

Data Love



Roberto Simanowski

Data Love



Matthes & Seitz Berlin

In einen hohlen Kopf geht viel Wissen.
(Karl Kraus)

And youth is cruel, and has no remorse
And smiles at situations which it cannot see.
(T. S. Eliot)

He was found by the Bureau of Statistics to be
One against whom there was no official complaint,
And all the reports on his conduct agree
That, in the modern sense of an old-fashioned word,
he was a saint.
(W. H. Auden)

Inhalt

Vorbemerkung	7
I. Jenseits der NSA-Debatte	16
1. Geheimdienstlogik	16
2. Doppelte Gleichgültigkeit	22
3. Self Tracking und Smart Things	28
4. Datenumweltkatastrophe	33
5. Kalter Bürgerkrieg	44
II. Paradigmenwechsel	56
1. Data Mining Business	56
2. Absichtslose Sozialingenieure	60
3. Stille Revolution	68
4. Algorithmen	76
5. Ästhetik der Theorielosigkeit	89
III. Glück der Zahl	97
1. Vermessungszwänge	97
2. Phänomenologie des Numerischen	102
3. Digital Humanities	113
4. Lessings Duplik	123
IV. Widerstände	133
1. Das Auge Gottes	133
2. Data Hacks	140
3. Vom richtigen Leben im falschen	155
Nachbemerkung	164
Anmerkungen	168



Vorbemerkung

Gelobt sei die Technologie, die uns erlaubt, in den Schweizer Alpen und in Hongkongs U-Bahn Berlins Info-Radio zu hören. Gelobt sei der Stadtplan, der per Klick von sich selbst erzählt und an die gewünschte Stelle führt, ohne dass man ihn studieren muss. Lob Shazam und all den Apps, die einen unbekanntem Song identifizieren und sogleich zu Text und Video linken. Lob dem Online-Fahrplan, der uns sekunden-schnell Verbindungen erstellt und zugleich das Ticket verkauft. Lob auch dem Asthma-Inhalator, dessen Gebrauch per GPS anderen Patienten die Gebiete anzeigt, die sie meiden sollten.

Wir lieben Information. Wir haben es immer getan. Wir scharten uns um den Wanderer, um von fernem Gegenden zu hören, als Bücher noch selten waren außerhalb der Klöster. Wir erfanden den Telegrafen, weil wir nicht auf Reisende warten wollten. Wir sahen der Morgenzeitung mit Spannung entgegen wie den Abendnachrichten im Radio, im Fernsehen, als hätten wir nur Gutes zu erwarten. Wir erhalten nun Neuigkeiten in Echtzeit und behandeln das eigene Leben wie News mit Updates rund um die Uhr auf Facebook, Twitter, Instagram. Wir sind so hungrig nach Information wie freigiebig mit ihr.

Wir betrachteten jeden Berg, jeden See, der nicht vermessen ist, als Beleidigung der menschlichen Ver-



nunft und vermessen nun mit endlosem Eifer die Netzwerke des Sozialen und uns selbst, wenn wir kommunizieren, fernsehen, joggen, essen, schlafen. Wir sind auf einer Mission der permanenten Daten-Produktion als Beitrag zur Erkenntnis: für Wirtschaft, Medizin, Gesellschaft. Wir glauben an Fortschritt durch Analyse. Die unser Leben erleichtert und sicherer macht.

Wir lieben uns als blauen Punkt im Navigationsgerät und hoffen auf die Smart City, die weiß, wo ihre Bürger sind, und ambulante Taxisstände dort entstehen lässt, wo sie gerade gebraucht werden. Wir hoffen auf die »wearable computer«, mit denen wir online sein können, ohne die Hände vom Lenkrad zu nehmen. Wir danken Google für die Auskunft, was wir als nächstes tun wollen, und freuen uns auf Google Glass.

Informationsgesellschaft ist, wenn jede Information nur Sekunden entfernt ist, zu allem, überall und jederzeit. Information at your fingertips. Wir leben in der Informationsgesellschaft. Und wir lieben es.

