MICHAEL SEEMANN

iRIGHTS media

DAS NEUE SPIEL

STRATEGIEN FÜR DIE WELT NACH DEM DIGITALEN KONTROLLVERLUST

Michael Seemann

Das Neue Spiel

Strategien für die Welt nach dem digitalen Kontrollverlust

Verlag iRights.Media

Oktober 2014

Teil I: Der Kontrollverlust

Kapitel 1 | Die drei Treiber des Kontrollverlusts

Ein Videobild, schwarz-weiß. Wir befinden uns in einem Hubschrauber und fliegen über eine Landschaft mit niedrigen Häusern. Sie wirkt hell, der Kontrast ist hart. In der Mitte des Bildes sehen wir ein Zielkreuz. Funksprüche durchbrechen das Hintergrundgeräusch von Rotoren. Eine Gruppe von Menschen läuft auf der Straße. Einer der Männer trägt einen Gegenstand über die Schulter gehängt. Die Soldaten identifizieren den Gegenstand als Waffe. „Free to engage“, ertönt es per Funk. Als das Schussfeld frei ist, feuert der Apache-Kampfhubschrauber mit seiner 30-Millimeter-Bordkanone in die Menge. Die Zeit zwischen dem Rucken des Maschinengewehrs und dem Einschlag der Kugeln beträgt ungefähr eine Sekunde. Die Menschen fallen oder werfen sich hin. Staub wirbelt auf. Die Apache-Besatzung schießt so lange, bis nur noch ein Verletzter zu sehen ist, der mühsam über den Bürgersteig kriecht. Ein Kleinbus hält an, Menschen versuchen, den Verletzten zu helfen. Wieder fragen die Soldaten die Erlaubnis zum Eingreifen an, wieder wird sie erteilt. Der Kleinbus wird zusammengeschossen.

An diesem Tag, dem 12. Juli 2007, sterben zwei Mitarbeiter der Nachrichtenagentur Reuters, Saeed Chmagh und Namir Noor-Eldeen. Was die Besatzung des Helikopters als Waffe interpretiert hatte, war Kamera-Equipment. Die irakische Familie, die ihnen zu Hilfe kam, starb ebenfalls; nur die Kinder überlebten das Massaker. Ein ganz normaler Tag in einem ganz normalen Krieg. Weil diesmal jedoch Journalisten betroffen waren, bestand Reuters auf einer Untersuchung. Die Redaktion fragte beim Militär das Videomaterial an, aber es wurde nie freigegeben, der Fall wurde nicht öffentlich aufgerollt. Bis zum 3. April 2010. „Collateral Murder“ [8] – unter diesem Titel wurde das Video schließlich veröffentlicht – war der Durchbruch für Wikileaks, jene Whistleblowing-Plattform, die die Welt im Jahr 2010 in Atem halten sollte. Collateral Murder war ein Schock für die amerikanische Bevölkerung und ein PR-Gau für das amerikanische Militär.

Die Kamera des Apache-Helikopters ist ein Kontrollinstrument: Die Befehlsketten beim Militär sind lang; bis eine Entscheidung getroffen ist, kann viel Zeit vergehen, oft zu viel Zeit. Mithilfe der neuesten Technik fliegt das Oberkommando in jedem Hubschrauber mit. Es sieht, was die Soldatinnen sehen, es hört, was die Soldaten reden. Und wenn sie nicht gehorchen, liegt gleich

Beweismaterial fürs Militärgericht vor. Im Fall „Collateral Murder“ handelten die Soldatinnen den Befehlen nicht zuwider. Dennoch wurde das Kontrollinstrument zum Zeugen der Anklage – vor dem Gericht der Weltöffentlichkeit. Die Medienanordnung wendet sich gegen ihre Kontrolleure.

Durch Wikileaks erlebten wir 2010, dass ein einzelner Whistleblower einer Supermacht wie der USA vor aller Welt die Hosen ausziehen kann. 2013 bestätigte Edward Snowden nicht nur, dass das möglich ist – wir erfuhren, dass auch wir selbst schon lange ohne Hosen dastehen. Die weltweiten Möglichkeiten zur Datensammlung, -verbreitung und -auswertung haben Dimensionen angenommen, mit denen wir nicht gerechnet haben. Wir haben die Kontrolle verloren. Egal, ob Regierung, Unternehmen, Institution oder Privatperson – alle sind betroffen. Überall leakt es, sickert es durch, wird kopiert und mitgeschnitten. Es: das Werk, der Brief, das Verhalten, die Dokumente, das Leben. Die Welt verwandelt sich in einen wachsenden Datenstrom, und der gerät außer Rand und Band.

Seit einigen Jahren stehen bei den Debatten um die digitale Revolution immer dieselben Themen im Mittelpunkt: das Urheberrecht, der Datenschutz, die Kommunikations- und Deutungshoheit von Journalistinnen, Unternehmen und Regierungen; seit 2010 vermehrt die Sicherheit von Staatsgeheimnissen. Und nun stellt sich heraus, dass wir alle von Geheimdiensten auf der ganzen Welt gescannt, dokumentiert und ausgewertet werden. Wir wissen das, weil ein einzelner Mensch unbemerkt so viele Dokumente aus den Informationsspeichern des US-amerikanischen Geheimdienstes NSA tragen konnte, wie es noch vor wenigen Jahren gar nicht möglich gewesen wäre – er hätte dafür mehrere Lastwagen gebraucht. Ratlos stehen wir vor den Snowden-Enthüllungen und diskutieren über unzureichende technische, politische oder soziale Lösungen.

In der Verunsicherung darüber, was mit unseren persönlichen Daten passiert, befinden wir uns in einem ähnlichen Stadium wie die Musikindustrie vor etwa 15 Jahren. Damals glaubten manche, mit technischen Kopierschutz-Systemen und Verschärfungen der Urheberrechtsgesetze dem ungehemmten Teilen und Tauschen von Daten Einhalt gebieten zu können. Kopierschutz sorgte dafür, dass Menschen ihre Musiksammlung vielleicht zu Hause, aber nicht im Auto oder beim Joggen hören konnten. Allerdings fanden findige Hacker auch immer wieder einen Weg, ihn zu knacken. Die Verschärfung des Urheberrechts ermöglichte horrende Massenabmahnungen, an denen Rechtsanwältinnen gut verdienten und die so manche

Familie an den Rand des Ruins drängten. Filesharing stoppen konnte sie nicht.

Für das Phänomen des Kontrollverlusts durch neue Medien lassen sich aber noch deutlich ältere Beispiele finden. Die Einführung des Buchdrucks – zunächst begrüßt, um das Wort Gottes in die Welt zu tragen – veränderte die Stellung der Kirche radikal. Während sie bis dahin die Datenflüsse regulierte, erfuhr sie durch die neue Technik einen enormen Kontrollverlust. Sie hatte nicht mehr die Autorität der reinen Lehre, alternative Glaubensmodelle konnten sich Bahn brechen. Schon damals war kein Kraut (oder Gebet) gegen die neue, unvorhersehbare Ausbreitung von Daten gewachsen, die nur noch selten im Sinne der Kirche war.

Der Kontrollverlust ist also keine Spezialität des Digitalen. Stattdessen liegt sein Kern in der spezifischen Struktur von Information selbst. Genauer: in der Irreversibilität der Mitteilung, die übertragen wird. Wir haben weder in der Kohlenstoff- noch in der digitalen Welt die Möglichkeit, Informationen wieder zurückzuholen. Oder mit Niklas Luhmann: „Wer schweigt, kann immer noch reden. Wer dagegen geredet hat, kann darüber nicht mehr schweigen.“ [9] Einmal in der Welt, sind Informationen nicht so einfach wieder herauszukriegen. Die meisten kennen wohl das peinliche Gefühl, nach einer durchfeierten Nacht etwas lieber wieder ungesagt machen zu wollen.

