, sondern auch weil das Internet stetig weiterentwickelt wird. Mit der nächsten Generation von vernetzten Geräten – dem sogenannten *Internet der Dinge* – werden Fragen des Schutzes der Privatsphäre noch einmal relevanter. Dann geht es nicht nur um den eigenen Computer und die eigenen Daten, sondern auch um das Auto, die Zeitung oder die Wohnungsinfrastruktur, die über das Internet «gesteuert» werden können. Hier entstehen neue Herausforderungen und

Sabotagemöglichkeiten, die besonderen technischen Schutz notwendig machen. Denn wenn ich via Internet die Heizung in meiner Wohnung an- und abstellen kann, können das rein technisch gesehen auch andere.

Die Hauptaufgabe, vor der wir als InternetnutzerInnen stehen, um unsere Sicherheit im Umgang mit Internettechnologie zu vergrößern, ist jedoch nicht technisch, sondern ganz banal und Kern jeder *Aneignungsstrategie:* mein Handeln zu reflektieren, Technik in ihrer Funktionsweise zu verstehen und ein eigenes Verhältnis dazu zu gewinnen.

7

«WIR MÜSSEN UNS VOR CYBERTERRORISTEN SCHÜTZEN.»

24

Was ist dran?

Die verschiedenen Geheimdienste dieser Welt gehören selbst zu den CyberterroristInnen, die sie angeblich bekämpfen wollen. Mit den ihnen zur Verfügung stehenden Ressourcen haben sie die Sicherheitsstruktur im Internet systematisch geschwächt und angreifbar gemacht, Sicherheitslücken gebaut und Sicherheitsstandards manipuliert. Ohne die Intervention der Geheimdienste wäre unsere Online-Welt wesentlich sicherer.

Durch Edward Snowden sind Aktivitäten der NSA und ihres britischen Pendants GCHQ bekannt geworden, die weit über das Spionieren und Überwachen hinausgehen und als Sabotageakte bezeichnet werden müssen. Ganz gezielt wurden beispielsweise einige Bestandteile von Verschlüsselungstechnologien, wie etwa einer der Zufallszahlengeneratoren, der manchen Verschlüsselungen zugrunde liegt, mit einer Hintertür versehen. Auf Betreiben der NSA wurde ebendieser Zufallsgenerator zu einem der Standardbausteine, auf dem zahlreiche Verschlüsselungsprogramme basieren.

Neben derartigen Sabotageakten sind darüber hinaus gezielte Angriffe der Geheimdienste ans Tageslicht gekommen. So wurde bereits 2010 öffentlich, dass mit der Schadsoftware «Stux-

Z.B. CLOUD-COMPUTING · STETS ONLINE · OHNE SCHUTZ STEHST DU IM REGEN.

net» gezielt das iranische Atomprogramm angegriffen wurde. Die Art des Angriffs legte die Vermutung nahe, dass der US-Geheimdienst zumindest einer der Auftraggeber war. Durch Snowden wissen wir heute, dass diese Vermutung richtig war – die NSA war nicht nur Auftraggeber, sondern sogar Ingenieur des Angriffs. Die Snowden-Leaks überraschten nicht nur mit der Enthüllung dieser Aktion, sondern vielmehr mit dem Ausmaß derartiger Angriffe: Nicht nur «Stuxnet», sondern Tausende solcher Angriffe gehen auf das Konto der Geheimdienste.

Erschreckend ist auch, wie breit gefächert die Angriffsziele der NSA sind: Neben iranischen Atomprogrammen und den Netzwerken angeblicher TerroristInnen werden nicht nur die Computer von AktivistInnen, einzelnen JournalistInnen oder gleich ganzer Zeitungsredaktionen, sondern auch die einfacher UserInnen von der NSA gezielt mit Trojanern infiziert und ausgespäht. Aber selbst die gezielten Angriffe mit Schadprogrammen, die beispielsweise eine bestimmte Urananreicherungsanlage als Sabotageziel haben, werden mit hohen Kollateralschäden durchgeführt, denn die in Umlauf gebrachten Computerviren erreichen weit mehr technische Anlagen und PCs als vorgesehen.

