Auch du bist verdächtig!

Dank Edward Snowden wissen wir, wie detailliert und umfassend die globale Überwachung abläuft. Dabei gilt: Jeder ist verdächtig. Die Ausmasse sind gigantisch, die Aussichten trübe. Das müsse sich ändern, schreibt der eidgenössische Datenschützer.

von Hanspeter Thür

Eines muss man der National Security Agency (NSA) attestieren: Durch ihre skandalösen Überwachungspraktiken hat sie eine weltweite Debatte über das gewaltige Ausmass der heute möglichen und auch praktizierten globalen Überwachung der Bürger in Gang gesetzt. Damit hat sie auch den oft zitierten Satz «Wer nichts zu verbergen hat, hat nichts zu befürchten» in seiner Naivität gründlich entlarvt. Es verwundert darum nicht, dass er kaum noch zu hören ist. Was hingegen weiterhin erstaunt, ist die grosse Indifferenz, mit der Bürger und Politiker den Skandal ertragen.

Entwarnung ist nicht angesagt und ein sorgfältigeres Hinschauen über Möglichkeiten staatlicher Überwachung und allfällige Gegenstrategien ein Gebot der Stunde. Denn so viel ist klar: Der gläserne Mensch ist keine Chimäre mehr, sondern längst Realität. Die Digitalisierung unserer Lebenswelt hat mit erbarmungsloser Konsequenz dazu geführt, dass früher oder später alles öffentlich wird, ob wir das nun wollen oder nicht. Dieser Konsequenz ist es zu verdanken, dass der Geheimdienst selber – Ironie der Geschichte – Opfer jener Untaten wurde, die er im Geheimen – nomen est omen – veranstalten wollte.

Snowden sei Dank, könnte man an dieser Stelle seufzen. Aber: Wer – wie er und die allermeisten Kommentatoren der losgetretenen Debatte – in der Frage der allumfassenden Überwachung nur auf die geheimen staatlichen Behörden fokussiert, greift zu kurz. Denn es sind gerade privatwirtschaftliche Firmen, die längst begriffen haben: Daten sind Business. Daten sind Geld. Daten sind Macht.

Die auf privater Basis entstandenen und laufend weiter entstehenden riesigen Datenberge sind das Material, mit dessen Hilfe jeder einzelne bis ins Detail in seinen Vorlieben, Eigenschaften, Stärken und Schwächen von der konsuminteressierten Wirtschaft ausgeforscht werden kann. Wenn Private diese Aufgabe freiwillig erledigen, liegt es auf der Hand, dass staatliche Behörden – da ist die NSA nur eine von vielen – auf Facebook und sonstwo auf das verfügbare Datenmaterial zugreifen. Konsument, User und potentiell verdächtiger Bürger konvergieren.

Dieser Datenberg wäre an sich so lange noch kein Anlass zur Sorge, als man einwenden könnte: «Wer findet in diesem Heuhaufen schon die Nadel?» Doch zeugt dieser Einwurf von der Unkenntnis technischer Möglichkeiten. Big Data ist dank der heutigen immensen Rechnerkapazitäten und automatisierten Analyseverfahren längst nicht mehr ein Buch mit sieben Siegeln. Heute gilt vielmehr die Losung: Je mehr Daten zur Verfügung stehen, desto präzisere Aussagen und Erkenntnisse über das gegenwärtige und künftige Verhalten der Menschen sind möglich.

Hanspeter Thür
ist Rechtsanwalt und seit 2001 Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter. Von 1987 bis 1999 war er Nationalrat für die Grüne Partei der Schweiz.