Doch nur, weil die Zahnpasta nicht zurück in die Tube geht, ist nicht jede ausgedrückte Tube ein Kontrollverlust. Kontrollverlust empfinden wir, wenn eine Erwartungshaltung enttäuscht wird: wenn die Annahme, wir seien im Besitz der Kontrolle, sich als Trugschluss herausstellt. Vielleicht war die Erwartung von Anfang an unrealistisch, vielleicht ist die Situation eskaliert. Der Grund ist erstmal nebensächlich. Entscheidend ist, dass die Erwartung enttäuscht wurde. Hier wirkt sich nun das Spezifische der Digitalisierung aus und verstärkt den Effekt. Sie verändert den Aggregatzustand von Information, macht sie allgegenwärtig, handhabbar und auswertbar. Die Zahnpasta spritzt immer schneller aus der Tube. Wir geraten in eine Situation, für die uns die Strategien fehlen.

Information und Kontrolle

Wir verwenden die Begriffe Daten, Informationen und Wissen im Kontext von Informationsökonomie und -gesellschaft in diesem Buch wie folgt.

Information ist der wesentlichste Begriff in dieser Gruppe. Der Philosoph

Gregory Bateson definiert sie genial einfach: „Information ist ein Unterschied, der einen Unterschied macht.“ [10] Das klingt erst einmal kryptisch, ist aber sehr schlüssig, gerade wenn die Definition mit den Begriffen „Daten“ und „Wissen“ verbunden wird.

Daten begreifen wir als den ersten Unterschied in dieser Definition. Daten sind Unterschiede. Sie sind alles, was sich mittels der Unterscheidung zwischen Null und Eins ausdrücken lässt. Das bedeutet, Informationen bestehen aus Daten, und wir können festhalten: Informationen sind Daten, die einen Unterschied machen. Doch wie und wo machen diese Daten einen Unterschied, wo finden wir Unterschied Nummer zwei? Systemtheoretiker sagen an dieser Stelle: im System – im psychischen oder sozialen System. Wir wollen den Systembegriff aber lieber ausklammern und sagen gleich „im Wissen“. Wissen ist für uns ein Netz aus Informationen. Wissen besteht aus Informationen, die mit anderen Informationen verknüpft sind. Mein Büro ist am Weichselplatz, der Weichselplatz ist in Neukölln und hat eine Wiese, auf einer Wiese wächst Gras, und so weiter.

Daten sind also Information, wenn sie im Wissen einen Unterschied machen. Und das sieht so aus: Eine Information knüpft sich an das Wissen an, sie wird Teil des Netzwerkes. Sie kann jedoch nur anknüpfen, wenn sie anschlussfähig ist. Wenn ich höre, dass Robin Williams gestorben ist, ihn aber nicht kenne, dann ist das zwar ein Datum (Singular von Daten), aber keine Information. Erst wenn ich weiß, dass Robin Williams ein berühmter Schauspieler war und ich vielleicht schon Filme mit ihm gesehen habe, dann wird das Datum seines Todes überhaupt zur Information.

Eine Information ist also immer nur eine Information im Zusammenhang mit einem bestimmten Wissen. Das Wissen von Menschen ist unterschiedlich. Was für den einen eine Information ist, ist für den anderen bloßes Datum. Daneben gibt es noch das gesammelte Weltwissen, das Wissen der Medizin, das Wissen der Rechtswissenschaft oder das Wissen der Wunderheilung. Wir verwenden den Begriff Wissen nicht im aufklärerischen Sinn – als gerechtfertigte, wahre Meinung –, sondern bezogen auf ein konkretes Netz aus Informationen – egal, ob diese der Wahrheit entsprechen. Wir implizieren, wenn wir von Informationen sprechen, dass es ein Wissen gibt, an das diese Information anschlussfähig ist, und zwar auch dann, wenn wir dieses Wissen nicht konkret benennen. Die Trias Daten, Information und Wissen lässt sich so zusammenfassen: Informationen sind Daten, die an ein Wissen anschlussfähig sind.

Betrachten wir auch den Begriff genauer, um den sich in diesem Buch alles dreht. Das Wort „Kontrolle“ kommt vom französischen contrôle, das sich zusammensetzt aus contre, „gegen“, und rôle, „Rolle“ oder „Register“. Ursprünglich bezeichnete es ein „Gegenregister zur Nachprüfung von Angaben eines Originalregisters“. Das heißt, bei jeder Kontrolle gibt es einen Ist- und einen Soll-Zustand. Kontrolle ist der stetige Versuch, beides anzugleichen.

Kontrolle ist der Eingriff in ein System mittels Erwartungswert und informationellem Feedback. Der digitale Kontrollverlust bezeichnet einen eigentümlich selbstreferenziellen Zustand. Er bedeutet nicht nur, dass die Ereignisse nicht mit dem Erwartungswert zusammentreffen, sondern dass die Erwartungswerte mithilfe von falschen Annahmen über die Welt gebildet wurden. Unsere Formeln für den Soll-Zustand sind hinfällig. Kontrollverlust bedeutet also nichts weniger, als dass wir nicht mehr wissen können, welche Erwartungen wir an die Zukunft haben können.

Die Folgen sind entsprechend dramatisch. Weil unsere Erwartungswerte nicht mehr stimmen, sind auch unsere Strategien für die Zukunft wertlos. Aktionen, die in der alten Welt funktioniert haben, verpuffen wirkungslos oder verschlimmern die Lage zusätzlich. Wir können zum Beispiel versuchen, eine missliebige Information aus dem Internet zu löschen. Doch wie wir sehen werden, geht es uns in diesem Fall wie dem mythischen Helden Herakles, wenn er versucht, einen Kopf der Hydra abzuschlagen und ihr sogleich zwei neue wachsen. Vor dem Kontrollverlust wird uns niemand retten; kein Meister kommt wie bei Goethes Zauberlehrling und schickt die Besen in die Ecke. Die Geister, die wir riefen, sind gekommen, um zu bleiben. Kurz: Wir sollten mit dem Kontrollverlust rechnen, ihn in unser Denken und Handeln – ja, in unsere Gesellschaft – integrieren. Vor allem müssen wir unsere Strategien an ihn anpassen. Wenn alle Dämme brechen, hilft nur noch schwimmen lernen.

Zukunftsforscherinnen bezeichnen die dominierenden Kräfte, die die gegenwärtigen Entwicklungen in der Welt bestimmen, als „Treiber“. Beim Kontrollverlust im Digitalen lassen sich drei solche Treiber identifizieren. Von Wikileaks über Napster bis zu den Snowden-Enthüllungen: Immer wieder sind dieselben Prinzipien zu erkennen, die die Phänomene des Digitalen kennzeichnen.

1. Die immer engere Verknüpfung der digitalen und analogen Welt, ermöglicht durch immer mehr und immer intelligentere Sensorik.
2. Die immer billigere Speicherung und schnellere Kopierbarkeit von Daten, die

durch beständig wachsende Kapazitäten von Leitungen und Datenträgern möglich ist.

3. Die sich ständig verbessernden und mit mehr Rechenkraft ausgestatteten Analysemethoden, die immer neue Einblicke in bereits existierende Datenbestände erlauben.

