
1781

Malte Spitz | Brigitte Biermann

Was macht ihr mit meinen Daten?

Hoffmann und Campe

Hintergründe zum Buch und Informationen darüber, wie Sie selbst Anfragen nach Ihren Daten stellen könne, finden Sie unter *www.was-macht-ihr-mit-meinen-daten.de*

1. Auflage 2014

www.hoca.de
Satz: Dörlemann Satz, Lemförde
Gesetzt aus der Sabon und der Frutiger
Druck und Bindung: C. H. Beck, Nördlingen
Printed in Germany
ISBN 978-3-455-50328-9

HOFFMANN UND CAMPE

Ein Unternehmen der
GANSKE VERLAGSGRUPPE

Inhalt

Für meine Frau Silke und meinen Sohn Hannes,
damit er selbstbestimmt im digitalen Zeitalter
aufwachsen kann.

1. Expedition zu meinen Daten

»Wer die Macht über unsere Daten hat? Wissen Sie es? Ich weiß es nicht.«
Prof. Dr. Johannes Tuchel, Leiter der Gedenkstätte Deutscher Widerstand, Berlin

März 2014, Washington D. C. Ich stehe vor dem Rayburn House Office Building. Das ist eines der drei Abgeordnetengebäude des US-Repräsentantenhauses am Capitol: der Grundriss ein H, die Fassade am Sockel rosafarbener Granit, darüber weißer Marmor, die Flure fünf Meter breit und so lang, dass ich mir ein Skateboard wünsche.

Ich bin verabredet mit James Frank Sensenbrenner jr., kurz: Jim. An der Tür zu seiner Büro-Suite, wie an jeder anderen auch, die amerikanische Flagge. Im Vorraum das holzgerahmte Antiterror-Gesetz, das meine politische Arbeit mit am intensivsten begleitet hat: der Patriot Act. Er räumt den US-Bundesbehörden, insbesondere der Bundespolizei FBI und den Geheimdiensten, einen immensen Spielraum zur Überwachung und Speicherung von Daten ein. Daneben ein Foto, das den damaligen Präsidenten George W. Bush zeigt, der das Gesetz kurz nach dem 11. September 2001 unterzeichnet hat. Hinter Bush steht Jim Sensenbrenner, zu jener Zeit Vorsitzender des Rechtsausschusses im Repräsentantenhaus. Er gilt als Vater des Patriot Act.

Und nun, März 2014, sitze ich diesem Mann, der im Repräsentantenhaus den fünften Wahlbezirk des Bundesstaates Wisconsin vertritt, gegenüber.

Der 70-jährige Republikaner ist groß und kräftig, sein Hände-

druck fest, er blickt mir gerade in die Augen. Seit über 30 Jahren ist er Abgeordneter und gilt als eisenharter Verhandler. Ich habe mich auf eine strittige Diskussion vorbereitet, doch wir sind uns schnell einig: Die Praktiken der Massenüberwachung, die seit dem Sommer 2013 nach und nach bekannt werden, sind nicht haltbar. Die Geheimdienste sind außer Rand und Band. Um dem entgegenzusteuern, hat Sensenbrenner mit dem demokratischen Senator Patrick Leahy und Dutzenden anderen Abgeordneten und Senatoren den Freedom Act eingebracht. Sie wollen mit diesem Gesetz die Verhältnismäßigkeit der Mittel wiederherstellen, die Massenüberwachung zurechtstutzen. Sensenbrenner spricht davon, dass er die Sensibilität der Deutschen aufgrund ihrer Geschichte nachvollziehen kann. Über Edward Snowden sagt er: »Er ist weder ein Held noch ein Verräter, er ist ein Krimineller. Allerdings hat er Informationen über Programme ans Tageslicht gebracht, die außerhalb der Grenzen des Gesetzes liegen und die Bürgerrechte von Amerikanern verletzen.« Jim Sensenbrenner will mithelfen, die transatlantische Zusammenarbeit wieder zu stärken. »Ich bin bereit, vor dem Ausschuss des Deutschen Bundestages zu sprechen, wie ich es im Europäischen Parlament getan habe, um Vertrauen in unsere Geheimdienste zurückzugewinnen und um sicherzustellen, dass der Datenschutz gewahrt bleibt.«

Dies zeigt, die Debatte wird nicht nur in Deutschland geführt, sondern weltweit, und zwar nicht nur im politisch linken Milieu, sondern auch bei waschechten Konservativen wie Jim Sensenbrenner, mit dem mich politisch ansonsten eher wenig verbindet. Die Furcht vor dem Verlust der Selbstbestimmung, die durch staatliche Überwachung und die Datensammelwut der Unternehmen ungeahnte Züge annimmt, schweißt eben neuartige Koalitionen zusammen.