In den letzten Jahren sind neben den durch die Snowden-Veröffentlichungen bekannt gewordenen Cyberangriffen durch die NSA und ihre Partner auch immer wieder Angriffe an die Öffentlichkeit gelangt, für die vermutlich andere Geheimdienste verantwortlich sind. Angriffe, die beispielsweise chinesische und nordkoreanische, russische, aber auch andere, westliche Geheimdienste durchgeführt oder in Auftrag gegeben haben. Wenn wir uns die Anzahl und das Ausmaß all dieser Cyberangriffe vergegenwärtigen, fällt auf, dass ein Großteil des angeblichen Cyberterrorismus durch die verschiedenen Geheimdienste dieser Welt betrieben wird. Wir befinden uns inmitten eines *Cyberwettrüstens,* bei dem die Sicherheit des Internets systematisch ausgehebelt wird.

Moralisch schwerwiegender ist das gebetsmühlenartig vorgebrachte Argument, Geheimdienste könnten Terrorangriffe verhindern. Der Terrorangriff in Paris am 14. November 2015 lehrt das Gegenteil: Die Attentäter waren den Behörden be-

kannt und wurden von den Geheimdiensten überwacht. Einer der Haupttäter, Abdelhamid Abaaoud, hatte die Anschläge sogar vorab im wichtigsten IS-Magazin *Dabiq* angekündigt und sich dort mit einem Maschinengewehr in der Hand abbilden lassen. Trotzdem gelang es nicht, die Attentate zu verhindern. Vielmehr lancierten Geheimdienste zunächst die Information, die Angreifer hätten verschlüsselt kommuniziert und darum nicht im Vorfeld von den Geheimdiensten identifiziert werden können. Keine 24 Stunden später entpuppte sich diese Meldung als falsch: Die Täter hatten die Anschläge mit herkömmlichen, unverschlüsselten SMS koordiniert.

Nicht wegen der fehlenden Überwachung, sondern *trotz der existierenden Überwachung* konnte der Anschlag nicht verhindert werden. Durch die eingesetzte Überwachungstechnologie konnte lediglich rückwirkend der Tathergang schneller rekonstruiert und aufgeklärt werden. Rechtfertigt das die Überwachung der gesamten Bevölkerung?

8

«DIE DEUTSCHE REGIERUNG SOLLTE DEM TREIBEN DER AMERIKANER EINEN RIEGEL VORSCHIEBEN.»

Was ist dran?

Die bisherigen Erkenntnisse des NSA-Untersuchungsausschusses deuten leider in eine ganz andere Richtung. Er konnte aufdecken, dass nicht nur der BND, sondern auch der Verfassungsschutz in die NSA-Überwachungsaffäre verstrickt ist. Die deutsche Regierung war offensichtlich über die NSA-Aktivitäten informiert, will dafür aber jetzt keine Verantwortung übernehmen. So wird der schwarze Peter vom BND zum Kanzleramt und von dort zum Innenministerium und zurück geschoben. Niemand will's gewesen sein, aber klar ist, dass alle davon gewusst haben. Das zeigt ganz deutlich, dass die deutsche Regierung Teil des Problems und nicht Teil der Lösung ist. Das zeigt uns aber auch: Nur wir, die Bevölkerung, die EndverbraucherInnen oder der «Rest des Internets» können dem Treiben der Geheimdienste einen Riegel vorschieben.

Der NSA-Untersuchungsausschuss hat es schwer. Weder die Geheimdienste noch die Regierung haben ein Interesse daran, Licht in das Dunkel um die Überwachungsaffäre zu bringen. Dementsprechend wird eine Aufklärung systematisch behindert und verzögert. Aber auch ohne genau nachweisen zu können, welche Personen oder welche Institutionen in welchem Ausmaß und mit welchen Techniken mit der NSA verstrickt sind, wird deutlich, dass – auch in Deutschland – Massenüberwachung und Manipulation durch Geheimdienste zum Alltagsgeschäft der Regierungen gehören.