Kontrollverlustapparate

„Collateral Murder“, die zu Beginn erzählte Kollision von digitaler und analoger Welt in Bagdad, ist ein Beispiel für Treiber Nummer eins; ein Beispiel dafür, wie sich der Kontrollapparat in einen Kontrollverlustapparat verwandelt.

Im Sommer 2013, knapp sechs Jahre nach dem Luftangriff, von dem die Öffentlichkeit ohne Wikileaks nicht erfahren hätte, veröffentlichte der Guardian die erste Enthüllung aus den Dokumenten von Edward Snowden. Es war die Gerichtsanordnung des Geheimgerichtes FISC (Foreign Intelligence Surveillance Court) an Verizon, einen populären amerikanischen Mobilfunkprovider. Verizon wird darin aufgefordert, der NSA alle Verbindungsdaten seiner Kunden zugänglich zu machen. Verbindungsdaten sind eine Form von Metadaten – zum Beispiel die Zeiten, zu denen telefoniert wurde; die Nummern beider Gesprächteilnehmerinnen; die Dauer des Anrufs; wann sich welches Gerät mit dem Internet verbunden hat; welche Websites besucht wurden.

Wenn der Geheimdienst früher jemanden beschatten wollte, schickte er ihm einen Agenten mit Schlapphut und Trenchcoat hinterher, um ihm „unauffällig“ zu folgen. Das ist nicht mehr nötig. Mein Mobilfunkprovider ist immer genau informiert, wo ich mich gerade befinde, damit seine Funktürme wissen, wie sie mein Handy zum Klingeln bringen können.

Es zählt nicht zum Allgemeinwissen, dass wir – sofern wir ein Handy benutzen – eine Ortungswanze mit uns führen, die jederzeit meldet, wo wir uns gerade befinden. Wir tragen sie mit uns herum, damit wir erreichbar sind für Freunde, Familie und Arbeitgeber. Damit die Dinge nicht außer Kontrolle geraten, daheim oder auf der Arbeit. Wir haben Smartphones dabei, um schnell mal etwas nachzuschlagen, eine E-Mail zu schreiben oder etwas fotografieren zu können. Die NSA und andere staatliche Dienste machen sich das zunutze. Sie wenden die Technik, die uns in unserem Leben unterstützen und erweitern soll, gegen uns. Auf die Art ist der Kontrollverlust in jeder

Medienapparatur als Möglichkeit eingebaut. Wir alle besitzen Kontrollverlustapparate.

Und die Kontrollverlustapparaturen befinden sich nicht nur in unseren Hosentaschen. Wenn wir über die Straße gehen, registrieren uns die allgegenwärtigen Überwachungskameras (CCTV), wenn wir zu Hause sind, registriert der intelligente Stromzähler, wie lange wir das Licht anhaben und ob wir nachts den Kühlschrank öffnen. In Zukunft werden smarte Thermostate auf unsere Anwesenheit reagieren, und selbstverständlich sind sie mit dem Internet verbunden; schließlich wollen wir sie von unserem Smartphone aus steuern. Nie war es leichter, Energie zu sparen – nie war es einfacher, die Lebensgewohnheiten von Menschen zu überwachen.

Die Überwachung unserer privatesten Räume hört damit noch nicht auf. Microsofts Spielkonsole XBox One kommt mit der sogenannten Kinect-Technologie. Kinect (von engl. kinetic, „kinetisch“ und connect, „verbinden“) ist ein Zusatzgerät, das es ermöglichen soll, mit der Spielkonsole durch komplexe Gesten im Raum zu interagieren. So sollen sich Spiele unmittelbarer als bisher steuern lassen. Mit Infrarotsensoren und mehreren Kameras ausgestattet, ist es fähig zu Überwachung in bisher unbekanntem Ausmaß. Kinect „sieht“ eine 3D-Repräsentation des Raumes und registriert in Echtzeit die Bewegungen aller Menschen darin. Kinect kann verschiedene Individuen auseinanderhalten, sieht, ob sie lachen oder angestrengt gucken, misst die Körpertemperatur und kann sogar den Puls anhand der Veränderungen der Hautpigmente ablesen. Was für eine großartige Technologie – was für ein Überwachungsalptraum!

Und das ist nur der Anfang. Zukunftsforscher sind sich einig, dass uns nur noch wenige Jahre von einem Alltag trennen, in dem selbstfahrende Autos selbstverständlich sind. Nur mit enorm vielen Daten – bereitgestellt über viele Kameras und Abstandssensoren an allen Seiten des Autos – ist es denkbar, dass Fahrzeuge sich autonom durch den Verkehr bewegen können. Das selbstfahrende Auto wird die motorisierte Mobilität revolutionieren. Ein Auto zu besitzen, wird nur noch für sehr wenige Menschen sinnvoll sein, wenn per Smartphone jederzeit eines spontan und flexibel zu einem gerufen werden kann. Selbstfahrende Autos werden eine wichtige Rolle spielen bei der Eindämmung des Klimawandels und unsere Straßen von vielen Millionen Kubikmetern parkenden Blechs befreien – alles ohne Einbußen an individueller Mobilität. Aber eben mithilfe einer allumfassenden Überwachung.

Die Überwachung des öffentlichen Raums wird eine neue Dimension erreichen,

wenn Flugdrohnen nicht mehr nur eine Spielerei für Nerds sind, sondern echte Aufgaben erledigen. Drohnen können eingesetzt werden, um Häuser zu bauen oder den Verkehr zu steuern. Sie werden schon heute zur Sicherung von Grundstücken und Gebäuden verwendet oder von der Polizei, um Demonstrationen zu überwachen. Es ist absehbar, dass in wenigen Jahren ein ständiger Schwarm von Fluggeräten mit Kameras und Sensoren ausgestattet über unseren Köpfen schwirren und die gesamte Umwelt aufzeichnen wird – nicht einmal als Hauptaufgabe, mehr so nebenbei. Und wahrscheinlich werden wir sie kaum sehen oder hören, denn der Trend zur Miniaturisierung setzt sich fort. Die Welt wird wie von Zauberhand funktionieren – und uns beobachten.

Wir selbst werden dabei Teil der Überwachungsmaschinerie. Wenn es nach Google geht, wird schon dieses Jahr das erste Smartphone auf den Markt kommen, das auf dem Kopf getragen wird. Mit Google Glass, einer intelligenten Brille mit Minidisplay im Sichtbereich und einer vorn angebrachten Kamera, wird es möglich sein, ständig den eigenen Blick auf die Welt zu dokumentieren und ihn, falls gewünscht, direkt ins Internet zu streamen. Eine einzelne Person, die in einer Großstadt unterwegs ist und ihre Erlebnisse streamt, lässt das „Recht am eigenen Bild“ für Millionen andere zur Makulatur werden.

„Internet of Things“ oder Ubiquitous Computing (etwa „Allgegenwärtige Computer“) wird dieser Trend gerne genannt. Egal, ob auf der Straße, im Auto, im Wohnzimmer oder in der Kleidung – intelligente Sensoren dringen immer weiter in unsere Welt ein. Sie sind sich ihrer Umwelt zunehmend “bewusst“, und natürlich sind sie online. Alles wird Teil des Internets. Zu glauben, dass bei der Verdatung der Welt die Menschen eine Ausnahme bilden werden, wäre naiv.