Denn Überwachung wirkt. Sie verändert unser Denken und Handeln, und sie tut das allein schon dadurch, dass wir glauben, wir würden überwacht. Forscher der Universität New-

castle dokumentierten das eindrucksvoll mit einem simplen Versuch: Sie brachten in der Kaffeeküche über einer Kasse auf freiwilliger Basis ein Foto an – ein weit aufgerissenes Augenpaar glotzte auf die Kasse. Über einer anderen Kaffeekasse schmückte ein Blumenposter die Wand. In der ersten Kasse fand sich siebenmal mehr Geld als in der zweiten. Wer sich überwacht fühlt, handelt bewusst und unbewusst entweder stärker im Sinne der Überwacher oder stärker gegen sie. Das Ergebnis ist also mehr Selbstkontrolle, mehr Konformität, mehr Misstrauen. Und nicht nur einzelne Menschen, eine ganze Gesellschaft verändert sich durch Überwachung. Menschen büßen Autonomie, Freiheit, Individualität ein, wenn sie das Gefühl haben, dass jemand ihnen zuschaut und sich dafür interessiert, was sie tun und denken. Das steht also außer Frage. Aber wie stark wir von wem überwacht werden, das wollte ich herausfinden.

Ich bin mit PC, Computerspielen und Handys in Telgte aufgewachsen. Das ist ein beschauliches Städtchen im Münsterland, bekannt als Wallfahrtsort und durch Günter Grass' Erzählung *Treffen in Telgte*, in der eine fiktive Dichterrunde kurz vor Ende des Dreißigjährigen Krieges über einen Friedensaufruf debattiert.

Mein Vater arbeitete im Vertrieb von IBM. Er kaufte seinen ersten PC, als ich vier Jahre alt war. Ein paar Jahre später kam ein Notebook dazu, ein unglaublich schweres, sperriges Ding. Ich war aber sehr stolz darauf, denn in der neunten Klasse durfte ich eine Klassenarbeit darauf verfassen.

Seit über zehn Jahren lebe ich in Berlin, mittlerweile mit Frau und Kind, bin zum Studium gekommen, für die Politik geblieben; ich war jahrelang Mitglied im Bundesvorstand von Bündnis 90/Die Grünen, heute gehöre ich dem Parteirat an.

Technik fasziniert mich. Ich bin zwar kein Bastler und Hacker, der Systeme neu zusammenlötet, Toaster repariert oder ein Handy so programmiert, dass man damit auch die Lam-

pen im Wohnzimmer bedienen kann. Aber ich weiß, wie man eine Festplatte ausbaut, den Speicher erweitert und seine Daten sichert. Seit Mitte der neunziger Jahre bewege ich mich im Internet in Foren und Chats. Dass Daten überall erhoben, gespeichert und ausgewertet werden, lag trotzdem lange Zeit außerhalb meines Vorstellungsvermögens.

An der Universität wurde es mir zum ersten Mal richtig bewusst. Unsere Immatrikulationsnummer war das A und O, nicht der Name. Suchte ich auf den Aushängen im Schaukasten meines Professors nach meinen Prüfungsergebnissen, fand ich sie nur unter der Nummer. Wollte ich etwas vom Prüfungsamt, hatte ich mich mit meiner Immatrikulationsnummer vorzustellen. Und so ging das immer weiter. Das soll Datenschutz gewährleisten, doch ist es auch ein ideales Instrument zur Kontrolle. Viele Hochschulen haben es perfektioniert: Mit der Immatrikulation bekommt man eine elektronische Karte wie im Hotel, und wie im Hotel dient sie als Schlüssel für Zimmer, zu denen man Zutritt hat, man kann damit in der Mensa bezahlen, in der Bibliothek Material ausleihen und das Konto für Drucker und Kopierer aufladen.