Im Jahr 2011 fand in Berlin die Konferenz *Data Love* statt, deren Titel wie folgt begründet wurde:

Heute sind Daten das, was Elektrizität für das industrielle Zeitalter war. Unternehmensberater, Marketingexperten und Agenturleiter stehen vor der Herausforderung, aus dem stets wachsenden Datenstrom neue Anwendungen mit zusätzlichem Wert für die Kunden zu entwickeln. In unserer von Daten gesteuerten Wirtschaft steht der Konsument im Mittelpunkt aller Über-



legungen. Denn sein Verhalten entscheidet, wer gewinnt, was Bestand hat und was sich verkauft. Daten sind der entscheidende Faktor für die Entwicklung relevanter Produkte und Serviceleistungen für den Kunden.¹

Was hier mit Nachdruck empfohlen wird, bestätigt das *Harvard Business Manager*-Magazin in seinem November-Heft 2012 *So beherrschen Sie Big Data* mit dem klassischen Leitsatz: »Was man nicht messen kann, kann man nicht managen.« Beide Aussagen zeigen: Data Love ist keineswegs bedingungslos. Sie zielt nicht auf Daten um ihrer selbst willen, sondern als Information, die dem Gegebenen (lateinisch *datum*) bedeutungsvoll Gestalt gibt (lateinisch *informare*).²

Data Love ist das euphemistische Begleitwort zum Leitbegriff der digitalen Informationsgesellschaft: Big Data Mining – die computergesteuerte Analyse großer Datensammlungen auf bestimmte Gesetzmäßigkeiten und unbekannte Zusammenhänge hin. Die Liebe ist dabei doppelter Natur. Sie zielt auf Daten als Objekt der Begierde, denn ohne sie ist kein Mining möglich. Zugleich sind die Daten das Subjekt der Liebe, gerichtet auf jene, von denen sie stammen und in deren Interesse die Personalisierung der Angebote erfolgt, die durch die Daten möglich wird. So steht es jedenfalls in der zitierten Auskunft: Die Kenntnis der Daten verbessert den Dienst am Kunden. Data Love ist ein Phänomen der Kontroll- wie der Konsumgesellschaft im Zeitalter ihrer digitalen Verfasstheit. Sie vollzieht sich im Interesse derer, die der Datenschutz retten will. Das ist, worum es hier geht.

Es geht um die Versprechen und Gefahren dieser ambivalenten, zum Großteil unausgesprochenen Liebe. Erörtert wird die Veränderung, die diese Liebe der menschlichen Situation bringt. Data Love erweist sich dabei nicht nur als Obsession übereifriger Geheimdienste oder findiger Geschäftsleute, sondern als Verstrickung aller, die mehr oder weniger – aus Geiz, Bequemlichkeit, Ignoranz, Narzissmus oder Leidenschaft – dabei helfen, dass immer mehr Daten ihres Lebens der statistischen Auswertung und individuellen Profilbildung zugeführt werden.

Wer den NSA-Skandal des Sommers 2013 nur als Spannung zwischen den beiden Grundrechten auf Freiheit und Sicherheit diskutiert, übersieht, dass das Transparenz-Gebot der sozialen Online-Portale, die Applikationen des Self Tracking und das Zukunftsversprechen des Internets der Dinge die allgemeine Datenerfassung auch jenseits der Geheimdienste zum Alltagsphänomen machen. Dem technisch Möglichen kann, noch immer, kaum jemand widerstehen. Das gilt naturgemäß vor allem für den Geheimdienst. Aber auch die Wirtschaft will nicht unter dem Stand der Technik operieren. Auch die Verwaltung nicht, und ebenso wenig ein Großteil der Bevölkerung. Darin liegt das philosophische Problem jenseits der politischen Diskussion des NSA-Skandals – und zugleich das paradoxe Versöhnungspotenzial der Gesellschaft mit ihrem Sicherheitsapparat: Im Zeitalter der zunehmenden Digitalisierung menschlicher Kommunikation ist der »full take« aller Daten von allen und allem die logische Konsequenz für alle. Entgegen anders-

lautender Wünsche und Erklärungen ist Privacy im 21. Jahrhundert outdated: durch Big Data und nicht zuletzt durch Data Love.