Die Flucht des John McAfee

Selbst Experten trifft diese Erkenntnis oft unvermittelt. John McAfee ist bekannt als IT-Sicherheitsexperte und Lebemann. Nach einer kurzen Karriere beim amerikanischen Rüstungshersteller Lockheed gründete er die erste Firma zum automatischen Aufspüren und Unschädlichmachen von Computerviren. Er ist der Erfinder der Antivirensoftware, die immer noch seinen Namen trägt, obwohl er die Firma bereits in den 1990er-Jahren verkaufte. Bis heute ist er sehr reich und – um es vorsichtig zu sagen – exzentrisch. Er wohnt im südamerikanischen Inselstaat Belize,

und sein Mitteilungsbedürfnis ist groß. In seinem Blog schreibt er über Drogen, Ausschweifungen, Sex und seine Paranoia. Diese Paranoia war es auch, die McAfee zur Flucht trieb. Im November 2012 wurde sein Nachbar Gregory Faull tot aufgefunden, die Behörden ermittelten in alle Richtungen. Auch McAfee geriet ins Visier. In einer Nacht-und-Nebelaktion tauchte er mithilfe eines Doubles sowie eines gefälschten nordkoreanischen Reisepasses unter.

Wochenlang blieb McAfee verschollen, veröffentlichte aber Blogposts und kommunizierte über seine Kontakte mit der Öffentlichkeit. Irgendwann willigte er ein, sich mit zwei Journalisten des Lifestylemagazins VICE zu treffen. Sie verbrachten vier gemeinsame Tage, und McAfee gab bereitwillig Interviews. Als VICE am 3. Dezember das Interview auf seiner Website ankündigte – die Journalisten waren noch bei McAfee vor Ort –, veröffentlichte das Magazin zum Beweis ein Foto, das McAfee zusammen mit den Journalisten zeigt. [11]

Allerdings hatte die Redaktion dabei vergessen, die EXIF-Daten zu löschen. Das so genannte EXIF-Metadatenformat kann mit so gut wie jeder Bildbearbeitungssoftware ausgelesen werden. Wenn wir ein digitales Bild auf einem Rechner öffnen, wird ein Füllhorn an Daten sichtbar, die moderne Kameras in jedem Foto mitspeichern. Dazu gehören die Hersteller- und Produktinformationen der Kamera selbst, die Uhrzeit und das Datum der Aufnahme, die Belichtungs-, Brennweite- und Blendeneinstellungen und – sofern es sich um ein GPS-fähiges Gerät handelt und die Ortung aktiviert ist – der Ort der Aufnahme. Im diesem Fall war das Gerät ein iPhone 4, das über eine metergenaue Positionsbestimmung verfügt, und so fand sich in den EXIF-Daten die genaue Position von McAfee. Auf einen Schlag wusste die ganze Welt, dass John McAfee in Guatemala war. Seine Flucht war beendet.

Wir haben nicht mehr im Blick, wann welche Daten abgespeichert werden. Welcher Sensor ist wann aktiv, was speichert er und wohin? Die Signalempfänger sind überall: Kameras, GPS-Sensoren, Thermometer, Mikrofone, Bewegungsmelder und Infrarotsensoren. Sie sind die vielfältigen Schnittstellen, die unsere reale Welt mit der Welt der Daten verschmelzen. Wenn selbst Computerexperten wie John McAfee den Überblick verlieren, und wenn das amerikanische Militär wie bei „Collateral Murder“ über seinen eigenen Überwachungsapparat stolpert – wie sollen dann normale Menschen ein Bewusstsein dafür entwickeln, wann sie wie in welcher Öffentlichkeit stehen? Wie sollen wir die Kontrolle darüber behalten, welche Daten

wann in welchen Kontext geraten, wenn die Dinge um uns herum immer intelligenter werden, Augen und Ohren bekommen und selbige immer kleiner, unsichtbarer und allgegenwärtiger werden?

Das amerikanische Militär wird die Kameras nicht aus seinen Apache-Hubschraubern entfernen, und auch wir sind nicht bereit, auf die Ortsbestimmung in unseren Smartphones zu verzichten. Wir sind abhängig von unseren Kontrollverlustapparaten, weil ihre Vorteile so viel offensichtlicher sind als die Probleme, die sie verursachen.

Die Ausbreitung digitaler Sensorik in der Welt ist der erste Treiber des Kontrollverlusts. Es gibt kein analoges Leben mehr im Digitalen. Wer Teil der Welt ist, wird Teil des Internets sein.

Barbra Streisands Haus im Zeitalter der digitalen Kopierbarkeit

Während die Sensorik die Welt in allen Einzelheiten durchdringt, stellt sich immer drängender die Frage, was mit diesen Datenmassen alles passiert. Die wachsenden Datenspeicher und Datenleitungen erlauben das immer billigere und schnellere Kopieren auch größter Datenmassen. Das ist der zweite Treiber des Kontrollverlusts.

Das Drama der Kopierbarkeit begann bereits vor der Digitalisierung der Welt. „United States – Vietnam Relations, 1945–1967: A Study Prepared by the Department of Defense“ lautet der sperrige Titel einer historischen Studie, die das Pentagon zusammen mit mit dem militärnahen Thinktank RAND Corporation ab 1967 anfertigte. So sperrig wie der Titel ist auch der Inhalt. Es handelt sich um über 4.000 Original-Dokumente, dazu Einschätzungen und Studien von vielen anonymen Autoren – versammelt auf insgesamt 3.000 Seiten. Die Studie sollte den genauen Verlauf des Vietnamkrieges dokumentieren, damit künftige Regierungen aus den Fehlern und Erfolgen lernen können. Die Studie war top secret, weswegen von dem 47 Bände starken Werk nur 15 Kopien angefertigt wurden. Jedenfalls dachte man das.

In Wirklichkeit waren es 17. Daniel Ellsberg, ein Mitarbeiter der RAND Corporation, hatte nicht nur Zugang zu diesen Bänden, sondern auch zu einer völlig neuartigen Technologie: dem Fotokopierer, der erst in den 1960er-Jahren von Xerox auf den Markt gebracht wurde. [12] Und Ellsberg war wütend – auf die Politik, auf das sinnlose Töten in Vietnam. Wochenlang nahm er jeweils einen der Bände mit nach Hause und fotokopierte zusammen mit seinem Sohn Seite für Seite. Am Ende dieses

langwierigen Prozesses hatte er alle 47 Bände jeweils zwei mal kopiert – eine Kopie landete schließlich bei der New York Times. Die „Pentagon Papers“, wie sie heute heißen, gingen als einer der spektakulärsten Leaks in die Geschichte ein und trugen zur Beendigung des Vietnamkriegs bei.

Vor den 76.911 Afghanistan-Papieren, den 391.832 Dokumenten zum Irakkrieg und den 251.287 diplomatischen Depeschen, die Chelsea Manning (damals noch Bradley Manning) 2010 auf der Whistleblower-Plattform Wikileaks veröffentlichte, hätte Daniel Ellsbergs Fotokopierer kapituliert. Genau genommen hätte er diese Masse an Dokumenten ohne eine LKW-Kolonne nicht mal aus dem Haus bekommen. Manning hingegen brannte eine DVD und schrieb zur Tarnung „Lady Gaga“ drauf.

Kopiermaschinen

In der Welt des Digitalen gibt es keinen Unterschied zwischen Speichern, Verschicken und Kopieren. Ein Browser kopiert erst einmal alle Dateien auf den Rechner, um sie anzuzeigen. Eine E-Mail wird vom Computer des Senders auf einen Server und von dort auf einen Verbund von Servern kopiert, bevor sie bei der Empfängerin – als Kopie – ankommt. Das Internet – dieser gewaltige Verbund von vernetzten Computern – ist eine riesige Kopiermaschine. Hinter jedem Klick, jedem Anschauen eines Youtube-Videos, jedem Facebook-Eintrag steckt in Wirklichkeit eine ganze Kaskade von Kopier-Operationen.