Je mehr Computer, Chipkarten, Lesegeräte wir in unserer Welt installieren, desto mehr solcher Daten werden überall erzeugt und verarbeitet. Jeder ist irgendwo erfasst, jeder hat inzwischen einen Zwilling, einen Datenschatten von sich selbst – ohne ihn zu kennen. Wer weiß schon, was Behörden, Firmen und Organisationen über ihn wissen? Wer von uns kennt all die Datenbanken, in denen etwas über uns steht?

Meine Neugier trieb mich, eine Expedition zu wagen. Nicht zum Südpol wie Roald Amundsen, der 1911 in die Antarktis aufbrach. Auch nicht zu den Berggorillas in Ruanda wie Dian Fossey. Mein Ziel schien mir überhaupt nicht so fern, und doch war die Suche mühsam, langwierig, manchmal entmutigend. Dabei musste ich nicht mit detektivischem Spürsinn vorgehen, ich habe nur die demokratischen Möglichkeiten genutzt, die unsere Gesetze bieten. Ich wollte in die Rechenzentren und

Datenbanken, wollte Daten von meinem Mobilfunkanbieter und meiner Krankenkasse, von meinem Bürgeramt und meiner Bank. Ich wollte wissen, was die Lufthansa über meine Flüge speichert, die Bahn über meine Zugfahrten, die Kreditkartenfirma über meine Einkäufe. Mich interessierte, was Polizei und Verfassungsschutz über mich sammeln. Ich wollte erfahren: Was macht ihr mit meinen Daten? Welche meiner Daten werden von wem gespeichert, wie werden sie verwendet, wer hat darauf Zugriff, und was kann daraus abgeleitet werden? Ich wollte herausfinden, ob wir schon in einem Überwachungsstaat leben.

Das muss sich nicht anfühlen wie im Nationalsozialismus oder der DDR. Diese Regimes ließen Datenberge anhäufen, um ihre Bürger zu überwachen und sie zu diskreditieren und ihre Persönlichkeit zu zerstören, wenn es ihnen angebracht schien. Es wird am Ende des Buches noch die Rede davon sein, ob solche Vergleiche taugen oder nicht.

Ich habe für dieses Buch viele Menschen getroffen, um mit ihnen über dieses Thema zu sprechen. Ich wollte herausfinden, ob auch sie unsere informationelle Selbstbestimmung in Gefahr sehen. Ich wollte wissen, was wir tun können, um das Grundrecht, selbst entscheiden zu können, wer was über uns weiß, zu verteidigen.

Es sind Menschen, die sich beruflich damit beschäftigen, wie Gus Hosein, Direktor von Privacy International, einer Organisation, die in London sitzt und mit einem Dutzend Mitarbeiter globale Datenschutzfragen bearbeitet. Wie Thomas Drake, ein früherer Mitarbeiter der NSA, der zum Whistleblower wurde. Oder wie der Politikwissenschaftler Ron Deibert, der in Toronto an der renommierten Munk School of Global Affairs lehrt und dort mit seinem Citizen Lab untersucht, wie Internetüberwachung weltweit, besonders in Ländern wie China, Syrien und Bahrain, stattfindet.

Gemeinsam mit zwei Abgeordneten von Bündnis 90/Die Grünen bemühte ich mich um einen Besuchstermin bei der

Zentrale der NSA in Fort Meade, um Konkretes über deren Arbeit zu erfahren. Wahrscheinlich wären wir eher bei Barack Obama vorgelassen worden. Die US-Botschaft in Berlin hatte den Weg über die deutsche Botschaft in Washington D. C. empfohlen. Die reichte unseren Wunsch, vermutlich mit Unterstützung des deutschen Auslandsgeheimdienstes, weiter an die NSA. Vorbedingung war, dass ich die Sicherheitsfreigabe für Angelegenheiten, die topsecret sind, also zur höchsten Geheimhaltungsstufe gehören, habe. Die habe ich natürlich nicht. Sie zu beantragen und das Genehmigungsverfahren zu durchlaufen, dauert Monate. Ich hatte keine Chance, aber auch Abgeordnete mit dieser Sicherheitsfreigabe wurden nicht vorgelassen.

