Daniel Leisegang

Schöne neue Überwachungswelt

Nun herrscht Gewissheit: Wir leben tatsächlich in einer Überwachungswelt. Diese Erkenntnis verdanken wir dem ehemaligen US-Geheimdienstmitarbeiter Edward Snowden. In den vergangenen Wochen veröffentlichte er in Kooperation mit dem britischen „Guardian" eine Reihe brisanter Dokumente, denen Interviews in Zeitschriften aller Welt folgten. Ihnen zufolge überwachen angelsächsische Nachrichtendienste fast unsere gesamte Kommunikation – auch und vor allem im Internet.

Überraschend ist weniger die Überwachung selbst, als vielmehr ihr ungeheures Ausmaß. So späht der amerikanische Militärgeheimdienst National Security Agency (NSA) insbesondere Kommunikationsdienste, Soziale Netzwerke sowie Cloud-Speicher aus – und das weltweit. Dazu fordert sein Spähprogramm *Prism* gezielt private Nutzerdaten bei Konzernen wie Microsoft, Yahoo, Google oder Facebook an. Jeden Monat spioniert die NSA zudem mehr als eine halbe Mrd. Telefonate, SMS-Nachrichten und Emails deutscher Bürger aus.

Auch der britische Dienst Government Communications Headquarters (GCHQ) liest im großen Stil mit. Statt wie die NSA nur die Nutzerdaten abzufragen, zapft er seit Jahren im Rahmen seines Spionageprogramms *Tempora* mehr als 200 internationale und interkontinentale Glasfaserkabel direkt an, darunter auch das TAT-14 im Atlantik, das einen großen Teil der deutschen Überseekommunikation weiterleitet. Die Briten teilen die abgesaugten Daten – schätzungsweise 21 000 Terabyte am Tag – mit den Vereinigten Staaten: 300 GCHQ- und 250 NSA-Agenten werten die Informationen gemeinsam aus.[1]

Noch immer dürften nicht alle Fakten der nachrichtendienstlichen Exzesse auf dem Tisch liegen. Doch schon jetzt steht fest: Die Grenzen zwischen dem Gebaren vorgeblich rechtsstaatlich begrenzter Geheimdienste im „Krieg gegen den Terror" und den Überwachungsmethoden totalitärer Staaten sind kaum noch zu erkennen. Die nun offenbar gewordene umfassende Spionage unterwirft die Bürger potentiell vollständiger geheimdienstlicher Kontrolle, hebelt ihre Grundrechte aus und unterhöhlt das Vertrauen in den demokratischen Rechtsstaat.

Geheimdienste außer Kontrolle

Dass es überhaupt soweit kommen konnte, liegt vor allem an der wachsenden Macht der Dienste. Verantwortlich dafür ist in erster Linie die unzureichende richterliche und legislative Kontrolle, der sie unterliegen. Das gilt für die USA und Großbritannien genauso wie für die Bundesrepublik.

Die NSA ist mit einem Jahresbudget von zehn Mrd. US-Dollar und über 30 000 Mitarbeitern der mächtigste der insgesamt zehn US-Geheimdienste. Unmittelbar nach den Enthüllungen verteidigte sie die Überwachungsmaßnahmen gegenüber der eigenen Bevölkerung: Diese würden gemäß des *Foreign Intelligence Surveillance Act (Fisa)* richterlich genehmigt; zudem seien allein Nicht-Amerikaner von den Spähaktionen betroffen.

1 Vgl. www.wired.co.uk, 24.6.2013 sowie Sean Gallagher, What the NSA can do with „big data", www.arstechnica.com, 12.6.2013.