Eines der ersten Ergebnisse des NSA-Untersuchungsausschusses war, dass die Überwachungspraktiken durch juristische ExpertInnen, wie ehemalige BundesverfassungsrichterInnen, analysiert wurden. Sie kamen zu dem Schluss, dass die flächendeckende anlasslose Speicherung von Telekommunikationsverkehrsdaten in Deutschland gegen die Verfassung verstößt und damit auch der BND ohne rechtliche Grundlage handelt.

Die deutsche Regierung reagierte prompt: Anstatt den Geheimdienst zurückzupfeifen, wurde eine Reform der Gesetze, die die Praxis des BND auf legale Füße stellt, in Angriff genommen. Jeder durchschnittliche Bürgerverstand hätte zumindest die Anpassung der Aktivitäten der Geheimdienste an die Befugnisse und nicht umgekehrt erwartet. Das wäre so, als würde die Schulpflicht abgeschafft werden, weil zu viele Kinder die Schule immer wieder schwänzen. In der Regierungswelt passiert genau das: Um das ungesetzliche Handeln der Geheimdienste einzuhegen und in einen gesetzlichen Rahmen zurückzuholen, müssen die Gesetze angepasst werden, bis wieder passt, was passend gemacht werden muss. Denn offenbar sieht selbst die Regierung keine realistische Chance, den anderen Weg zu gehen und die Geheimdienste in die gesetzlichen Schranken zu weisen. Darum wird die Forderung an die deutsche Regierung, den amerikanischen Geheimdiensten einen Riegel vorzuschieben, folgenlos bleiben.

Neben dem Problem, dass die deutsche Regierung massiv in diese Überwachungsaffäre verstrickt ist, ist die von vielen geforderte nationale digitale Souveränität aber auch technisch kein Weg, um das Internet sicherer zu machen. Denn das *Internet ist nicht national.* Die verschiedenen Knotenpunkte und die dazu-

gehörigen Kabel und Leitungen sind nicht so aufgebaut, dass eine nationale Abwicklung des Datenverkehrs derzeit möglich wäre. Ein nationales Internet ließe sich nur nach dem Modell Chinas realisieren: mithilfe einer großen Firewall und viel staatlicher Kontrolle. Das wäre de facto das Ende des freien Internets.

Sicherheit im Internet gibt es nur global. Eine nationale Strategie kann nur dann sinnvoll sein, wenn sie sich zum Ziel setzt, die deutschen Geheimdienste zu zähmen und das Internet wieder und weiter zu demokratisieren.

9

«WIR BRAUCHEN POLITISCHE LÖSUNGEN, KEINE TECHNISCHEN.»

Was ist dran?

Politische Lösungen sind immer auf einen bestimmten geografischen Rechtsraum beschränkt. Gleichzeitig müssen politische Lösungen auch technisch durchgesetzt werden, damit sie nicht durch technische Angriffe immer wieder unterwandert werden. Technische Lösungen können potenziell global sein. Wenn sie aber politisch nicht gewollt sind, können sie in den einzelnen Rechtsräumen verboten und kriminalisiert werden. Deshalb müssen politische und technische Lösungen Hand in Hand gehen. Wir müssen die IT-Unternehmen und unsere Regierungen in die Pflicht nehmen und gleichzeitig die Umgestaltung des Internets selbst vorantreiben.

In den Monaten nach den Snowden-Veröffentlichungen diskutierte die technische Community – SoftwareentwicklerInnen, SicherheitsexpertInnen, NetzaktivistInnen –, was die bekannt gewordene Praxis der Massenüberwachung für das Internet bedeutet. Man war sich schnell einig und gab das Motto aus: «Trust the Math!» – Vertraut der Mathematik! –, denn Verschlüsselungen sind nach wie vor sicher, sie müssen nur technisch ordentlich und flächendeckend implementiert werden, um Massenüberwachung wirksam zu behindern.