Aber ich sprach mit Peter Schaar, der in den zehn Jahren seiner Amtszeit als Bundesdatenschutzbeauftragter immer wieder die Konfrontation mit den Bundesregierungen suchte, wenn deren Ideen zu staatlichen Eingriffen zu weit gingen. Ich traf mich mit Thorsten Höche, dem Chefsyndikus des Deutschen Bankenverbandes, der dafür streitet, dass unsere Bankgeschäfte nicht bis ins Kleinste durchleuchtet werden. Und mit Frank Rieger, einem der Sprecher des Chaos Computer Clubs (CCC), der mittlerweile eine Institution ist, wenn es darum geht, Fragen und Abwägungen im Bereich Datenschutz, Überwachung und IT-Sicherheit zu klären. Mit Silke Lüder, einer Ärztin aus Hamburg, die für mehr Datenschutz im Gesundheitswesen streitet. Und mit Annette Mühlberg von der Gewerkschaft Ver.di, die sich dort maßgeblich mit dem Thema digitaler Wandel beschäftigt.

Ich wollte also die Überwachung kennenlernen. Die Folgen der Verdatung all unserer Lebensbereiche, ob in der Schule, bei der Arbeit, beim Einkaufen, auf Reisen oder in der Arztpraxis, egal ob online oder nicht, die können wir im Alltag nur ansatzweise erkennen. Ich wollte am eigenen Leib erfahren, was es heißt, bei jeder Bewegung, bei jeder Handlung beobachtet zu werden.

Denn: Nur wenn wir wissen, wie unsere Datenwelt funktioniert, können wir verhandeln, gegen welche Auswüchse wir uns wehren wollen, können wir Grenzen ziehen und dazu beitragen, dass informationelle Selbstbestimmung nicht zu einem Recht von vorgestern verkommt, sondern auch in der digitalen Zukunft zentraler Bestandteil unseres Alltags bleibt. Nur so können wir die Macht über unsere Daten behalten. Das ist zwar in erster Linie eine politische Aufgabe, letztendlich aber sind wir alle dafür verantwortlich.

Denn Datenschutz und Kontrolle über unsere Daten brauchen wir. Das war schon klar, lange bevor Computer und Sensoren in jedem Telefon begannen, uns auszuforschen. Ein wesentlicher Grundstein für unsere Datenschutzgesetzgebung wurde nach dem Protest gegen die Volkszählung Anfang der achtziger Jahre gelegt. Das Bundesverfassungsgericht schrieb 1983 mit seinem Volkszählungsurteil das Recht auf informationelle Selbstbestimmung als Grundrecht fest und forderte, dass jeder Einfluss darauf haben müsse, was mit seinen Daten geschieht. In dem Urteil heißt es: »Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. (…) Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.«

Datenschutz ist also nicht erst seit den Enthüllungen von Edward Snowden gesamtgesellschaftlich relevant, auch wenn er uns erst klargemacht hat, wie hemmungslos und bar jeglicher Verhältnismäßigkeit Geheimdienste in unserem Privatleben herumwühlen, unsere Mails auswerten, unsere Telefonate mithören, unsere Konten überwachen und in unsere Computer eindringen.

Es ging mir bei meiner Expedition nicht um die Alternative, ob ich Twitter, Facebook und andere Netzwerke nutze oder nicht, ich war auch nicht auf der Suche nach der Smartphone-

App, die die meisten Daten abgreift. Mündige Bürger können das für sich selbst entscheiden.

Ich habe da angesetzt, wo es für den Einzelnen kein Entkommen gibt. Wo Daten oft im Auftrag des Staates gespeichert werden. Wo die Grundlage für Überwachung geschaffen wird.

Wir haben alle einen Personalausweis, wir sind beim Einwohnermeldeamt erfasst, im Melderegister gespeichert. Jede und jeder besitzt eine Krankenversicherung, die nicht nur die Arztrechnungen begleicht, sondern auch genaue Profile über unsere Gesundheit anlegt. Die meisten von uns telefonieren, führen ein eigenes Bankkonto, reisen in der Welt umher, surfen im Internet.

