Geraldine de Bastion und Markus Beckedahl

Für eine digitale Bürgerrechtsbewegung

Am 1. Dezember wurde Edward Snowden in Stockholm mit dem Alternativen Nobelpreis geehrt. „Edward Snowden hat den Bewohnern dieses Planeten einen riesigen Dienst erwiesen", begründete Jakob von Uexküll, der Gründer der Right-Livelihood-Award-Stiftung, die Auszeichnung. „Ohne seinen Mut wüssten wir immer noch nichts über das Ausmaß der neuen Verbrechen, die der technische Fortschritt möglich gemacht hat."

In der Tat würden wir ohne Snowden noch heute im Dunkeln tappen. Zumal die Bundesregierung weder willens scheint, die Ausspähung durch ausländische Geheimdienste aufzuklären, noch irgendwelche Konsequenzen aus diesem Skandal zu ziehen. Stattdessen treten immer wieder neue Details der globalen Überwachung zutage. So wurde nur wenige Tage vor der Verleihung des Alternativen Nobelpreises bekannt, dass der Bundesnachrichtendienst seit 2005 wusste, dass die USA und andere „befreundete Staaten" uns ausspionieren. Dennoch hatte das Bundeskanzleramt seit Beginn der NSA-„Affäre" im Juni vergangenen Jahres immer wieder beteuert, dass es derlei Kenntnisse nicht besessen habe.

Angesichts der andauernden Verweigerungshaltung der Bundesregierung kommt es nun mehr denn je auf eine starke digitale Bürgerrechtsbewegung außerhalb der Parlamente an. Diese muss von unten den Druck auf die politisch Verantwortlichen erhöhen. Andernfalls werden wir womöglich nie das wahre Ausmaß der Überwachung erfahren, geschweige denn diese stoppen können. Dass die netzpolitische Bürgerbewegung dazu in der Lage sein kann, hat sie in der Vergangenheit bereits mehrfach bewiesen. So konnten die bundesdeutsche und europäische Zivilgesellschaft die Einführung der Vorratsdatenspeicherung verhindern und das multilaterale Handelsabkommen ACTA abwenden. Diese Erfolge gingen nicht zuletzt auf die Fähigkeit der Bürgerrechtsorganisationen zurück, zahlreiche Menschen gegen den Abbau der Grundrechte, die Einschränkung des Datenschutzes und die Einrichtung von Überwachungsinstrumenten zu mobilisieren.

Die unsichtbare Überwachung

Im Fall der NSA-Ausspähung ist eine solche Mobilisierung bislang ausgeblieben. Der Hauptgrund dafür liegt in der Unsichtbarkeit der Überwachung: Anders als im Fall der Stasi vollzieht sich die digitale Überwachung durch NSA, GCHQ und Co. größtenteils außerhalb unserer Wahrnehmung. Fing die Stasi Briefe ab, erkannte der Empfänger dies am beschädigten Umschlag. Wir dagegen bemerken es nicht, wenn unsere E-Mails und Chat-Nachrichten in Echtzeit abgegriffen, von Algorithmen gerastert und ausgewertet werden. Ebenso unbemerkt bleibt es, wenn Geheimdienste auf Datenbanken zugreifen, wo unsere Kommunikation, unsere Vorlieben und unser Nutzerverhalten gespeichert sind.

Auch waren sich die meisten DDR-Bürger darüber im Klaren, dass der Nachbar oder die Kollegin jederzeit Informationen an die Stasi weitergeben konnte. Häufig genug bekamen die Betroffenen die Folgen am eigenen Leib zu spüren, etwa wenn sie vorgeladen oder ihnen bestimmte Leistun-

gen verweigert wurden. Heute bleibt die Überwachung oft ohne sichtbare Konsequenzen. Daher sind noch immer viele Bürgerinnen und Bürger davon überzeugt, dass vor allem die Eliten aus Wirtschaft, Politik und Medien von der Ausspähung betroffen sind. Gleichzeitig beruhigen sie sich selbst damit, dass sie ohnehin nichts zu verbergen hätten.