Auch auf parlamentarischer Ebene wurde die Massenüberwachung kritisiert: «Ausspionieren unter Freunden? Das geht

CRYPTOPARTY-SMALLTALK: »WARSTE FRÜHER AUCH EIN SCHLÜSSELKIND?«

gar nicht!» war der berühmt gewordene Kommentar von Bundeskanzlerin Angela Merkel. Da die Snowden-Veröffentlichungen in den Wahlkampf zur Bundestagswahl fielen, gab sich die Bundesregierung, die gern wiedergewählt werden wollte, entschlossen. Ein No-Spy-Abkommen sollte mit der US-amerikanischen Regierung abgeschlossen werden, um das Ausspähen politisch zu unterbinden. Dass sich diese Offensive hinterher als reine Wahltaktik entpuppte, ändert nichts am Wahlsieg der CDU. Darüber hinaus bleibt vollkommen unklar, warum es ein neues Abkommen braucht, wenn die Praxis der Überwachung auch schon auf der Basis bereits existierender Gesetze illegal ist.

Eines der zentralen Probleme kam innerhalb der parlamentarischen Diskussion zudem bislang noch gar nicht zur Sprache: Politische und technische Lösungen können nicht getrennt voneinander diskutiert werden. Was nützt die beste Verschlüsselung, wenn die Regierungen sich mithilfe von Sonder- und Ausnahmegesetzen Möglichkeiten verschaffen, diese zu umgehen, indem sie beispielsweise verpflichtende Hintertüren beschließen und andernfalls die ganze Technik verbieten? Was nützen No-Spy-Abkommen, wenn für Geheimdienste Ausnahmen gelten?

Festzuhalten bleibt: Jede technische Lösung muss politisch durchgesetzt werden und jede politische Lösung muss technisch realisierbar sein. Ein aktualisiertes Recht auf informationelle Selbstbestimmung könnte heute das Recht auf Ende-zu-Ende-Verschlüsselung sein: Dadurch, dass nur «Sender» und «Empfänger» die technische Möglichkeit besitzen, die Kommunikation zu entschlüsseln, stellt sie die einzige technische Möglichkeit dar, die Inhalte privater Kommunikation technisch zu schützen.

10

«MAN KANN SOWIESO NICHTS DAGEGEN TUN.»

Was ist dran?

Omnipotenz ist genau das Bild, das Geheimdienste gern von sich vermitteln wollen. Entmündigte, ohnmächtige Menschen, die sich nicht mehr wehren, sind ihnen dabei am liebsten. Zum Glück gibt es aber genug Menschen, die das anders sehen, und gemeinsam können wir sehr viel erreichen: Wir konnten das Gesetz zur Vorratsdatenspeicherung beim ersten Mal wieder abschaffen – warum nicht auch ein zweites Mal? Wir konnten eine Aufklärung der Geheimdienstaffäre einfordern, sodass ein NSA-Untersuchungsausschuss eingerichtet wurde – warum nicht auch den öffentlichen Druck aufbauen, damit der Ausschuss auch Ergebnisse produzieren kann? Wir können uns über Computersicherheit informieren, wir können unsere E-Mails von einem lokalen vertrauenswürdigen Provider verwalten lassen. Wir können viel mehr tun, als uns bewusst ist.

«Wenn Geheimdienste deine Daten wollen, wird auch eine Verschlüsselung sie nicht aufhalten.» Solche oder ähnliche Bewertungen hört man oft, wenn es um Möglichkeiten geht, sich gegen die aktuellen Angriffe auf unsere Privatsphäre digital selbst zu verteidigen. Überwachung, Sabotage und Manipulation durch Geheimdienste sind vielschichtig. Dementsprechend vielschichtig sind auch die Möglichkeiten, sich dagegen zur Wehr zu setzen:

Die US-amerikanische Bürgerrechtsorganisation Electronic Frontier Foundation (EFF) hat im Januar 2015 eine *Strategie gegen die Massenüberwachung* durch die NSA vorgelegt. Im Zentrum des Plans steht – wenig überraschend – die Verschlüsselung, die an drei verschiedenen Stellen vorangetrieben werden muss:
(1) bei den IT-Firmen, damit sie Verschlüsselungstechnologien unterstützen, implementieren und zum Standard erheben und auch ihre eigene Infrastruktur gegen geheimdienstliches Spähen absichern;
(2) bei den NutzerInnen, damit sie stärker von Verschlüsselungstechnologien Gebrauch machen und

(3) bei EntwicklerInnen, damit sie benutzerfreundliche Verschlüsselungstechnologien entwickeln.