In der analogen Welt musste einiger Aufwand betrieben werden, um eine Information an ihre Empfänger zu senden. Mehr als hundert Leute zu erreichen war nur unter großem Ressourceneinsatz machbar. Heute ist ähnlicher Aufwand nötig, um dieselbe Information nicht sofort weltweit zugänglich zu machen. Doch wir denken immer noch in analogen Kategorien und erschrecken, wenn wir merken, dass die Welt längst ganz anders funktioniert. Lange haben wir beispielsweise gedacht, dass, wenn wir eine E-Mail schreiben, nur die Empfängerin sie liest. Edward Snowden belehrte uns eines Besseren.

Prism, die zweite große Snowden-Enthüllung, betraf die großen Digitalkonzerne: Google, Facebook, Microsoft und Apple. Auf fast unleserlichen hässlichen Powerpoint-Folien ist dokumentiert, wie die NSA direkt auf die Daten dieser Firmen zugreifen kann. Ebenfalls kam heraus, dass der britische Geheimdienst GCHQ in die privaten Datennetze von Google, Yahoo und anderen Anbietern eingedrungen ist, um

den internen Datenverkehr innerhalb der unzähligen Rechencenter der Konzerne mitzuschreiben. Die Cloud – eines der wichtigsten Schlagworte in der Technologiebranche der letzten Jahre – wurde von der NSA „geownt“ (was im Hackerjargon bedeutet, dass ein System von einem Angreifer kontrolliert wird). Cloud Computing bezeichnet den Trend, Computerisierung und Datenhaltung mehr und mehr auf zentrale Hochleistungs-Server im Internet zu verlagern. Immer wenn wir unsere E-Mails auf der Website von Google Mail lesen und bearbeiten, wenn wir Dateien auf Dropbox speichern, die Daten unseres iPhones in der iCloud sichern oder schlicht und ergreifend Facebook nutzen, sind wir Nutzer von Cloud Computing. Unsere Daten sind dann nicht einfach auf unserem Rechner gespeichert, sondern irgendwo da draußen in der Internetwolke.

Natürlich gibt es für diese Wolke (engl. cloud) in Wirklichkeit einen physischen Ort. In Utah hat die NSA gerade ein neues Rechenzentrum gebaut. Auf 100.000 Quadratmetern sollen schätzungsweise fünf Zetabyte (circa fünf Milliarden 1-Terabyte-Festplatten) an Daten gespeichert und verarbeitet werden. Umgerechnet auf die Weltbevölkerung sind das 700 Gigabyte pro Person. Das britische Pendant des GCHQ sitzt in England an der entscheidenden Stelle der Seekabelverbindung zwischen Europa und den USA und speichert alle durchgehenden Daten bis zu dreißig Tage ab, um sie nach verdächtigen Inhalten zu durchsuchen. Dieses sogenannte Tempora-Programm beschäftigt 500 Mitarbeiterinnen, die mehr als 200 Glasfaserleitungen überwachen. Wenn wir bei Google etwas suchen, bei Facebook etwas liken oder eine E-Mail von einem Yahoo-Nutzer bekommen, landen die Daten auch auf britischen Festplatten.

Nicht die Geheimdienste und ihre Handlungen haben sich verändert, sondern „nur“ ihre Mittel. Geheimdienste sollen Informationen beschaffen. Das taten sie zu allen Zeiten und schon immer mit allen verfügbaren Mitteln. Vor dreißig Jahren waren diese Mittel angezapfte Telefonleitungen und Tonbandgeräte. Heute sind es Glasfaserkabel und Rechenzentren. Die Reichweite der Geheimdienste wuchs mit ihren Möglichkeiten. Wir haben James-Bond-Filme geschaut und die Thriller von John le Carré gelesen, aber wir nehmen die Welt der Spionage wahr als eine, die uns völlig fremd, von uns getrennt ist.

Wir wissen: Militärs, Staatschefinnen, Diplomaten und Terroristinnen geraten regelmäßig ins Visier geheimdienstlicher Überwachung. Doch mit den neuen Technologien ist diese Welt bis in die unsere herunter gewachsen. Die Dienste

zeichnen all unsere Worte und Handlungen auf. Mit den Möglichkeiten, die NSA und GCHQ zur Verfügung stehen, hat sich das abstrakte Szenario des Kontrollverlusts über die persönlichen Daten in der Realität manifestiert. Die überbordende Echtzeitüberwachung eines Großteils der Weltbevölkerung ist Wirklichkeit geworden, weil es geht. Der Politikberater Andrew B. Denison sagte es in der Polit-Talkshow „Anne Will“ ganz unverblümt: Geheimdienste seien dafür da, die Gesetze anderer Staaten zu übertreten. Nur steht ihnen dafür heute eine ganz anderes Instrumentarium zur Verfügung als früher. Sie reiten auf der Welle des Kontrollverlusts wie ein Surfer und nutzen geschickt die Möglichkeiten, die er ihnen bietet.

Der Streisand-Effekt

Nicht nur die Geheimdienste wurden durch die neuen Technologien gestärkt. Auch für unseren eigenen Umgang mit Daten eröffneten sich ganz neue Möglichkeiten. Kenneth Adelman dachte sich nichts Böses, als er 2002 mit seinem „California Coastal Records Project“ begann. Sein Ziel war der Aufbau einer Bilddatenbank über die kalifornische Küste. 12.000 Fotos hatte er bereits beisammen, als er 2003 von der Schauspielerin Barbra Streisand verklagt wurde – auf 50 Millionen Dollar Schadensersatz, weil sie durch das Projekt ihre Privatsphäre verletzt sah. Gegenstand des Anstoßes war ein Foto, auf dem auch die pompöse Villa des Hollywoodstars an der Küste von Malibu zu sehen war. Als der Prozess öffentlich wurde, fand er ein gewaltiges Echo im Netz. Internetnutzer in aller Welt machten sich über den Versuch der Künstlerin lustig, sich selbst aus dem Internet zu streichen. Das Foto mit ihrer Villa, für das sich bislang niemand interessiert hatte, wurde auf Tausenden von Websites und Blogs veröffentlicht und kommentiert. Die Villa selbst wurde rot markiert und mit dem Hinweis versehen, dass es sich hier um die Villa von Barbra Streisand handle.

Nicht nur den Prozess hat Barbra Streisand verloren. Auch ihre eigentliche Intention – die Wiederherstellung von Privatsphäre für Haus und Hof – hat sie mit dem Prozess selbst konterkariert. Ihr Handeln und die Reaktion im Netz prägten einen eigenen Begriff: Immer, wenn jemand versucht, eine unerwünschte Information aus dem Internet zu entfernen, wird der „Streisand-Effekt“ herausgefordert. Das Ganze kann gutgehen, aber viele hundert Beispiele des Streisand-Effekts gemahnen an die

bittere Wahrheit: Einmal im Netz, lassen sich Informationen kaum mehr wieder aktiv entfernen.