Und ich wollte bei meiner Expedition nicht nur meine Daten finden, sondern auch etwas darüber erfahren, wie sie miteinander verbunden sind und wie daraus Überwachung entsteht. Schließlich handelt es sich um einen Verlust von Freiheit, wenn diese Daten immer umfassender genutzt werden, wenn unser Leben immer mehr von unseren Scoring-Werten bestimmt wird. Ich habe mit etlichen Experten darüber gesprochen. Darüber, wie das Ganze funktioniert, wie sich dadurch unsere Welt verändert und wohin sich unser Leben durch die Verdatung entwickelt, wer die Macht über unsere Daten hat.

Was derzeit passiert, entspricht einer Neuvermessung. Wie Menschen künftig denken und handeln, wird sich durch die Nutzung dieser riesigen Datensammlungen grundlegend ändern. Viele Staaten und Unternehmen werden sich künftig damit befassen, wie sie optimalen Gewinn aus den immer größer werdenden Datenhaufen ziehen werden. Hieß es in George Orwells berühmtem Roman *1984* »Big brother is watching you«, gilt heute »Big data is watching you«. Dieser Horrorvision entgegenzuwirken, um nichts anderes geht es.

Denn meine Sorge ist groß, dass sich durch den digitalen Wandel ein System entwickelt, das unsere persönliche Freiheit am Ende mehr einschränkt, als uns neue Wege eröffnet. Eins ist jetzt schon klar: Der Preis, den wir für die vielen neuen Mög-

lichkeiten der Wissensvermittlung, der kulturellen Vielfalt, der neuen Arbeitswelt und des technologischen Fortschritts zahlen müssen, wird sehr hoch sein.

Meine Expedition startete ich vor über fünf Jahren. Damals erbat ich von meinem Mobilfunkanbieter Deutsche Telekom, damals noch T-Mobile, alle zu meiner Person gespeicherten Daten. Weil man mir erst gar keine und auf mein Insistieren nur eine unvollständige Auskunft erteilte, entschied ich mich dafür zu klagen. Ich wollte nicht hinnehmen, dass Daten, die ich mit meinem Handy erzeugt hatte und die einen Teil meines Lebens widerspiegeln, für mich selbst nicht zugänglich sind. Denn auch das ist ein Merkmal dieser neuen Welt – wir wissen nicht, was andere über uns wissen, und es wird auch noch vor uns geheim gehalten. Wollen wir es erfahren, bekommen wir keine oder nur eine unvollständige Antwort.

Gleichzeitig wird gezielt immer mehr gespeichert. Mit dem 2007 verabschiedeten Gesetz zur Vorratsdatenspeicherung sind zum Beispiel Anbieter von Telefon- und Internetdiensten verpflichtet worden, Kommunikationsverkehrsdaten von jedem Nutzer mindestens sechs Monate ohne jeden Anlass aufzuheben.

Deutlicher kann ein Staat nicht zeigen, wie sich Datenspeicherung – und damit Datenschutz – in den vergangenen Jahren gewandelt hat. Glücklicherweise hat der Europäische Gerichtshof mittlerweile die Richtlinie, die diesem Gesetz als Blaupause diente, für unrechtmäßig erklärt, die Eingriffe in unsere Privatsphäre und den Datenschutz waren zu umfassend, die Anlasslosigkeit nicht vereinbar mit unseren Grundrechten.

Der Protest vor dreißig Jahren gegen die Volkszählung zielte noch auf den Staat, der seine Bürger zählen und messen wollte. Heute halten sich staatliche Behörden meist im Hintergrund und überlassen die Schmutzarbeit des Datensammelns anderen. Sie zwingen Unternehmen, Daten zu erheben, zu speichern und für ihre Interessen aufzubereiten. Liegen Daten verteilt bei verschiedenen Unternehmen unterschiedlicher Branchen, seien es

Telefongesellschaften, Banken oder Reiseanbieter, muss niemand Angst vor dem allwissenden Staat haben.

Das ist aber ein Irrtum. Nur weil die Daten nicht auf den Servern des Staates liegen, heißt das nicht, dass er sie nicht gegen uns verwendet. Der Staat räumt sich umfassende Zugriffsrechte ein, deren Hürden er immer weiter senkt.