Diese drei Ansatzpunkte zeigen, dass alle NutzerInnen auf verschiedenen Ebenen Möglichkeiten haben, gegen Massenüberwachung aktiv zu werden. Die heute stattfindende Massenüberwachung der Onlinekommunikation durch Geheimdienste geschieht in erster Linie, weil sie möglich ist: Der technische Aufwand ist gering, die Überwachung ist billig und leicht zu organisieren. Das ist aber nur deshalb so, weil die Verschlüsselung der Onlinekommunikation nicht verbreitet ist. Dazu können wir alle ohne Probleme einen Beitrag leisten: Die Messenger, die ihr nutzt, bieten Verschlüsselung an? Nutzt sie. Die Websites, die ihr besucht, bieten https an? Nutzt es. Eure E-Mail-Provider und Mail-Programme unterstützen PGP mithilfe von Erweiterungen oder Plug-ins, sodass ihr ohne viel Aufwand verschlüsseln könnt? Macht mit. Sobald eine kritische Anzahl von NutzerInnen mit Verschlüsselungstechnologien einen alltäglichen Umgang gefunden hat, werden viele andere folgen und mitmachen.

Laut der Snowden-Berichte stehen mindestens 1,2 Millionen Menschen auf der Liste der NSA, die für die *komplette Ausforschung* ausgewählt wurden. Es wurden Beispiele von Personen bekannt, die aufgrund von Vorurteilen oder Zufällen auf diese Liste gelangt sind. Oder von Personen, die sich kritisch mit der US-Politik auseinandergesetzt haben, beispielsweise JournalistInnen, die über zivile Drohnenopfer berichtet haben. Ebenso wurden Beispiele von Personen bekannt, die als potenzielle Attentäter auf dieser Liste geführt wurden und später Attentate durchführten, ohne vom Geheimdienst daran gehindert worden zu sein.

Wer ins Visier der geheimdienstlichen Zielpersonen-Überwachung gerät, hat es schwer, sich gegen die totale Ausspähung des eigenen digitalen Lebens zu wehren. Die Snowden-Dokumente zeigen, wie vielfältig die Angriffsmöglichkeiten sind und wie viele personelle und technische Ressourcen den Geheimdiensten zur Verfügung stehen.

In den veröffentlichten Snowden-Dokumenten wurde *nicht* über die Beispiele berichtet, bei denen die Geheimdienste auf-

grund von Verschlüsselung bei der Überwachung gescheitert sind. Es gibt diese Beispiele aber in der Praxis, in den veröffentlichten Unterlagen sind sie nur nicht dokumentiert. Das ist auch nicht verwunderlich, denn bei den veröffentlichten Materialien handelt es sich zumeist um interne Präsentationen, die der Selbstdarstellung der NSA dienen. Und warum sollte der US-amerikanische Geheimdienst dabei sein eigenes Scheitern in den Mittelpunkt stellen?

Darum gilt auch hier: Verschlüsselung und Umsicht im Umgang mit der eigenen digitalen Kommunikation schützen besser als keine Verschlüsselung. Eine Verschlüsselung umgehen zu müssen bedeutet immer Aufwand und kostet Ressourcen. Es gibt zwar keine Garantien für eine absolut abgesicherte digitale Kommunikation, aber es gibt auch keine allmächtigen Geheimdienste, denen unbegrenzte Ressourcen zur Verfügung stehen.

«Das Internet ist kaputt.» So fasste Sascha Lobo, Deutschlands bekanntester Blogger, das Ergebnis der Snowden-Enthüllungen für viele NutzerInnen zusammen, die zuvor im Internet einen Raum für mehr Demokratie, Freiheit und Emanzipation gesehen hatten. Spätestens mit den Snowden-Leaks wurde klar: Das Internet ist ein Medium totaler Kontrolle, das die Grundlagen der freiheitlichen Gesellschaft untergräbt.

Diesem Zustand etwas entgegenzusetzen und für die *Aneignung der digitalen Gesellschaft,* für ein *demokratisches Internet* zu kämpfen, ist die Herausforderung, vor der wir aktuell stehen.