Zwar muss der sogenannte Fisa-Gerichtshof (Fisc) die Überwachungen der NSA in der Tat genehmigen. Er ist jedoch kaum mehr als ein Schattengericht: Gerade einmal 11 der insgesamt knapp 34 000 Überwachungsanträge hat der Fisc zwischen 1979 und 2012 abgewiesen; seine Sitzungen und Beschlüsse unterliegen zudem grundsätzlich der Geheimhaltung.[2]

Aus diesem Grund blieb auch die seit Jahren währende Ausspähung von Millionen US-Bürgern lange Zeit geheim. Erstmals im Jahr 2006 zwang der Fisc den größten Mobilfunkanbieter der USA, Verizon, die Verbindungsdaten all seiner Kunden – wer mit wem, wann und wie lange kommuniziert hat – für die Dauer von drei Monaten an die NSA zu übermitteln. Die Vorsitzende des Kongressausschusses für die Nachrichtendienste, Dianne Feinstein, hat inzwischen eingeräumt, dass das Gericht den Beschluss seit sieben Jahren alle drei Monate erneuert.[3]

Noch im März erklärte der Direktor der nationalen Nachrichtendienste, James Clapper, auf die Frage des *Senate Intelligence Committee*, ob die NSA Daten amerikanischer Bürgern sammle: „Zumindest nicht willentlich." Wie wir heute wissen, war das glatt gelogen. Nach den Enthüllungen rechtfertigte sich Clapper dreist, er habe damit nur die „am wenigsten unwahre Antwort" gegeben. Die Reaktion veranschaulicht, wie machtlos die parlamentarischen Ausschüsse dem Treiben der NSA zusehen. Und niemand hindert diese daran, weiter aufzurüsten: Im kommenden Herbst eröffnet die NSA im US-Bundesstaat Utah ein neues Rechenzentrum, und zwar das größte der Welt. Dessen Kapazitäten reichen theoretisch aus, um jedem lebenden Menschen mindestens ein Terabyte Speicherplatz zu reservieren.[4]

2 Vgl. Foreign Intelligence Surveillance Act Court Orders 1979-2012, www.epic.org.
3 Vgl. „The Guardian", 6.6.2013.
4 Ein Terabyte entspricht etwa der Größe einer derzeit handelsüblichen Festplatte.

Das britische Gegenstück zum Fisa – der *Regulation of Investigatory Powers Act* (Ripa) – erlaubt es dem GCHQ, abgefangene Kommunikationsinhalte für drei Tage und Metadaten[5] sogar für 30 Tage zu speichern und nach Kriterien wie „Organisierte Kriminalität, Sicherheit, Terrorismus und wirtschaftliches Wohlergehen" zu durchleuchten. Eine richterliche Kontrolle benötigt der Dienst nicht: Um sämtliche Abhörmaßnahmen für die Dauer von sechs Monaten zu autorisieren, bedarf er nur der Generalvollmacht des britischen Außenministers.[6]

Das deutsche Prism: Die „Strategische Fremdaufklärung"

Von den Lauschangriffen will der Bundesnachrichtendienst (BND), der dem Bundeskanzleramt untersteht, angeblich nichts gewusst haben. Das ist allerdings wenig glaubwürdig: Schon länger kooperiert der deutsche Geheimdienst mit den Briten und Amerikanern – und dürfte dabei neidvoll auf deren Programme blicken.[7]

Denn der BND verfügt zwar ebenfalls über ein Spähprogramm – mit dem sperrigen Titel „Strategische Fernmeldeaufklärung". Die Bedingungen unter denen deutsche Nachrichtendienste das im Grundgesetz garantierte Brief-, Post- und Fernmeldegeheimnis verletzten dürfen, nennte dabei das sogenannte Artikel-10-Gesetz. Demnach dürfte der Dienst bis zu 20 Prozent der grenzüberschreitenden Kommunikation auswerten. Allerdings kann er – aus technischen Gründen – derzeit nur fünf Prozent bearbeiten.[8]

Auch der BND schöpft die Kommunikation direkt im Netz ab: Dazu werden Daten, die über den zentralen

5 Metadaten enthalten Informationen über die Eigenschaften anderer Daten.
6 Vgl. „The Guardian", 24.6.2013.
7 Vgl. „Der Spiegel", 28/2013.
8 Der BND soll daher in den kommenden Jahren technisch aufgerüstet werden, vgl. „Frankfurter Allgemeine Sonntagszeitung", 21.6.2013.

deutschen Internetknoten „DE-CIX“ in Frankfurt am Main laufen, teilweise für ihn „ausgeleitet“.[9] Wie dies genau geschieht und ob der deutsche Dienst die Informationen auch an die NSA weitergibt, werden wir wahrscheinlich nie erfahren – weder von den Geheimdiensten noch von unseren gewählten Abgeordneten: Sie unterliegen, sofern sie überhaupt Details erfahren, einer strengen Schweigepflicht.