Die Unsichtbarkeit der Überwachung und die Naivität auf Seiten der Überwachten erschweren jedoch die Kampagnenarbeit netzpolitischer Gruppen. Darüber hinaus verstärkt die systematische Aufklärungssabotage der Bundesregierung die Resignation bei den Bürgerinnen und Bürgern. All das erleichtert es der Regierung, die eminenten Rechtsverstöße unter den Teppich zu kehren.

Mangel an Personal

Gleichwohl gibt es hierzulande rund ein Dutzend netzpolitischer Organisationen. Zu diesen zählen unter anderen der Chaos Computer Club, DigitalCourage, Free Software Foundation Europe, AK Zensur, AK Vorrat, Open Knowledge Foundation und die Digitale Gesellschaft. Warum gelingt es ihnen nicht, diesen Teufelskreis aus Verharmlosung und Resignation zu durchbrechen?

Tatsächlich sind die einzelnen Organisationen zwar meist gut miteinander vernetzt, allerdings gibt es viele personelle Überschneidungen der zumeist ehrenamtlichen Aktivisten. Im Ergebnis beschäftigt sich daher gerade einmal ein halbes Dutzend Festangestellte mit dem größten Überwachungsskandal der Menschheitsgeschichte. Darunter leidet insbesondere die professionelle Lobbyarbeit mit dem Ziel, Gesetze durchzusetzen, die dieser Ausspähung einen Riegel vorschieben sollen.

Ganz anders sieht es auf Seiten der Industrie aus: In den vergangenen Jahren haben insbesondere die großen Konzerne ihre Lobbyaktivitäten massiv ausgebaut. Deren Personal übersteigt das der Nichtregierungsorganisationen um ein Vielfaches: Alleine bei Google, Microsoft oder der Deutschen Telekom sitzen mehr bezahlte Lobbyisten als der digitalen Bürgerrechtsbewegung insgesamt zur Verfügung stehen. Die Interessen, die diese Lobbyisten im Auftrag der Konzerne verfolgen, stehen in aller Regel im Gegensatz zu denen der Bürgerrechtler. So versuchen die Internetunternehmen derzeit mit allen Mitteln, die geplante Reform der EU-Datenschutzgrundverordnung zu torpedieren. Diese könnte zu mehr Datensparsamkeit führen und Geheimdiensten den Zugriff auf gespeicherte Nutzerdaten erschweren. Das widerspricht jedoch den Geschäftsmodellen von Google, Microsoft und Co.

Erschwerend kommt hinzu, dass Netzpolitik ein breites Themenfeld ist. Neben der NSA-Affäre binden zahlreiche andere netzpolitische Debatten die Kräfte und Kapazitäten der Organisationen: von der Reform des europäischen Datenschutzes über den Kampf gegen das Freihandelsabkommen TTIP und für den Erhalt der Netzneutralität bis zur überfälligen Urheberrechtsreform.

Einen Ausweg aus der Misere böte eine bessere finanzielle Ausstattung der netzpolitischen Bürgerrechtsbewegungen. Allerdings gibt es in Deutschland nach wie vor kaum Stiftungen oder Verbände, die netzpolitisches Engagement gezielt fördern.[1] Aus diesem Grund sind die meisten Gruppen auf Spendengelder angewiesen. In anderen Ländern sieht die Finanzierungslage wesentlich besser aus: So gibt es in den Niederlanden professionell arbeitende Nichtregierungsorganisationen, beispielsweise *bits of freedom*. Sie allein beschäftigt so viele Mitarbeiter wie alle deutschen netzpolitischen Organisationen zusammen.

1 Eine Ausnahme bietet die Stiftung Bridge, eine Unterstiftung der Bewegungsstiftung.

Herausforderung Vernetzung

Kompensieren ließe sich die dünne Personaldecke durch eine engere Verflechtung der netzpolitischen Gruppen. Allerdings finden sich in den verschiedenen Gruppierungen – trotz der personellen Überschneidungen – sehr unterschiedliche politische Ansätze, wie mit den Snowden-Enthüllungen umzugehen ist.