Mit bis dahin ungekannter Wucht schlug der Streisand-Effekt zu, als die US-Regierung 2010 versuchte, gegen Wikileaks vorzugehen, und zu jedem Mittel griff, das ihr einfiel. Unter anderem setzte sie Zahlungsanbieter wie Paypal und American Express unter Druck, Wikileaks den Geldhahn zuzudrehen. Auch der Domain-Anbieter von Wikileaks, EveryDNS, stellte auf entsprechenden Druck die Zusammenarbeit ein. Die Website war unter der Domain www.Wikileaks.org auf einmal nicht mehr zu erreichen. Innerhalb von zwei Tagen sprossen daraufhin 750 „Mirrors“, komplette Kopien aller Daten des Wikileaks-Servers, auf anderen, ans Netz angebundenen Rechnern. Wenige Wochen später waren es bereits 1.426.

Die Wege der Daten sind unergründlich. Einmal digitalisiert, rinnen sie durch alle Ritzen und Öffnungen, immer schneller und immer mehr. Und das Leck scheint größer zu werden, je kopierbarer die Daten werden. Der zweite Treiber des Kontrollverlusts lässt uns die Kontrolle darüber verlieren, wer wann auf welche Daten Zugriff hat und wen wir davon ausschließen können.

Die verknüpften Daten und der General

Immer mehr Daten entstehen, werden gesammelt und aufgezeichnet, und ihre Wege werden immer unkontrollierbarer. Aber erst ihre intelligente Verknüpfung macht Wissen daraus und erzeugt damit die eigentliche Wucht des Kontrollverlusts. Neue Techniken der Analyse, Verknüpfung und Korrelation großer Datenmengen bescheren Erkenntnisse, die nicht darin zu vermuten waren. Das ist der dritte Treiber, und er sorgt für den endgültigen Verlust der Kontrolle: Wir können nicht einmal mehr wissen, wie groß das Aussagepotenzial von Daten ist.

In seinem Buch „Wikileaks. Inside Julian Assange’s War on Secrecy“ beschreibt der britische Journalist David Leigh die monatelange Arbeit an den Wikileaks-Enthüllungen. Assange hatte es geschafft, eine internationale Phalanx von Zeitungen und Nachrichtenmagazinen vom britischen Guardian über den SPIEGEL bis zur New York Times und der Washington Post dafür zusammenzutrommeln. Die Redaktionen entdeckten Skandale, entfernten sensible Daten aus den Dokumenten, entwarfen Schautafeln und Infografiken und verarbeiteten das Material zu Geschichten. Diese sorgfältige Aufbereitung war wichtig, denn in den Originaldokumenten fanden sich

Namen von Oppositionellen in diktatorischen Regimen und von inoffiziellen Informantinnen der amerikanischen Streitkräfte in den Krisenregionen sowie Daten und Fakten, die die nationale Sicherheit bestimmter Staaten in Gefahr hätten bringen können. Auf den Journalisten lastete eine entsprechend hohe Verantwortung.

Von all dem berichtet Leigh in seinem Buch, und auch davon, wie er selbst an die Dokumente kam. Auf dem Wikileaks-Server gab es ein verstecktes Verzeichnis. In diesem Verzeichnis befand sich eine mehrere Gigabyte große, stark verschlüsselte Datei. Die Datei enthielt die gesamten unredigierten Dokumente, noch in dem Zustand, wie Wikileaks sie von Manning bekommen hatte. Bei seinem Treffen mit Leigh gab Julian Assange ihm den Link zu der versteckten Datei auf dem Wikileaks-Server sowie das Passwort zu ihrer Entschlüsselung.

Als Leighs Buch 2011 herauskam, muss Julian Assange ein wenig geschwitzt haben an der Stelle, wo es um dieses Treffen geht. Leigh beschreibt dort nicht nur die Anekdote selbst in allen Einzelheiten. Unter der Kapitelüberschrift steht außerdem: „ACollectionOfDiplomaticHistorySince_1966_ToThe_PresentDay#“. Es ist das Original-Passwort zu der verschlüsselten Datei, das Assange ihm gegeben hat. Leigh wird später sagen, dass er sich dabei nichts Böses gedacht habe und nicht glaubte, dass das Passwort noch gültig sei, wenn das Buch erscheinen würde. Vielleicht dachte auch Assange noch für einen kurzen Moment daran, schnell das Passwort der Datei zu ändern, bevor sie jemand fände. Doch dann werden ihm die 1.426 Mirrors des Wikileaks-Servers eingefallen sein. Auf 1.426 anderen Servern lagen zu dem Zeitpunkt exakte Kopien der Datei, die weiterhin mit dem Passwort zu entschlüsseln waren, das in einem Buch abgedruckt war, das es in jedem Buchladen zu kaufen gab. Es dauerte nicht lange, bis Hackerinnen die Datei entdeckt und das Passwort ausprobiert hatten. Die gesamte Weltöffentlichkeit hatte damit auf einen Schlag Zugriff auf die ungefilterten, unzensierten und unbearbeiteten Manning-Dokumente.

Der Fall zeigt, wie Daten ihre Brisanz erst in der Verknüpfung mit anderen Daten entfalten: Die Veröffentlichung des Passworts in dem Buch war allein noch kein großer Schaden, es hätte rechtzeitig geändert werden können. Die verschlüsselte Datei, auch auf den vielen Wikileaks-Spiegelungen, hätte alleine niemandem weh getan – niemand konnte sie ohne Passwort lesen. Erst die Kombination aus der vervielfältigten Datei und dem publizierten Passwort machte den Unterschied. Beides für sich genommen hatte überschaubare Auswirkungen, in Kombination bedeutete es den Totalverlust der Kontrolle über die Manning-Dokumente. An dem Beispiel wird

deutlich, wie schwer es ist, die von einem Datum ausgehende Gefahr zu beurteilen.

Die verknüpften Daten der NSA

Auch die NSA sammelt nicht nur Daten, sondern befragt sie, mit ihren eigenen Analysetechnologien. Eines der Programme, von denen wir durch Edward Snowden erfahren haben, ist XKeyscore. Oberflächlich betrachtet wirkt es erst mal wie eine einfache, nicht besonders schön gestaltete Website; ein Formular zum Eintragen von verschiedenen Suchbegriffen und Suchparametern, dem wir bei einer Begegnung in der freien Wildbahn des Internets eher zögerlich sensible Daten anvertrauen würden.

Doch dahinter steckt die gesammelte Datenkraft der NSA und ihrer Partner. Alle Daten, die die NSA mit ihren Programmen und Partnerprogrammen sammelt, werden hier aufbereitet und zusammengeführt und können von diesem Interface aus abgefragt werden. Metadaten aller Kommunikationen – wer mit wem gechattet, telefoniert,oder gemailt hat – werden kombiniert mit den Inhalten aus den Chats und dem Mailverkehr. Alle Ergebnisse dieser Auswertung werden wiederum mit Registrierungs- und Adressdaten, Rechnungsdaten und anderen Identifikationsmerkmalen angereichert und verknüpft. Heraus kommen detaillierte, automatisch zusammengestellte Dossiers über jeden einzelnen Menschen – weltweit. Identifizieren lassen sich die Personen per Name, E-Mail-Adresse, Geräteadressen oder Browsersignatur.

Eine Browsersignatur ist etwas unbekannter als die IP-Adresse eines Rechners, gehört aber zum Internetalltag. Es handelt sich dabei selbst um ein Datum aus verknüpften Daten: Jeder Browser schickt standardmäßig Informationen zu Browsertyp, Browserversion, Betriebssystem und -version, Bildschirmauflösung und andere Daten an jede aufgerufene Website. In Summe, als verknüpftes Muster, verrät das, wer eine Seite besucht hat. Jede einzelne Information für sich ist harmlos. In der Zusammenführung ergibt sie ein Muster, das eindeutige Identifizierung ermöglicht, wie bei einem Fingerabdruck.