WAS TUN?

Die konkreten Möglichkeiten und Praxen der Massenüberwachung verändern sich derzeit ständig: Weitere Veröffentlichungen oder Erkenntnisse des NSA-Untersuchungsausschusses führen zu neuen Diskussionen und Handlungsnotwendigkeiten, Terroranschläge werden zum Anlass genommen, um die Gesetzeslage weiter zu verschärfen, mit Protestbewegungen versuchen AktivistInnen, sich gegen die steigende Anzahl der Zugriffe und Überwachungsmöglichkeiten zu wehren. Auf dem Blog **http://netzfueralle.blog.rosalux.de** werden wir fortlaufend über die aktuellen Entwicklungen berichten.

Denn wir können vieles tun: jede und jeder für sich, vor allem aber auch gemeinsam. Hier eine kleine Auswahl von Ideen und Anregungen für ein demokratisches, sicheres Internet ohne Massenüberwachung.

(QUELL-)OFFEN, DEMOKRATISCH, FREI ZUGÄNGLICH

Viele InternetpionierInnen waren von den demokratischen und emanzipatorischen Potenzialen, die durch die Internettechnologie, durch eine direkte Vernetzung der Weltbevölkerung theoretisch denkbar wurden, fasziniert und angetrieben. Diese Visionen und Hoffnungen haben sich auf unterschiedlichen Ebenen ins Internet eingeschrieben: Ideen wie die Netzneutralität, Entwicklungen wie das World-Wide-Web, aber auch Software-Lizenzen wie Gnu Public Licence (GPL) und Bewegungen wie die Free Software Foundation sind Ausdruck davon.

Free/Libre Open Source Software

Freie Software ist ein Prinzip bei der Entwicklung von Software, das die Freiheiten der EntwicklerInnen und NutzerInnen der Software zentral mitdenkt. NutzerInnen erhalten mit Empfang der Software die vollen Nutzungsrechte und -möglichkeiten. Das beinhaltet, dass der sogenannte Quellcode, also die Dokumentation der Programmierung der Software, für die NutzerInnen zur Analyse und Weiterentwicklung zur Verfügung

gestellt wird. Es beinhaltet auch die Freiheit zur Zusammenarbeit, sodass jede und jeder die Software verändern und anpassen, kopieren und weitergeben darf. Wer freie Software nutzt, hilft bei der Verbreitung von freier Software. Wer die Entwicklung von freier Software durch Arbeitsleistung oder Geldspenden unterstützt, hilft, dass es diese Art von Software überhaupt gibt. Bekannte Beispiele von Freier Software sind die Microsoft Office Alternative *Open Office,* die Cloudspeicher-Alternative *OwnCloud,* der Webbrowser *Firefox,* das E-Mail-Programm *Thunderbird,* das Programm zur E-Mail-Verschlüsselung *GPG* oder das Betriebssystem *Linux.*

Freie Hardware

Ergänzend zur Freien Software gibt es nach gleichem Prinzip auch Freie Hardware, die nach lizenzkostenfreien Bauplänen erstellt wird und dadurch einen Selbstbau und Nachbau ermöglicht. Diese Bewegung ist nicht auf Computertechnologie beschränkt, sondern in vielen Bereichen der Maschinenproduktion vorhanden. Die Bandbreite reicht von freien Strickmaschinen bis zu freien Landmaschinen.

Faire Produktion

Die Produktion von IT-Technologie steht wegen der schlechten Arbeitsbedingungen in den Herstellerbetrieben in der Kritik. Ein bekanntes Beispiel ist einer der weltweit größten Produktionsbetriebe für elektronische Produkte, Foxconn, der vor allem durch unmenschliche Arbeitsbedingungen, hohe Selbstmordraten und niedrige Löhne von sich reden machte. Auf der Ebene der Rohstoffgewinnung fangen die Probleme schon an: Einige zur Herstellung von Computer- und Mobiltelefontechnologie benötigten Metalle, wie beispielsweise Coltan, Cobalt und Zinn, werden in von Warlords kontrollierten Minen abgebaut. Aus den dort erwirtschafteten Gewinnen werden beispielsweise Bürgerkriege finanziert. Inzwischen gibt es erste Unternehmen, die diese Missstände in den Blick nehmen und «faire» Technologien entwickeln wollen. Als Pionier auf diesem Gebiet gilt die niederländische Gesellschaft Fairphone B.V., die ein fair produziertes Smartphone entwickelt und vertreibt.