Konsequente Verdächtigung

Mit Hilfe von leistungsfähigen Computern und riesigen Speichermedien ist es möglich, diesen Heustock zu durchwühlen und Korrelationen und Muster – sprich Algorithmen – zu entdecken, die aufsehenerregende Erkenntnisse zutage fördern. Diese gefundenen Korrelationen müssen in absolut keinem logischen Zusammenhang stehen. Ist der Datenberg gross genug, kann vielleicht ein Algorithmus entdeckt werden, der mit hoher Wahrscheinlichkeit voraussagt, dass eine Glatze hat, wer gelbe Schuhe trägt. Man mag hier einwenden: Mit welcher Wahrscheinlichkeit und unter welchen Umständen jemand eine Glatze trägt, ist auf den ersten Blick keine Erkenntnis, die uns schockieren müsste. Ich würde erwidern: Gefährlich kann es immer werden, weil auf diesem Weg kompromittierende Handlungen oder Eigenschaften von Menschen entdeckt werden können. Gefährlich deshalb, weil der Algorithmus nie eine gesicherte Erkenntnis darstellt und schon gar nie eine nachprüfbare, wissenschaftlich gesicherte Kausalität ausdrückt. Es sind immer Aussagen, die mehr oder weniger wahrscheinlich zu- bzw. eintreffen können. Wenn der Algorithmus Aussagen zu einem möglichen kriminellen Verhalten von Menschen macht, kann dies für den einzelnen verheerend sein. Mit Sicherheit ungemütlich wird es für Herrn X dann, wenn ein Geheimdienst aufgrund der Datenlage einen Algorithmus entdeckt, der ihn mit 90prozentiger Wahrscheinlichkeit als Terroristen identifiziert. Kommt hinzu, dass dieser Algorithmus für viele andere Personen ebenfalls zutreffen kann, wenn eine grosse Menschenmenge unter

Hanspeter Thür, photographiert von Philipp Baer.

die Lupe genommen wird und diese Menschen dann ebenfalls unter Verdacht fallen.

Genau so operieren Geheimdienste wie die NSA, denen die Unschärfe ihrer Analyse offenbar egal ist. Der Zweck der angeblichen Sicherheit heiligt die Mittel der konsequenten Verdächtigung. Das kann durchaus dramatische Folgen für Bürgerinnen und Bürger haben: Die amerikanische Menschenrechtsorganisation ACLU beschuldigte 2009 das FBI gestützt auf einen Prüfbericht des US-Justizministeriums, hunderttausende Menschen ohne ausreichende Beweise als Terrorverdächtige auf einer Liste zu führen.

Algorithmen können die Persönlichkeitsrechte und das informationelle Selbstbestimmungsrecht der Bürger auch in weniger heiklen Fällen verletzen. Zum Beispiel, wenn sie im Rahmen von Marktanalysen von privaten Firmen eingesetzt werden. Denn die Analyse einschlägiger Daten kann den Schluss nahelegen, dass Frau Y sehr wahrscheinlich vor einer Scheidung steht. Bedenklich ist nicht, dass Frau Y deswegen gezielt mit Ratgeberliteratur bedient wird, sondern dass die Datenanalytiker offensichtlich Dinge wissen, die Frau Y nicht an die grosse Glocke hängen möchte und unter Umständen sogar selber noch gar nicht weiss.

Vor acht Jahren hat mir ein Spezialist auf diesem Gebiet folgende Geschichte aus seiner Praxis erzählt: Eine Bank wollte herausfinden, aus welchen Gründen Kunden ihre Bankbeziehung in gehäuftem Masse beendeten. Sie stellte dem Analytiker zu diesem Zwecke sämtliche Transaktionsdaten ehemaliger Bankkunden zur Verfügung. Dabei entdeckte er einen Algorithmus, mit dem er den bevorstehenden Tod von Kunden mit einer sehr hohen Wahrscheinlichkeit voraussagen konnte. Der IT-Spezialist erzählte diese Geschichte in einem sehr kleinen Kreis, wo es um die Möglichkeiten und auch die moralischen Fragen rund um das Costumer Relationship Management ging. Wer da keine Skrupel hat, der hat ganz rasch ein lukratives Angebot auf dem Tisch. Daten sind Geschäftspotential. Sind Geld. Sind Macht. Darum gilt die Regel: Firmen und Staaten machen, was technisch machbar ist – sofern sie nicht durch individuelles Verantwortungsbewusstsein, Verfassung und Gesetze eingeschränkt werden. Der genannte Analytiker erinnerte sich an ersteres, bekam nach der Übernahme dieses Auftrags Skrupel – und beendete ihn.

Was lehrt uns diese Geschichte? Bereits vor acht Jahren konnten mit der Analyse von Transaktionsdaten einer Bank weitreichende Aussagen über eine Person und sie betreffende künftige Ereignisse gemacht werden. Inzwischen hat sich die Situation in verschiedene Richtungen dramatisch verändert. Der zur Verfügung stehende Datenberg ist immens gewachsen. Und er wächst täglich mit 2,5 Quintillionen Byte (eine Zahl mit 30 Nullen!) und verdoppelt sich alle zwei Jahre. Kommt hinzu, dass sich die Rechner- und Speicherkapazitäten, die erst die Durchleuchtung dieses wachsenden Datenbergs ermöglichen, ebenfalls ständig verbessern. Werfen wir einen Blick in die Zukunft, bewegen wir uns längst auf dem Boden gesicherter Fakten, wenn wir in Aussicht stellen: In absehbarer Zeit kann jeder auf diesem Globus, der aus irgendeinem Grund in den Fokus bestimmter politischer, geheimdienstlicher oder wirtschaftlicher Interessen gerät, bis in weite Teile seiner Persönlichkeit durchleuchtet werden. Und andere Menschen wissen Dinge von ihm, die ihm selber unbekannt sind. Die Tyrannei der Algorithmen wird zu einer totalen Vermessung des Menschen und einer Vorhersage seines möglichen Verhaltens führen.