So sollte beispielsweise mit dem Programm namens ELENA eine umfassende Datenbank von Sozialversicherungsdaten entstehen; gespeichert werden sollten Name, Geburtsdatum und Anschrift, Beruf, Lohn und Steuerklasse, Arbeits- und Fehlzeiten, Urlaubsanspruch und tatsächlich genommene Urlaubstage, Angaben zu Entlassungen, Abmahnungen und Kündigungen, sogar die Teilnahme an Streiks. Und das alles von über 35 Millionen abhängig Beschäftigten. Brave Arbeitnehmer wären damit hervorragend von aufmüpfigen zu trennen gewesen.

Mit der Vorratsdatenspeicherung sollte unsere gesamte digitale Kommunikation gehortet werden, also nicht nur, wann wir an welche Adresse eine Mail oder eine SMS schicken, wann wir uns ins Internet einloggen. Gespeichert werden sollte auch, wo wir uns dann gerade befinden – und all das für mindestens sechs Monate.

Dass Fluggastdaten jahrelang aufgehoben werden, ist längst Realität. Fluggesellschaften müssen schon vor dem Start Behörden in den Zielländern wie den USA und Kanada eine umfassende Datenübersicht des jeweiligen Passagiers vorlegen, inklusive Essensbestellungen, Zahlungsdaten und Sonderwünschen.

Na und? Ich hab doch nichts zu verbergen, so reagieren viele auf das Problem. Wirklich nicht? Niemand erzählt doch überall rum, dass sein Konto meistens im Minus ist, dass man schon mal beim Psychiater war, dass man einen HIV-Test durchgeführt hat, dass man abends einen Abstecher ins Bordell gemacht hat, dass die Tochter einen Freund ohne Schulabschluss hat. Oder?

Diese Ist-mir-doch-egal-Haltung ist fahrlässig und eine Gefahr für uns alle. Denn auch, wenn man ein gesetzestreuer Bürger ist, der seine Rechnungen und Steuern bezahlt, nicht bei Rot die Straße überquert und in Ortschaften konstant fünfzig Kilometer in der Stunde fährt, kann man zum Opfer von Überwachung und Repressalien werden. Heutzutage entscheiden nicht meine Erscheinung, mein Auftreten und mein Verhalten darüber, ob mich der Staat oder Unternehmen in Ruhe lassen, sondern die über mich gespeicherten Daten. Es werden längst nicht mehr mal hier und mal da ein paar Informationen herausgepickt; Ziel ist eine durch Algorithmen erzeugte, auf Statistik und Soziologie basierende Einordnung des Menschen in Gruppen, Klassen, Muster. Daten lösen unser tatsächliches Handeln ab.

Fatal, wenn sie nicht der Realität entsprechen. Sie können fehlerhaft sein oder falsch zugeordnet, verkürzte Inhalte können zu widersinnigen Schlussfolgerungen führen, sie können falsch ausgewertet, missbraucht, gestohlen sein – trotzdem werden sie im Zweifel gegen uns verwendet. Es genügt, dass unsere Daten denen eines Terroristen nur ähneln, um verdächtig zu werden. Wer häufig mit dem Flugzeug in bestimmte Länder reist, ist vielleicht Handelsvertreter einer großen Firma – vielleicht aber auch ein Drogenschmuggler. Datenbanken unterscheiden nicht, beide Personen sind zunächst aufgrund der über sie gespeicherten Informationen verdächtig, sie werden überwacht, festgehalten, durchsucht, befragt.

Diese Gefahr sieht auch Johannes Masing. Er ist seit 2008 Richter im Ersten Senat am Bundesverfassungsgericht und zuständig für Verfahren zum Datenschutz. Auf einer Konferenz Ende Januar 2014 in Berlin hielt er eine Rede, was ungewöhnlich für amtierende Verfassungsrichter ist, die sich nur selten öffentlich zu Wort melden. Darin beschreibt Masing die Gefahren der zunehmenden Datensammlung: »Das Verfügbarhalten von Daten, das unsere Freiheitswahrnehmung festhält, gefährdet diese wie schleichendes Gift: Freiheit wird mit Angst be-

setzt – den falschen Film zu sehen, die falsche Veranstaltung oder Demonstration zu besuchen, die falsche Zeitung zu lesen oder die falsche Website aufgerufen zu haben, kann gefährlich werden.« Er sieht darin eine Gefahr für jeden Einzelnen, wie für die »politische demokratische Ordnung«.