Die Freizügigkeit mit den eigenen Daten wurde mit der Umweltkatastrophe verglichen: So wie der individuelle Energieverbrauch keine persönliche Angelegenheit sei, habe auch der Umgang mit den eigenen Daten gesellschaftliche Konsequenzen von ethischer Dimension. Diese Perspektive führt die Diskussion über die beschönigende Feindlogik Bürger kontra Staat hinaus und entschärft das Problem zugleich auf neue Weise. Denn während die Bewahrungsethik der Umweltbewegung auf den Erhalt der menschlichen Existenz zielt, wogegen niemand ernsthaft Einwände haben wird, operiert das Konzept der »Datenkatastrophe« im Grunde kulturpessimistisch und wertkonservativ, was nicht nur einen Großteil der jüngeren Generation gegen sich hat. Wenn im Zuge des NSA-Skandals von einem »kalten Bürgerkrieg« die Rede ist, gilt dies vor allem als Konflikt *in* jedem Bürger: zwischen dem Interesse an den Vorteilen und der Angst vor den Nachteilen, die in der Vermessungs- und Analysebesessenheit einer zunehmend digitalisierten und datenfixierten Gesellschaft liegen.

Die unmittelbaren Akteure des Big Data Mining sind die Number Cruncher und Data Scientists, deren Berufsbild in der Gegenwart an Sexappeal gewinnt und Millionengewinne verspricht. Ihre Erfindungen eines effizienteren Datenmanagements und erkenntnisreicherer Datenanalysemethoden verändern unbemerkt und unaufhaltsam die kulturellen

Werte und sozialen Normen der Gesellschaft. Die Softwareentwickler sind die neuen Sozialingenieure, deren einziges Programm für die Welt deren Programmierbarkeit ist, gelegentlich garniert durch vage Worte über den emanzipativen Wert der Partizipation und Transparenz. Die heimlichen Helden – und das Pandorageschenk – dieser »stillen Revolution« sind die Algorithmen, die als entfesselte Artificial Intelligence zweifach die Herrschaft über die Menschen antreten: Zum einen übernehmen sie immer mehr Wenn-Dann-Handlungsanweisungen, um sie sogleich bedingungslos umzusetzen. Zum anderen erkunden sie im Big Data Mining immer mehr Wenn-Dann-Korrelationen und stellen mit diesem neuen Wissen die Gesellschaft unter den Handlungsdruck, bei unerwünschten *Dann*-Folgen auf der *Wenn*-Ebene einzugreifen.

Die Angstworte der Zukunft lauten deswegen nicht NSA oder Big Brother, sondern *predictive analytics* und *algorithmic regulation*. Es sind Geistesverwandte der technokratischen Rationalität, die einst als dunkle Seite der Aufklärung unter den Stichworten Verdinglichung und Verantwortungslosigkeit kritisch diskutiert wurde. Der statistische Blick auf die Gesellschaft im Schlepptau des Big Data Mining verschärft die Gefahrenlage und ermahnt zu einer Diskussion, die weit über die Frage hinausgeht, wie in Zeiten der digitalen Medien und im Kontext der Terrorismusbekämpfung das Briefgeheimnis gewahrt bleiben kann. Die Frage ist vielmehr, welches Bild die moderne Gesellschaft von sich selbst hat und welchen Spielraum sie den

Technologien, die sie hervorbringt, für die Veränderung dieses Bildes einräumt.

Treibt man die Diskussion über die Tagesaktualität hinaus, zeigt sich, dass parallel zum Überwachungs- und Privacy-Problem selbst wissenschaftstheoretische Entwicklungen dem Paradigma des Data Mining zuarbeiten. Angesichts der statistisch ermittelbaren Erkenntnisse wird das »Ende der Theorie« ausgerufen und der Geisteswissenschaft unter dem Stichwort »Digital Humanities« empfohlen, sich als »harte« Wissenschaft zu begreifen, die quantitativ gesichertes Wissen erzeugt. Diese Umstellung vom Subjektiven und Ambivalenten des Interpretierens auf das Mathematische algorithmischer Analyse findet ihre Erfüllung in der Vision des »Semantic Publishing«, das Aussagen in isolierbare Einheiten formalisiert, vergleichbar den Einträgen in einer Datenbank. Der kulturwissenschaftliche Blick auf diese Entwicklung weiß, wie weit man sich damit entfernt von Humboldts Bildungsideal und Lessings Wissenskonzept, das die Bestimmung des Menschen weniger im Finden der Wahrheit sah als im Prozess der Suche nach ihr.