XKeyscore arbeitet mit dieser Verknüpfbarkeit von Daten. Das Programm verwandelt die riesigen Datenschätze, die die NSA zusammenträgt, aus totem gespeichertem Wissen in auswertbares Material; ähnlich wie wir es von Google kennen, nur mit mehr und präziseren Möglichkeiten. Die Suchen darin lassen sich beliebig einschränken und filtern, zum Beispiel nach bestimmten Schlagwörtern, Geschlecht, Uhrzeit und Ort der Kommunikation, hinsichtlich der verwendeten

Sprache, ob Verschlüsselung eingesetzt wird oder nicht. Komplexe Abfragen wie „Zeige mir alle verschlüsselten Word-Dokumente in Iran“ können ohne weiteres generiert werden – oder auch „Gib mir alle Google-Suchanfragen der letzten 10 Tage nach ‚Islam‘ samt IP-Adresse, Sprache und verwendetem Browser in Deutschland und suche mir die Profile der betreffenden Nutzerinnen zusammen.“

Mit jedem zusätzlichen Datensatz wird einem anderen Datensatz neues Leben eingehaucht. Mit jeder Korrelation entstehen neue Such-Möglichkeiten, mit jeder Abfrage potenzielle neue Aussagen.

Big Data und das Ende der Anonymität

Das in der Debatte um die Digitalisierung herumgeisternde Schlagwort „Big Data“ bezeichnet im Grunde genau das beschriebene Prinzip: Erkenntnisgewinne durch die statistische Befragung großer Datenmengen. Empirische Forschung arbeitete bis vor kurzem ausschließlich mit kleinen, selbst zusammengesuchten Datenmengen, etwa aus der aufwendigen Befragung von circa tausend Leuten, um daraus ein repräsentatives Ergebnis abzuleiten. Seit einigen Jahren steht nun aber eine ganze Menge Daten zur Verfügung, die nicht aufwendig gesammelt werden müssen, sondern einfach „anfallen“; etwa die Verbindungsdaten von Handys, die Klickgewohnheiten auf Websites, die Angaben auf Facebook-Profilen oder die Bewegungsdaten von Menschen.

Chris Anderson, Herausgeber der Zeitschrift Wired, brachte Big Data einmal auf die Formel, es sei das „Ende der Theorie“ [13] – in Zukunft brauche niemand mehr eine Hypothese aufzustellen, stattdessen könne man die riesigen Datenmassen einfach direkt befragen. Das ist übertrieben. Dennoch verändert sich durch die Verfügbarkeit großer Datenmassen das wissenschaftliche Vorgehen. Daten können in einer Art Brainstormingphase korreliert und ausgehend davon statistische Auffälligkeiten genauer unter die Lupe genommen werden. Dafür gibt es inzwischen jede Menge Beispiele.

Seinen Übersetzungsdienst „Translate“ hat das Unternehmen Google ohne große Kenntnis über Syntax und Grammatik so unterschiedlicher Sprachen wie Chinesisch und Arabisch entwickelt. Stattdessen konzentrierten sich die Google-Ingenieure auf die Suche nach genügend Texten, die in viele verschiedene Zielsprachen übersetzt worden sind. Aus diesem Rohmaterial „lernte“ Google Translate. Das funktioniert

ausgehend von zehn oder hundert Texten nicht, aber bei einer Million Texten schon recht gut. Nach dem gleichen Prinzip erkennt Google auch, wie sich Grippeepidemien verbreiten. Die Kombination der entsprechenden Suchworte (zum Beispiel bestimmte Medikamente) mit dem Ort ihrer Abfrage erlaubt es, auf einer Landkarte in Echtzeit zu verfolgen, wohin die Grippe wandert.

Der Navigationsgeräte-Hersteller TomTom erkennt in Zusammenarbeit mit dem Mobilfunkprovider Vodafone Staus. Verändern sich die Standortdaten vieler Handys auf Autobahnen über einen längeren Zeitraum nur noch wenig, ist das ein sicheres Zeichen für zäh fließenden Verkehr. Per Mobilfunk kann das Navigationssystem dann „Stau“ auf den Geräten der TomTom-Kunden melden. TomTom versichert den Datenschützerinnen, dass die ausgewerteten Mobilfunkdaten für die Analyse natürlich anonymisiert werden. Das heißt, es werden keine Namen oder Telefonnummern in den Datensätzen verwendet. Doch wie anonym können Daten heute überhaupt sein?

Unter Wissenschaftlern ist Deanonymisierung inzwischen sowas wie eine Art Big-Data-Sport geworden. Am MIT in Cambridge extrahierten sie aus anonymisierten Mobilfunk-Zellendaten (ähnlich denen, mit denen TomTom arbeitet) nicht nur genaue Bewegungsprofile der einzelnen Handybesitzerinnen, sondern fanden heraus, dass lediglich vier Datenpunkte nötig waren, um diese mit 95-prozentiger Genauigkeit zu identifizieren. [14] Solche Datenpunkte können zum Beispiel Ortsdaten sein, wie Check-in-Daten auf Diensten wie Foursquare oder Facebook oder die Geo-Koordinaten in Fotos oder Tweets.

Die deanonymisierte Affäre

Vor der deanonymisierenden Macht verknüpfter Daten sind selbst Chefs von Geheimdiensten nicht sicher. General David Petraeus ist ein Mann, der sein Leben im Griff hat. Verheiratet, Kinder und erfolgreich im Job. Ein Mustersoldat: Seit 37 Jahren beim amerikanischen Militär, Vier-Sterne-General, ehemaliger Kommandeur der amerikanischen Streitkräfte – erst im Irak, dann in Afghanistan, dann, nach dieser beispielhaften Karriere, freiwillig in den Ruhestand gegangen. Barack Obama persönlich hat ihn reaktiviert und auf den Chefsessel der CIA gesetzt.

Auch in Paula Broadwells Leben verläuft offensichtlich alles nach Plan. Sie hat selbst eine militärische Karriere hinter sich, unter anderem in einer Spezialeinheit. Sie ist verheiratet und gilt als *hockey mum*, als außerordentlich engagierte Mutter, die

ihre Kinder jeden Morgen persönlich zum Schulbus bringt. Nebenher engagiert sie sich ehrenamtlich für Kriegsveteranen. Eine amerikanische Vorzeige-Superfrau. Paula Broadwells Interesse an Petraeus war zunächst ein journalistisches: „Der Mustersoldat“ war der Arbeitstitel der Biografie, die sie über ihn schreiben wollte. Jahrelang begleitete sie ihn; auch in den Irak und nach Afghanistan, überall war sie mit dabei. Die Öffentlichkeit bekam nichts davon mit, dass sich die beiden auch abseits des Beruflichen näherkamen.

Eine Affäre mit einem amtierenden CIA-Chef geheim zu halten, ist nichts für Anfänger. Doch Broadwell passte gut auf. Nie machte sie den Fehler, Intimes mit Petraeus von ihrer persönlichen Handynummer oder E-Mail-Adresse aus zu kommunizieren. Die beiden legten einen gemeinsamen, anonymen E-Mail-Account bei einem freien Webmailer an. Wenn Broadwell Petraeus etwas mitteilen wollte, schrieb sie ihm eine E-Mail – doch statt sie abzuschicken, speicherte sie sie in den Entwürfen. Petraeus, der ebenfalls das Passwort zu dem Account hatte, konnte ihre Nachricht dort lesen und antworten. Broadwell war nie so dumm, sich von ihrem heimischen Internetanschluss aus in den Account einzuloggen. Sie nutzte ausschließlich öffentliche Internetzugänge, um mit Petraeus zu kommunizieren.