Die G-10-Kommission, die „über die Zulässigkeit und Notwendigkeit von Beschränkungsmaßnahmen“ entscheidet, tagt geheim. Sie besteht aus vier vom Bundestag ernannten Mitgliedern – von denen derzeit nur eines dem Parlament angehört. Und auch die legislative Kontrolle der Geheimdienste erfolgt im Verborgenen: Dem zuständigen Parlamentarischen Kontrollgremium (PKG) gehören elf Bundestagsabgeordnete an. Dabei entscheidet die Bundesregierung, welche Informationen sie dem Gremium vorlegt. Getagt wird ebenfalls hinter verschlossenen Türen, alle Mitglieder sind zur strikten Verschwiegenheit verpflichtet – auch gegenüber anderen Abgeordneten. Kurzum: Gerade einmal 12 der insgesamt 620 Bundestagsabgeordneten erhalten detailliertere Informationen über die Arbeit der Geheimdienste.

Mit dem neuen Telekommunikationsgesetz, das seit dem 1. Juli in Kraft ist, wird dem BND das Ausspähen privater Daten zusätzlich erleichtert. Es erlaubt Ermittlern bereits bei Verdacht auf eine Ordnungswidrigkeit, die bei Telefon- und Internetanbietern hinterlegten Personendaten und IP-Adressen abzufragen – ohne vorherige richterliche Prüfung. Weil mehr als 4000 Bundesbürger diese sogenannte Bestandsdatenauskunft als verfassungswidrigen Eingriff in ihre informationelle Selbstbestimmung werten, haben sie in Karlsruhe Verfassungsbeschwerde eingereicht.[10]

Die Aushebelung der Grundrechte

Die Annahme, das Internet sei ein rechtsfreier Raum, hat sich somit bewahrheitet – wenn auch ganz anders als bislang immer behauptet: Jahrelang haben Regierungen uns weismachen wollen, das Netz benötige mehr Regulierung und Überwachung, um kriminellem Treiben Einhalt zu gebieten. Derweil schufen sie hinter unserem Rücken einen Überwachungskomplex, der sich selbst rechtsstaatlicher Kontrolle entzieht und demokratische Grundrechte aushebelt.

Eben darin zeigt sich auch der wesentliche Unterschied zwischen polizeilicher und nachrichtendienstlicher Arbeit: Polizeilichen Ermittlungen muss ein ausreichender Anfangsverdacht vorausgehen. Erst dann ist auch die Einschränkung des Fernmeldegeheimnisses erlaubt. Bei den Ausspähprogrammen der Geheimdienste ist jedoch genau das Gegenteil der Fall: Jeder Internetnutzer wird potentiell überwacht, in der Hoffnung, irgendwann ein Muster zu erkennen und einen Treffer zu landen – eine Unschuldsvermutung existiert nicht. Der Stabschef des ehemaligen US-Verteidigungsministers Leon Panetta veranschaulichte dies kürzlich so: „Wer eine Nadel in einem Heuhaufen sucht, benötigt zuerst einmal einen Heuhaufen.“[11]

Auf diese Weise erklären die Dienste alle Bürger zu Verdächtigen, ja sogar zu Staatsfeinden: Von Prism und Tempora wissen wir nur, weil uns ein Whistleblower unter hohem persönlichen Risiko darüber informiert hat. Statt jedoch zu den schwerwiegenden Anschuldigungen Stellung zu nehmen, hat die Obama-Regierung derzeit nichts Besseres zu tun, als den „Landesverräter“ erbarmungslos zu jagen. Edward Snowden ist dabei beileibe kein Einzelfall: Die derzeitige US-Regierung hat aufgrund des *Espionage Act* aus dem Jahr 1917 bisher doppelt

9 Vgl. www.heise.de, 2.7.2013.
10 Vgl. www.bestandsdatenauskunft.de.
11 Vgl. „The New York Times“, 8.6.2013.

so viele Fälle wegen Geheimnisverrats verfolgt wie alle Regierungen vor ihr.[12]