Die Frage, die viele umtreibt, die ein Bewusstsein haben für die kulturellen Folgen der stattfindenden technologischen Entwicklung, ist, welche Möglichkeiten dem Individuum bleiben, in diesen Prozess einzugreifen. Die Antwort beginnt mit der Erkenntnis, dass man nicht für die Mehrheit spricht. Solange etwa Google sich als Auge Gottes im Sinne der Fürsorge statt der Überwachung präsentieren kann, hat

jeder Einspruch zum Big Data Mining jene gegen sich, die von dessen Ergebnissen profitieren. Was die durch den NSA-Skandal angefachte Überwachungs- und Privacydebatte übersieht, ist eben dieses allgemeine Einverständnis: Ich will ja, dass Google alles über mich weiß, damit es seinen Kundendienst – von den personalisierten Suchergebnissen über geo-lokale Empfehlungen bis zum Hinweis, was ich als nächstes tun soll – so effektiv wie möglich erfüllen kann. Ich sehe ja ein, dass die *Smart Things* im Internet der Dinge mir nur in dem Maße Arbeit abnehmen können, wie sie – und damit alle, die Zugriff auf sie haben – über mich Bescheid wissen.

Die Disziplinierung der Geheimdienste ist der einzige gemeinsame Nenner, auf den sich die Gesellschaft noch halbwegs einigen kann. Und nicht einmal hier sind alle einer Meinung. Denn es stellt sich die Frage, warum Menschen als Staatsbürger auf eine Privatsphäre pochen, die sie als Konsument leichthin preisgeben. Wer in diesem Kontext zur Rettung des Internets vor seinem Missbrauch als Mittel der Überwachung aufruft, gemahnt zu Recht an die Hoffnungen, die man einst mit diesem neuen Medium als Ort der Emanzipation und Demokratisierung verband. Er erinnert aber auch an die heute belächelten oder vergessenen Intellektuellen, die, vor dem ausgerufenen »Ende der Geschichte«, zur Verbesserung der Gesellschaft mahnten und dem interesselosen Volk zuriefen: Es gibt kein richtiges Leben im falschen. Wie die Zeit zeigt, der Spruch mag zwar stimmen, gut leben lässt sich trotzdem im gesellschaftlichen Status quo.

Medien sind noch schwerer zu ändern als Gesellschaften, weil sie selbst verändern wollen. Sie haben neben dem Sozialen, das sie bedingt, ihren Eigensinn, mit dem sie wiederum die Gesellschaft umgestalten. Bei Computer und Internet heißt dies: Berechnen, Verbinden, Regulieren. Das Problem, vor dem wir stehen, ist die logische Konsequenz der Medienentwicklung. Zugleich radikalisiert das Big Data Mining den Vermessungsimpuls der Aufklärung, dem sich nun nichts und niemand mehr entziehen kann. Was digital passiert, produziert Daten. Deren Analyse – dies- und jenseits herkömmlicher Datenschutzkonzepte – ist nicht der ›Autounfall‹ des Datenhighways, sondern erklärtes oder akzeptiertes Ziel für viele. Data Love ist, in ihrem doppelten Sinn, die Umarmung, der man in dieser Situation kaum noch entkommt. Welche Formen sie annimmt, welche kulturellen und sozialen Nebenwirkungen sie hat und was aus philosophischer, kulturwissenschaftlicher Perspektive dazu zu denken ist, davon handelt dieses Buch.

I. Jenseits der NSA-Debatte

1. Geheimdienstlogik

Im Sommer 2013 flog der neunundzwanzigjährige IT-Spezialist Edward Snowden mit geheimen Dokumenten seiner Dienststelle, der National Security Agency der USA (NSA), ins Ausland und klärte aus dem Transitraum des Moskauer Flughafens mithilfe des *Guardian* und der *Washington Post* die Welt darüber auf, in welchem Ausmaße ihre Kommunikation im Internet und im Telefonnetz vom amerikanischen Sicherheitsdienst überwacht wird. Der Whistleblower Snowden war weit erfolgreicher als der frühere Abteilungsleiter der NSA, Thomas Drake, der aus gleichen Motiven die unverhältnismäßigen Überwachungspraktiken der NSA erst auf dem Amtsweg kritisiert hatte, bevor er sie 2010 einer Journalistin der *Baltimore Sun* verriet und dafür der Spionage angeklagt wurde. Snowdens Enthüllungen sorgten über viele Monate für internationales Aufsehen und schufen das, was die Geschichtsschreibung später als das letzte große Erweckungserlebnis der Mediengesellschaft bezeichnen sollte.