Jeder Internetanschluss ist identifiziert durch eine IP-Adresse. Sie ist einmalig im Internet, aber zunächst nicht direkt an eine Person gebunden. Doch der Internetprovider weiß, welche IP-Adressen welchen Kundinnen zugeordnet sind.

Als das FBI in einem Fall von Stalking in General Petraeus’ Umfeld ermittelte, stieß es auf den anonymen E-Mail-Account. Mit den IP-Adressen, die auf den Account zugriffen, konnten die FBI-Agenten kaum etwas anfangen; dahinter befanden sich nur öffentliche Cafés in verschiedenen Städten sowie verschiedene Hotels. Die Hotels wurden Broadwell zum Verhängnis. Anhand der Check-in-Informationen aller Hotels, deren IP-Adressen auf das Konto zugegriffen hatten, konnten die FBI-Agenten die Hoteldaten untereinander abgleichen und analysieren. Gab es einen Namen, der in allen diesen Hotels zu den fraglichen Zeiten eingecheckt war? Es genügten wenige übereinstimmende Datenpunkte, um zu Paula Broadwell zu führen. Das FBI wartete noch ein paar Monate, bis nach der Wiederwahl von Barack Obama, bevor es die Sache auffliegen ließ. General David Petraeus legte am 7. November 2012 sein Amt als CIA-Chef nieder – gestürzt über Datenanalyse.

Die Nadel im Big Heuhaufen

Auch die Datenbanktechnologie der NSA ist weit fortgeschritten. Sie beruht auf der Datenbanksoftware Accumulo, einer Weiterentwicklung von Googles Software Big Table. Mit ihr lassen sich Mustererkennungsanalysen bewerkstelligen. In großen Datenmassen können sich wiederholende Strukturen gefunden und erkannt werden.

Das Interessante dabei sind aber oft gar nicht die Muster, sondern die Abweichungen davon. Wo eine Nadel im Heuhaufen gesucht wird, ist normalerweise jeder Halm einer zu viel. Big Data dagegen mag Heu. Jeder Halm ist anders als alle anderen, deswegen will Big Data möglichst viele von ihnen kennenlernen. Denn je besser das Verständnis des Computers für Heu ist, desto schneller findet er darin die andersartige Nadel. Die NSA braucht darum eine Menge Kommunikationsdaten: Je besser der Computer versteht, was „normale Kommunikation“ (Heu) ist, desto eher findet er die „verdächtige Kommunikation“ (Nadel).

Es liegt außerdem nahe, sich mithilfe der Analyse der Kommunikations-Metadaten ein Bild davon zu machen, wer mit wem kommuniziert und auf welche Weise einzelne Gruppen untereinander vernetzt sind. Die sogenannte Graphen-Analyse ist heute ein gängiges Verfahren, um versteckte Zusammenhänge zwischen Personen oder Fakten in großen Datenmengen zu finden. Accumolo ist darauf spezialisiert.

Daten, die viele von uns sorglos veröffentlichen, weil sie keiner sensiblen Information verdächtig sind, erlauben Rückschlüsse auf durchaus sensible Daten. 2008 zeigten Studierende an der Technik-Uni MIT, dass sie mithilfe einer Analyse von Facebook-Freundschaften errechnen konnten, mit welcher Wahrscheinlichkeit jemand homosexuell ist. Die Idee des Projekts „Gaydar“ ist einfach: Manche Menschen haben ein engeres Verhältnis zu bestimmten Menschengruppen als andere Menschen. In jedem sozialen Netzwerk lassen sich also besonders eng vernetzte Gruppen erkennen – das nennt sich Clustering. Homosexuelle stehen oft in Kontakt zu anderen Homosexuellen. Lässt sich eine Person einem Cluster mit vielen bekennenden Homosexuellen zuordnen, lässt sich davon mit einer gewissen Wahrscheinlichkeit auf ihre sexuelle Orientierung schließen. Die Genauigkeit lag im Fall des MIT-Experimentes bei 86 Prozent. [15]

Als die Idee des Datenschutzes geboren wurde, hatte man die Daten im Sinn, die nach damaligem Verständnis gelesen und entziffert werden konnten. Wenn bekannt ist, welche Daten von einem selbst existieren und was sie aussagen, kann man versuchen, den Zugriff darauf zu kontrollieren. Die „informationelle Selbstbestimmung“, wie sie

das Bundesverfassungsgericht 1983 anerkannte, räumt jedem das Recht ein, über den Zugang zu seinen Daten und ihre Verwendung bestimmen zu dürfen. Auch wenn schon in den 1980ern bekannt war, dass sich Mess- und Analysemethoden kontinuierlich verbessern und dass es Techniken zur Verknüpfung von Daten gibt: Es sah noch aus, als ob Daten das bleiben würden, was sie zur Zeit der Speicherung waren. Wir glaubten noch zu wissen, dass eine Spur zu hinterlassen und sogar, einen „Write“ in eine Datenbanktabelle auszuführen ein endgültiger Vorgang sei, der das Feld seiner Interpretation von vornherein absteckt. Aber wir haben uns geirrt.

Der dritte Treiber des Kontrollverlusts besteht in den immer weiter wachsenden Möglichkeiten zur Verknüpfung von Datensätzen. Die Aussagefähigkeit von Daten wird damit in eine unbekannte Zukunft katapultiert. Weder wissen wir heute, was morgen Daten sein werden, noch wissen wir, was Daten von heute schon morgen aussagen können.

Wir haben die Kontrolle über die Daten also auf dreifache Weise verloren: Wir wissen nicht mehr, welche Daten zu welcher Zeit erhoben werden können, weil die ganze Welt durch die allgegenwärtige Verbreitung von Sensoren digitalisiert wird. Wir bestimmen nicht selbst, was mit diesen Daten geschieht, wo sie gespeichert werden, wo sie hinkopiert werden, wer darauf Zugriff hat. Und wir können nicht ermessen, welche Dinge diese Daten potenziell aussagen. Kurz: Daten, von denen wir nicht wussten, dass es sie gibt, finden Wege, die nicht vorgesehen waren, und offenbaren Dinge, auf die wir nie gekommen wären.

8 http://www.collateralmurder.com

9 Niklas Luhmann, Geheimnis, Zeit und Ewigkeit, S. 105.

10 Gregory Bateson: Geist und Natur, S. 123.

11 „We are with John McAfee right now, suckers!“, in: Vice, http://www.vice.com/read/we-are-with-john-mcafee-right-now-suckers

12 Lisa Gitelman, „Daniel Ellsberg and the Lost Idea of the Photocopy“, http://www.academia.edu/2053410/Daniel_Ellsberg_and_the_Lost_Idea_of_t

13 Chris Anderson, „The End of Theory: The Data Deluge Makes the Scientific Method Obsolete“, http://archive.wired.com/science/discoveries/magazine/16-07/pb_theory

14 Konrad Lischka, „Smartphone-Studie: Das Märchen vom anonymen Bewegungsprofil“, http://www.spiegel.de/netzwelt/web/mobilfunkspuren-lassen-sich-leicht-menschen-zuordnen-a-891850.html

15 Stan Schroeder, „GAYDAR: Your Facebook Friends Can Reveal Your Sexual Orientation“, 21.09.2009 http://mashable.com/2009/09/21/facebook-friends-sexual-orientation/