Verteilte Systeme, vernetztes Handeln

Die Idee von verteilten Systemen ist in vielen Technologien umgesetzt und eigentlich ganz einfach. Wenn es möglich ist, Rechenleistung oder Speicherplatz nicht mehr an einem Ort zu zentralisieren, sind die Lasten und Kosten breit verteilt und das Ausfallrisiko ist geringer. Wenn nur ein zentraler Server für eine bestimmte Leistung zuständig ist, bricht das ganze System zusammen, wenn der zentrale Server ausfällt, abgeschaltet oder kompromittiert wird. Auf dieser Idee basiert Software wie *Tor,* die anonymes Surfen im Internet ermöglicht. Diese Idee ist nicht an Software gebunden – auch die gesamte Internetinfrastruktur lässt sich in diese Logik übersetzen.

Support (your) local provider

Es gibt in vielen Großstädten regionale Diensteanbieter, die sich nicht mit dem Ziel der Profitmaximierung gegründet haben, sondern sich als Vereine oder Genossenschaften für eine Aneignung und Demokratisierung der Internettechnologie starkmachen. Oftmals stellen diese Anbieter nicht nur E-Mail-Adressen, Webspace und vergleichbaren Service zur Verfügung, sondern kümmern sich auch um die Vernetzung und Beratung von NutzerInnen.

Ein Diensteanbieter ganz anderer Art ist die Freifunk-Initiative. Die bundesweite Initiative von Freiwilligen setzt sich für freie Funknetzwerke ein – kostenloses, freies WLAN für alle. Auch hier gilt: Je mehr Menschen mitmachen, desto größer wird die Initiative, desto stabiler werden die Freifunk-Netzwerke: **http://freifunk.net.**

GEHEIMDIENSTE EINSCHRÄNKEN UND KONTROLLIEREN

Bürgerinitiativen, die Grundrechte starkmachen und durchsetzen, haben die Idee von Grundrechten erst politische Realität werden lassen. Aktuell gibt es verschiedene Initiativen, die gegen Massenüberwachung durch Geheimdienste und den Abbau von demokratischen Grundrechten aktiv sind.

NSA-Untersuchungsausschuss

Als Initiative des deutschen Bundestages in seinen Handlungsmöglichkeiten auf die Untersuchung von Regierungshandeln beschränkt, bemüht sich der erste parlamentarische Untersuchungsausschuss um Aufklärung über das Ausmaß und die Hintergründe der Ausspähungen durch ausländische Geheimdienste in Deutschland. Zusätzlich soll nach Strategien gesucht werden, wie die Telekommunikation mit technischen Mitteln besser geschützt werden kann. Nur ein breites außerparlamentarisches Interesse und hohe Erwartungen an diesen Ausschuss können dafür sorgen, dass er Ergebnisse produziert, die Licht ins Dunkel bringen.

Ausgeschnüffelt: Verfassung schützen – Geheimdienst abschaffen!

Die Kampagne «Verfassungsschutz abschaffen!» der Humanistischen Union wird von einem bundesweiten Team von Ehrenamtlichen durchgeführt. Eine Campaignerin in der Bundesgeschäftsstelle der Humanistischen Union begleitet die Kampagne. Das Kampagnenteam ist offen für Ehrenamtliche, die sich mit Tatkraft und Ideen einbringen wollen: **www.verfassung-schuetzen.de/.**

ANEIGNUNG: MEIN COMPUTER GEHÖRT MIR!