Dank demselben Rechenpotential lässt sich heute eine Person mit Hilfe sehr weniger Informationen identifizieren. Postleitzahl, Geschlecht und Geburtsdatum genügen, um eine Person in den USA mit einer Wahrscheinlichkeit von 87 Prozent zu bestimmen. Und mit Blick auf Big Data – das grosse Geschäft der Zukunft – muss man wissen, dass die Forderung nach Anonymisierung kaum einen ausreichenden Schutz gewährleisten wird. Der renommierte IBM-Forscher Günter Karjoth (ein Mann mit über 60 wissenschaftlichen Publikationen und zahlreichen Patenten) präsentierte kürzlich an einer Veranstaltung eine Krankenakte mit Geburtsdatum, Postleitzahl, Geschlecht und Krankheit und sagte: Wird ein solcher Datensatz mit einem öffentlichen Wahlregister abgeglichen, wie es in den USA existiert, können 60 bis 80 Prozent der Datensätze deanonymisiert werden. Acxiom, der weltgrösste amerikanische Datenbroker, behauptet stolz von sich, weltweit über 700 Millionen detaillierte Profile von Konsumenten zu verfügen. Was heisst hier detailliert? Man höre und staune: Acxiom will eigenen Angaben zufolge 3000 Eigenschaften pro Konsument kennen, angefangen bei Ethnie und politischer Neigung über Quadratmetergrösse der Wohnung bis hin zum Typ des hauseigenen Autos. Und jährlich nimmt die Firma aus Arkansas 11 Billionen Aktualisierungen vor, um die Profile à jour zu halten und zu ergänzen.

Gibt es harmlose Daten?

Die Tatsache, dass zahlreiche Akteure mithelfen, das Wachstum des Datenbergs zu beschleunigen, ruft gebieterisch nach der Frage, ob es überhaupt noch harmlose Daten gibt, weil sie mit allem und jedem verknüpft werden können; weil sie auf die eine oder andere Weise stets auch dazu dienen können, eine Person noch besser zu beschreiben. Wie ist Open Data Government, das von Verwaltung, Politik und Wirtschaft massiv vorangetriebene Projekt, das grosse Teile staatlicher Datenbestände öffentlich zugänglich und wirtschaftlich verwertbar machen will, unter diesem Aspekt zu beurteilen? Und wie Big Data, das Öl der Zukunft, wie ihre Promotoren euphorisch verkünden? Und wie soziale Netzwerke, wo Nutzer im grossen Stil zum Teil sehr Intimes über ihre Wünsche und Absichten kundtun, weil sie immer noch nicht begriffen haben, dass die Dienste letztlich einen hohen Preis haben, weil sie Geschäfte mit den Daten der User machen?

Kurz und gut, was ist aus datenschutzrechtlicher Sicht zu tun angesichts dieser Perspektive? Längst gibt es Stimmen, die verkünden, Privatsphäre sei ein überholtes Konzept und passe

«Daten sind Geschäftspotential. Sind Geld. Sind Macht. Firmen und Staaten machen, was technisch machbar ist.»

Hanspeter Thür

nicht mehr in die heutige Zeit. Jeder soll alles über alle wissen können. Eric Schmidt von Google höhnt: «Wenn es etwas gibt, von dem Sie nicht wollen, dass es irgendjemand erfährt, sollten Sie es vielleicht nicht tun.» Marc Zuckerberg von Facebook formuliert es so: «Die Zeiten, in denen man seinen Kollegen eine Persönlichkeit präsentieren konnte und Freunden eine andere, sind vorbei.»