So spricht sich ein Teil der netzpolitischen Bewegung nicht nur für das Ende der Massenüberwachung aus, sondern fordert auch die Abschaffung aller Geheimdienste. Ein anderer Teil plädiert für eine „realpolitischere" Herangehensweise und tritt für die Reform von Geheimdiensten und eine bessere parlamentarische Kontrolle ein. Eine dritte Gruppe hat die Hoffnung auf eine Selbstkorrektur der Politik völlig aufgegeben: Überzeugt davon, dass die politisch Verantwortlichen zu tief im Überwachungssumpf stecken, konzentriert sie sich ganz auf die digitale Selbstverteidigung. Ihre Kernforderung: die Schaffung möglichst sicherer und damit vertrauenswürdiger IT-Infrastrukturen, die Anonymisierungs- und Verschlüsselungstechnologien implementiert haben. Kurzum: Die sogenannte Netzgemeinde ist keine politische Interessengemeinschaft, die über *eine* gemeinsame Position verfügt – nicht einmal im Fall der Ausspähaffäre. Aus diesem Grund wurden in der jüngsten Vergangenheit verschiedene Protestaktionen höchst unzureichend koordiniert. Bisweilen verliefen sie sogar parallel und behinderten sich damit gegenseitig.

Besonders deutlich wurde dies am Tag der Menschenrechte im Sommer 2013. Zu diesem Anlass stellte ein von der Digitalen Gesellschaft e. V. initiiertes Bündnis unter dem Motto „Stop Surveillance" konkrete Forderungen an die Politik. Mit dabei war ein breites Spektrum an Organisationen, darunter der Chaos Computer Club, Greenpeace und die Reporter ohne Grenzen. Parallel dazu ging ein Netzwerk von kritischen Schriftstellern als „Writers Against Mass Surveillance" mit einer eigenen Petition, „Die Demokratie verteidigen im digitalen Zeitalter", an die Öffentlichkeit. Während die Feuilletons über die Forderungen der Schriftsteller berichteten, erhielt „Stop Surveillance" vor allem in den sozialen Medien Zuspruch. Auf diese Weise nahmen sich beide Ansätze gegenseitig den Wind aus den Segeln, anstatt sich gegenseitig zu bestärken.

Dieser Mangel an Koordination steht exemplarisch für die strukturellen Defizite der Netzbewegung. Sie ist offensichtlich nicht einmal in der Lage, einen Super-GAU wie die Snowden-Enthüllungen politisch gezielt zu nutzen – ganz im Gegensatz zur Umweltbewegung. Nach der Katastrophe von Fukushima gelang es dieser, gemeinsam mit anderen Bündnispartnern, eine große Anzahl von Menschen zu Protestaktionen zu mobilisieren – etwa über Vernetzungsorganisationen wie X1000malquer. Angesichts des wachsenden Drucks sah sich die Bundesregierung schließlich zu einer Abkehr von ihrer Atompolitik gezwungen. Auch wenn es der hiesigen netzpolitischen Zivilgesellschaft gelungen ist, zahlreiche Menschen für das Thema Überwachung zu sensibilisieren – ein vergleichbarer Erfolg liegt derzeit in weiter Ferne.

Digitale Selbstverteidigung

Dennoch müssen wir der anhaltenden Überwachung keineswegs hilflos gegenüber: Jeder Einzelne kann sich schon jetzt gegen die Ausspähung durch die Geheimdienste zur Wehr setzen – mit Hilfe digitaler Selbstverteidigung.

Bislang unterstützten Anonymisierungswerkzeuge wie TOR vor allem Dissidenten in repressiven Regimen bei ihrer politischen Arbeit. TOR verschleiert die Herkunft von Anfragen

im Internet und schützt Nutzer damit effektiv vor staatlicher Verfolgung und Repression. Mehr und mehr werden diese Instrumente zur digitalen Selbstverteidigung jedoch auch bei uns eingesetzt. Alleine in Deutschland ließ sich 2013 eine Vervierfachung der Nutzer des TOR-Netzwerkes beobachten: Deren Zahl stieg von rund 60 000 auf 230 000.