Natürlich ist nicht jede Datenspeicherung beziehungsweise deren Verarbeitung zu verdammen. Und nicht jede lädt ein zu Missbrauch. Dass dabei an vielen Stellen auch ein Mehrwert für die Gesellschaft herausspringt, ist absehbar und sehr wahrscheinlich.

Einer meiner Bekannten, der Amerikaner John Wilbanks, hat in Kalifornien das Projekt »Consent to Research« (Einwilligung zur Forschung) gestartet. Er erbittet die Gesundheitsdaten von Menschen samt deren Erlaubnis, diese zu sammeln und weiterzugeben. John will mit diesen Daten erreichen, dass mehr Unternehmen in die Forschung investieren, vor allem aber, dass sie sich um seltene Krankheiten kümmern, was bislang meist als unrentabel abgetan wird. Um dafür einen Anreiz zu schaffen, sind Zehntausende erfasste Daten erforderlich.

Es gibt sie also, die positive Nutzung von Big Data. Aber nur, wenn wir die dafür notwendigen Informationen freiwillig und zweckgebunden preisgeben und wenn überflüssige gar nicht erst erhoben werden. Wenn Transparenz herrscht statt Vertuschung und Vertrauen in die beteiligten Akteure.

Durch die Menge unterschiedlicher Datenbanken, durch die immer weitreichendere Nutzung von Smartphones, Kunden-, Kredit- und Gesundheitskarten wird das digitale Abbild unseres Lebens immer genauer. Daten sind nicht nur für Google, Facebook und Co. bares Geld wert, sondern auch für Einwohnermeldeämter, Krankenkassen, Reiseunternehmen, Versicherungen, Banken, Autohersteller, Kaufhäuser und Versandhändler. Je mehr Informationen die Krankenkasse über die Lebenssituation, die Ess-, Sport- und Alltagsgewohnheiten eines Mitgliedes besitzt, umso genauer kann sie bewerten, ob eine Leistung genehmigt werden sollte oder nicht. Aus den gespei-

cherten Daten meiner vergangenen Reisen schlussfolgert der Computer meines Reisebüros, dass ich Wert auf Qualität lege, man wird mir also keine Rucksackreisen für Studenten anbieten. Es ist natürlich nicht die Regel, dass die Polizei im Zuge von Ermittlungen einer Straftat Daten von einem Reisebüro anfordert oder Kontobewegungen abgleicht. Aber es ist möglich, und es geschieht. Geheimdienste hingegen greifen mittlerweile höchstwahrscheinlich weltweit alle Daten ab, derer sie habhaft werden können, nicht nur von ein paar Tausend, sondern von Millionen Menschen. Das Risiko, in das Netz der Überwachung zu geraten, war in der Bundesrepublik Deutschland nie so groß wie heute.

Ob ein solcher Eingriff in unsere Menschenrechte durch das zunehmende Aushöhlen unserer Privatsphäre noch in irgendeinem Verhältnis zum Gewinn an vorgeblicher Sicherheit steht, wird derzeit heftig diskutiert. Sicherheitspolitische Hardliner in Deutschland, den USA und anderswo auf der Erde führen immer wieder ins Feld, die gewünschte Sicherheit sei nur zu haben, wenn wir auf individuelle Freiheiten verzichten. Das ist aber nur die halbe Wahrheit.

Polizisten arbeiten nicht mehr nur daran, Verbrechen aufzuklären – sie sollen sie verhindern, bevor sie geschehen. Sie sollen bereits vor einem Anschlag wissen, wer ihn plant. Doch das funktioniert nur, wenn prinzipiell jeder verdächtigt werden kann und von allen Informationen gespeichert werden. Die Unschuldsvermutung gibt es nicht mehr. Darin sehen Geheimdienste ihre Legitimation, die Überwachung auf all unsere Lebensbereiche immer weiter auszudehnen.