Keine Kapitulation

Als Datenschützer kann ich mit derlei naiven, sozusagen dem Tag verhafteten Verlautbarungen nicht viel anfangen. Ihnen fehlt die historische Perspektive. Ich betrachte sie als Kapitulation vor der Macht des Faktischen. Wir haben eine Verfassung, die die Freiheitsrechte schützt – und dazu gehören auch der Schutz der Privatsphäre und informationelle Selbstbestimmung –, und diese Grundsätze gilt es auch im digitalen Bereich durchzusetzen. Doch stellt sich die Gretchenfrage, ob Verantwortungsträger in Politik und Wirtschaft auf der Höhe ihrer Aufgabe sind und das tun, was zur Verteidigung der verfassungsrechtlichen Ordnung nötig ist. Ich habe, ehrlich gesagt, meine Zweifel. Obwohl seit längerem – ausgelöst durch den technischen Fortschritt – Big-Brother-Szenarien Gegenstand öffentlicher Debatten sind, ist unsere Demokratie merkwürdig passiv geblieben. Daran änderte auch der NSA-Skandal – jedenfalls bis heute – nicht viel. Man schüttelt den Kopf, aber hat sich damit abgefunden. Warum bloss? Was muss passieren, damit Unbehagen in Protest umschlägt? Warum haben viele das Gefühl, man könne ohnehin nichts tun – ausser E-Mails verschlüsseln (die die Geheimdienste dennoch knacken) oder sich aus sozialen Netzwerken verabschieden?

Was Edward Snowden aufgedeckt hat, sei der Prototypus einer Zeitmaschine, mit der man in die Vergangenheit und die Zukunft reisen könne. Datenfusion (bzw. Datenverknüpfung) diene der Beantwortung von zwei Fragen: jener nach dem, was einer getan habe, und, noch wichtiger, jener nach dem, was er noch tun werde. Mit diesen Worten beschreibt die Schriftstellerin Juli Zeh in der FAZ den Erkenntnisgewinn dank Snowden. Und sie fragt: Wenn die algorithmische Prognose ergebe, dass eine Person mit einer 95prozentigen Wahrscheinlichkeit in Kürze ihren Erbonkel umbringen werde – wäre die Polizei nicht verpflichtet, sie zu verhaften, um das Verbrechen zu verhindern? Und sie fordert zu Recht: Angesichts solcher ethischer Dilemmata müsse zumindest offen darüber diskutiert werden, ob die Verwendung solcher Techniken nicht beschränkt und bestimmte Formen von Datenfusionen gar verboten werden müssten.

Es gäbe im Blick auf den durch die technische Entwicklung gefährdeten Persönlichkeitsschutz noch andere Aspekte zu debattieren: Soll es den Unternehmen freigestellt sein, wie sie in ihren Produkten die Grundeinstellungen zum Schutz der Privatsphäre wählen wollen? Oder sollen marktmächtigen globalen Unternehmen zum Schutz der Privatsphäre nicht vielmehr Einschränkungen bei der Ausgestaltung ihrer allgemeinen Geschäftsbedingungen (AGB) auferlegt werden?

Das sei völlig aussichtslos, weil stets auch eingesetzt werde, was technisch möglich sei. Die User würden ihre Daten ja freiwillig zur Verfügung stellen, was solle also Ehrenrühriges daran sein? Und die Unternehmer würden nur machen, was die Konsumenten wünschten. Mit dieser Argumentation liesse sich freilich jedes Verbot lächerlich machen: von einfachen Verkehrsregeln über Kartellverbote bis hin zum Verbreitungsverbot von Atomwaffen. Darum ist sie nicht zielführend.

Eine Bürgerbewegung!

Eines ist bei alldem klar: Die beeindruckende technische Entwicklung schafft neben ihren grossen Vorzügen für Konsum und Vernetzung auch erhebliche Risiken für die Privatsphäre. Diese Kollateralschäden der technischen Revolution können wir nur in den Griff bekommen, wenn wir uns dieser Gefahren bewusst werden, eine Debatte darüber stattfindet und die verfassungsrechtlich geschützte Privatsphäre weiterhin als ein zentraler Wert eines freiheitlich demokratisch organisierten Staates anerkannt und gefordert wird. Wie soll das geschehen? Gerhart Baum, ehemaliger deutscher Innenminister, brachte es auf den Punkt: Es brauche eine kräftige Bürgerbewegung für die Verteidigung des Grundrechts auf Privatsphäre in der digitalen Revolution, in der wir uns gerade befänden, sagte er kürzlich in einem Referat in Zürich. Nur dann nehmen sich Politiker endlich dieses Themas an, das unser aller Leben fundamental verändern wird. ‹