Dass Verschlüsselung eine Ausspähung zumindest erheblich erschwert, zeigt sich bereits daran, dass die Verbreitung von TOR der US-Regierung ein Dorn im Auge ist. Anfang Juli wurde bekannt, dass der Erlanger Student Sebastian Hahn unter besonderer Beobachtung der NSA steht. Der Grund: Hahn betreibt einen eigenen TOR-Server, dessen Dienste Nutzer auf der ganzen Welt in Anspruch nehmen können. Laut internen Geheimdienstdokumenten macht dies den Studenten zum Extremisten. Sebastian Hahn hingegen sieht sein kostenloses Angebot vor allem als Ausdruck bürgerschaftlichen Engagements zum Wohle der Allgemeinheit: „Privatsphäre ist Grundrecht, kein verschrobenes Ziel sogenannter Extremisten", so Hahn.

Dass unbescholtene Bundesbürger von den US-Behörden als Extremisten eingestuft und besonders überwacht werden, zeigt, wie bedroht unsere demokratischen Grundwerte schon jetzt sind. Und auch hierzulande wurden Aktivisten, die sich für digitale Selbstverteidigung einsetzen, immer wieder von Politik und Sicherheitsbehörden in die Nähe von Kriminellen gerückt. So bezeichnete der Verfassungsschutz die Nutzer von Verschlüsselungssoftware ebenfalls pauschal als Extremisten.

Seiner Verantwortung für die Rechte seiner Bürger einzustehen, wird der Staat dadurch gerade nicht gerecht: Statt Instrumente der digitalen Selbstverteidigung zu kriminalisieren, müsste er die nutzerfreundliche Entwicklung von Open-Source-Projekten fördern, wie etwa die Mailverschlüsselung *gnupg*. Nur dann ist es langfristig möglich, dass solche Instrumente auch von nichttechnikaffinen Menschen genutzt werden können.

Immerhin hat die Wirtschaft das Potential sicherer Kommunikationsinstrumente längst erkannt – auch wenn sie dabei nicht in erster Linie den Schutz der Grundrechte, sondern ihren eigenen Profit im Sinn hat. So bieten GMX und andere deutsche Anbieter inzwischen an, E-Mails verschlüsselt zu übertragen. Damit ist zwar noch nicht die sichere Verschlüsselung der Nachrichten selbst, sondern nur die Absicherung ihres Übertragungswegs gemeint. Dennoch lassen derlei Ankündigungen hoffen, dass die Bedienung von Verschlüsselungssoftware künftig einfacher wird und so mehr Menschen ihre Daten vor fremdem Zugriff schützen werden. Denn nicht nur für Journalisten und politisch Aktive sollte eine vertrauliche Kommunikation selbstverständlich sein, sondern auch für alle anderen Bürgerinnen und Bürger.

Fest steht aber auch: Die neuen Produkte senken nicht den politischen Handlungsdruck. Die Enthüllungen Edward Snowdens haben die Frage nach dem politischen System, in dem wir leben wollen, auf die politische Tagesordnung gehoben – und wie der Bürger vor unzulässigen Zugriffen des Staates geschützt werden kann.

„Seine Bevölkerung auszuspionieren ist der Anfang von Totalitarismus", sagte der ehemalige technische Direktor der NSA, William Binney, bei der vierten Anhörung im NSA-Untersuchungsausschuss im Deutschen Bundestag und beklagte „die größte Bedrohung der Demokratie seit dem Amerikanischen Bürgerkrieg".

Gegen diese neue Form des Totalitarismus anzukämpfen, ist die Aufgabe der digitalen Bürgerrechtsbewegung. Dabei geht es um nicht weniger als die Souveränität der Bürger, eine funktionierende Gewaltenteilung sowie die Transparenz staatlichen Handels – sprich: um die Grundwerte unserer Demokratie.