Und es gibt einen weiteren Grund für die massenhafte Verdatung: Geld. Daten sind im 21. Jahrhundert eine zentrale Währung geworden, darauf aufbauende Geschäftsmodelle sorgen für Milliardenumsätze in der ganzen Welt. Daher greifen viele Wirtschaftsunternehmen nur allzu gern jede Idee zur Datenspeicherung auf. Und da sie, rechtlich abgesichert, ihre Datenbanken ins Uferlose ausweiten dürfen, sind sie im Gegenzug

natürlich bereit, staatliche Stellen damit zu versorgen, ihnen zumindest den Zugang zu gewähren. Deshalb wird Big Data derzeit vor allem als wirtschaftlicher Motor und als technologische Herausforderung diskutiert. Welchen Nutzen wir Bürger daraus ziehen und wie sehr unsere informationelle Selbstbestimmung dafür weiter minimiert wird, ist die große Unbekannte.

Ich befürchte, dass das System der Verdatung unseres Lebens nicht mehr nur immer raffinierter wird, sondern dass es eines Tages so intelligent ist, uns in unseren Lebensentscheidungen, den großen wie den alltäglichen kleinen, noch entscheidender zu prägen. Schon jetzt können Finanzdienstleister durch Scoring unser Kaufverhalten und unsere Zahlungsmoral abfragen und danach befinden, ob wir einen Kredit für die Unternehmensgründung erhalten oder nicht. Unsere Datenprofile könnten bereits festlegen, wer neben uns im Flugzeug sitzt, welche Arztpraxis wir aufsuchen und welche Behandlungsmethode wir erhalten. Die Navigations-App auf dem Smartphone könnte uns zu Läden lenken, die unsere Kaufkraft kennen und die dafür bezahlt haben, dass die Software uns an ihren Schaufenstern vorbeischickt. Versicherungen könnten unser Verhalten beobachten und mittels digitaler Sensoren messen, was wir tun oder lassen, um zu errechnen, wie viel wir für eine Police zahlen müssen. Künftig könnte die Hausratversicherung unsere Beiträge danach ausrichten, ob wir Türen und Fenster schließen und ob wir Geschirrspüler und Waschmaschine ausstellen, wenn wir das Haus verlassen.

Verfassungsrichter Masing erkennt die Tragweite dieses Prozesses: »Durch die Verfügbarkeit individueller Daten wird der Einzelne erpressbar und manipulierbar. Unser Handeln kann durch statistische Berechnungen vorhergesagt werden – die Beherrschung der Daten legt uns auf Handlungsmuster fest, die wir weder kennen noch beherrschen, und nach diesen Bildern werden unsere Chancen definiert – sei es, wer welches Angebot, welchen Kredit oder welchen Arbeitsplatz erhält, sei es, wer

von der Polizei durchsucht wird oder einen Flug antreten darf. Die Daten wissen mehr über uns als wir selbst, individuelle Freiheit droht als statistische Unschärfe zu verschwinden.«

Das ist keine Zukunftsmusik. Unlängst hat Google eine Firma namens Nest gekauft, die Daten sammelnde Heizungsthermostate und Rauchmelder herstellt. Das sind die Sensoren, die künftig auch in unseren Wohnungen überwachen, was wir tun, und die diese Daten an Firmen und letztlich auch an Staaten senden.

Das Zusammenspiel von Informationen aus unterschiedlichen Quellen, die Masse der Daten, der Speicherort, die Menschen, die darauf Zugriff haben – all das birgt Gefahren, von denen wir heute noch nichts ahnen. Denn wer die Macht über Daten hat, kann uns auf Schritt und Tritt verfolgen, Entscheidungen manipulieren, Probleme bereiten und damit unser Leben nicht nur überwachen, sondern auch steuern. Dieses Wissen kann in Menschen ein Gefühl von Ohnmacht erzeugen.

Daher wird es in den kommenden Jahren neben dem Kampf gegen den Klimawandel und dem Umgang mit der sozialen Entwicklung einer alternden Gesellschaft eine unserer zentralen Aufgaben sein, unsere informationelle Selbstbestimmung zu retten und zu wahren. Datenschutz ist eine der zentralen Machtfragen des 21. Jahrhunderts.