Die Ohnmacht der Bürger

Der einzelne Bürger steht dem totalitären Anspruch der Dienste weitgehend machtlos gegenüber. In Sorge um die wachsenden Datenberge privater Konzerne wie Apple, Google oder Facebook kann er zwar sein dortiges Nutzerkonto kündigen, wenn jedoch staatliche Institutionen im Verborgenen agieren und dauerhaft Grundrechte missachten, gibt es für den Bürger kein Entkommen.[13]

Gewiss, er könnte resignativ den sakrosankten Status seiner Privatsphäre aufgeben – ganz nach dem Motto: „Wer nichts zu verbergen hat, hat auch nichts zu befürchten". Eine solche Haltung hieße jedoch, eine für die Demokratie wesentliche Begrenzung aufzugeben: Gerade der Lebensbereich des Privaten soll vor dem unverhältnismäßigen Zugriff des Staates schützen. Unterhöhlen die Geheimdienste diesen Rückzugsraum, droht damit ein Fundament demokratischer Gesellschaften wegzubrechen.

Auch eine konsequente Verschlüsselung der eigenen Kommunikation hilft nur begrenzt. Gerade verschlüsselte Daten speichert beispielsweise die NSA solange, bis eine eingehende Analyse der Daten und möglicherweise sogar ihre Entschlüsselung erfolgen kann. Diese Form der digitalen Selbstverteidigung mag daher ein sinnvoller Schritt sein, um den Geheimdiensten die persönlichen Daten nicht auf dem Silbertablett zu servieren. Am Ende kommt es jedoch zum Wettlauf zwischen einzelnen, technisch versierten Nutzern und den Nachrichtendiensten – wobei Letztere aufgrund ihrer Kapazitäten wahrscheinlich den längeren Atem haben werden.

Daher bietet allein eine politische Lösung den Ausweg aus dem geheimdienstlichen Ausnahmezustand. Gerade von der Bundesregierung sollte man ein rasches und entschlossenes Handeln erwarten: Schon die lückenhafte Aufklärung des Versagens des Bundesamtes für Verfassungsschutzes bei den NSU-Morden hat das Vertrauen der Bevölkerung in die hiesigen Behörden erheblich geschwächt.[14]

Dieses Mal könnte der Vertrauensverlust noch dramatischer ausfallen: Denn der „Krieg gegen den Terror" dient den Regierungen und ihren Geheimdiensten in erster Linie als Legitimation, um weitere Befugnisse und mehr Macht einzufordern. Ein Staat jedoch, der seine eigenen Bürger (und die Bürger anderer Staaten) systematisch ausspioniert, ist kein freiheitlicher Rechtsstaat mehr. Um die Balance zwischen Freiheit und Sicherheit wiederherzustellen, müssen die Regierungen daher die Ausspähung der Bürger beenden und die Geheimdienste einer strikten demokratischen Kontrolle unterwerfen.

Das will auch Barack Obama erkannt haben – wenn man seinen Worten denn noch Glauben schenken darf. Ende Mai – und damit nur wenige Tage vor den Enthüllungen Snowdens – kündigte der Präsident in einer aufsehenerregenden Rede die grundlegende Prüfung der US- Sicherheitspolitik an: Auch der „grenzenlose, weltweite Krieg gegen den Terror" müsse einmal ein Ende finden.[15] In der Tat, es ist höchste Zeit: Der „mächtigste Mann der Welt" sollte seinen Worten Taten folgen lassen und seine Geheimdienste stoppen – bevor es am Ende zu spät ist.

12 Vgl. „Frankfurter Allgemeine Zeitung", 21.5.2013; vgl. auch Ralph Sina, George W. Obama: Das Ende einer Hoffnung, in: „Blätter", 7/2013, S. 5-8.

13 Besonders drastisch zeigt sich dies am Beispiel Guantánamo, wo noch immer 46 „Terrorverdächtige" ohne Aussicht auf ein rechtsstaatliches Verfahren als „unbefristete Häftlinge" eingestuft sind. Vgl. „Spiegel Online", 18.6.2013.

14 Vgl. den Beitrag von Micha Brumlik und Hajo Funke in dieser Ausgabe.

15 Vgl. „The New York Times", 23.5.2013.