Neben dem Aufbau von kooperativen, alternativen Infrastrukturen, politischen Kampagnen und parlamentarischen Initiativen ist jede und jeder individuell gefragt, etwas für ein sicheres, demokratisches Internet zu tun. Wir alle brauchen mehr Verständnis für die technischen Geräte, die wir benutzen, mehr Verschlüsselung in der Alltagskommunikation, mehr Wissen um die technischen Entwicklungen und die Auseinandersetzungen, die derzeit darum geführt werden. Am besten werden wir aber dennoch nicht allein aktiv, sondern gemeinsam mit unseren FreundInnen, NachbarInnen und KollegInnen. Denn zum einen findet Kommunikation in Gruppen statt und kann in diesen auch am besten verändert werden. Zum anderen ist die Aneignung von technischem Wissen in Gemeinschaft viel einfacher als allein.

CryptoPartys besuchen

CryptoParty ist der Name für eine Bildungskampagne, die das Ziel verfolgt, sich im Rahmen eines Do-it-yourself-Treffens gegenseitig grundlegende Verschlüsselungstechniken, wie zum Beispiel Tor, OpenPGP und Festplattenverschlüsselung, beizubringen. CryptoPartys sind öffentlich und unkommerziell und richten sich nicht an ExpertInnen, sondern an DurchschnittsnutzerInnen. Sie finden weltweit in vielen Großstädten statt. Wenn es in deiner Stadt noch keine Cryptoparty gibt, fühle dich eingeladen, eine zu organisieren: **www.cryptoparty.in/parties/upcoming.**

Alltagskommunikation verschlüsseln

Wer schon weiß, wie verschlüsselte Kommunikation mit GPG, OTR, Tor und anderen Werkzeugen geht, kann helfen, diese im Alltag zu verbreiten. Oftmals braucht es nur einen kleinen Anstoß, mit seiner Familie, NachbarInnen oder FreundInnen über sichere Kommunikation zu reden und gemeinsam ganz konkret damit anzufangen. Ihr findet eure Alltagskommunikation nicht wichtig genug? Dann lasst euch versichern: Nichts ist wichtiger für eure Privatsphäre als eure Alltagskommunikation!

Netzpolitik.org lesen

Die Auseinandersetzung um das Recht auf Verschlüsselung, um die Aufklärung der Überwachung durch die Geheimdienste im NSA-Untersuchungsausschuss, um den gesellschaftlichen Wandel hin zu einer digitalen Gesellschaft findet in einem rasanten Tempo statt. Wer bei dieser Auseinandersetzung mit dabei sein will, muss sich darüber informieren. Zu diesem Zweck gibt es Blogs, die sich mit den technischen und regulativen Entwicklungen auseinandersetzen. Einer der bekanntesten Blogs, der ausführlich und umfassend über diese Prozesse berichtet, ist **http://netzpolitik.org.**

Impressum
luxemburg argumente Nr. 10
wird herausgegeben von der Rosa-Luxemburg-Stiftung
V. i. S. d. P.: Stefan Thimmel
Franz-Mehring-Platz 1 · 10243 Berlin · www.rosalux.de
ISSN 2193-5831 · Redaktionsschluss: Juli 2016
Autorin: Susanne Lang
Redaktion: Patrick Stary
Illustration: Navid Thürauf · www.zersetzer.com |||| ||| freie grafik
Lektorat: TEXT-ARBEIT, Berlin
Satz/Herstellung: MediaService GmbH Druck und Kommunikation
Gedruckt auf Circleoffset Premium White, 100 % Recycling

AKTUELLE VERÖFFENTLICHUNGEN

Anna Schiff

IST DOCH EIN KOMPLIMENT ...

Behauptungen und Fragen zu Sexismus

luxemburg argumente Nr. 9
40 Seiten, ISSN 2193-5831
Juni 2016
Download unter:
www.rosalux.de/publication/42416

Bestellung beider Publikationen unter **bestellung@rosalux.de** oder unter **Tel. 030 44310-123**

Christian Jakob

GEGENHALTEN – FLÜCHTLINGE WILLKOMMEN – IMMER NOCH!

Mythen und Fakten zur Migrations- und Flüchtlingspolitik

luxemburg argumente Nr. 8
3., vollständig überarbeitete Auflage
72 Seiten, ISSN 2193-5831
März 2016
Download unter:
www.rosalux.de/publication/40329


ROSA LUXEMBURG STIFTUNG