So oder ähnlich könnte ein Bericht in ferner Zukunft über die Ereignisse um den NSA-Skandal im Jahr 2013 beginnen. Der Bericht wird den Vorgang mit der gebotenen historischen Distanz bewerten, ganz


ohne die Aufgeregtheit und Enttäuschung früherer Geschichtsschreiber. Denn aus der Perspektive der Zukunft war dieses »Erweckungserlebnis« nur der letzte Aufschrei vor der Einsicht in die Notwendigkeit, einer Einsicht, die so unvermeidlich war, dass selbst der ›Aufschrei‹ schon wenig mehr als ein verhaltenes Räuspern war. Der Bericht wird den Fall mit historio-
grafischer Sachlichkeit rekonstruieren und damit be-
ginnen, wie die Mächtigen der Welt sich in dem Fall verhielten:

Die USA erklären Snowdens Reisepass als ungültig und erlassen Haftbefehl wegen Geheimnisverrat und Diebstahl. Die brasilianische Präsidentin protestiert vor der UN gegen das Ausschnüffeln brasilianischer Staatsbürger (einschließlich ihrer selbst), sagt ihr geplantes Treffen mit dem Präsidenten der USA ab und zeigt mit der Bildung einer Untersuchungsgruppe wieder Handlungsfähigkeit nach dem Trauma der *Vemprarua*-Unruhen im eigenen Land. Ecuador, dessen Londoner Botschaft seit einem Jahr WikiLeaks-Gründer Julian Assange beherbergt, stellt Snowden Asyl in Aussicht und verzichtet dafür auf Zollvergünstigungen in den USA. Deutschland lehnt Snowdens Asylantrag aus formalen Gründen ab, da ein solcher nicht aus dem Ausland gestellt werden könne. Russland gewährt Snowden Asyl für ein Jahr und provoziert damit eine weitere Abkühlung seiner Beziehungen mit den USA, die postwendend ein Gipfeltreffen zwischen Obama und Putin absagen.


Die Netztheoretiker begrüßten natürlich Snowdens Tat, weil sie der Gesellschaft eine Debatte aufzwang,

die sie längst hätte führen müssen. Zustimmung gab es allerdings nicht nur von diesen. Auch SPD-Kanzlerkandidat Peer Steinbrück und EU-Justizkommissarin Viviane Reding dankten Snowden für seine Zivilcourage und die angestoßene Debatte,³ und selbst der frühere Präsident der USA, Jimmy Carter, nahm Snowden in Schutz: Die staatliche Invasion in die Privatsphäre sei zu exzessiv gewesen, ihre Aufdeckung durch Snowden langfristig wahrscheinlich nützlich. Der aktuelle Präsident blieb solchen Überlegungen selbst dann verschlossen, als er auf der Pressekonferenz des Weißen Hauses am 11. August 2013 eingestand, dass die Arbeit des Geheimdienstes transparenter werden müsse, und die Einsetzung eines Datenschutzbeauftragten ankündigte. Der Ansicht, dass man demzufolge Snowden statt als Verräter eigentlich als Patriot behandeln müsse, widersprach Obama vehement mit einer Plausibilität, die kein Proseminar bestehen würde: »Nein, ich halte Herrn Snowden nicht für einen Patrioten«, hieß es lapidar: »Ich habe schon eine gründliche Untersuchung unserer Überwachungspraktiken angeordnet, bevor Herr Snowden diese vertraulichen Daten enthüllt hat. Ich, und ich denke alle Amerikaner, hätten eine gesetzliche, ordnungsgemäße Untersuchung dieser Enthüllungspraktiken vorgezogen.«⁴ Selbst wenn Obama Snowden im Handeln voraus war; dass dieser ihm für seine Nachfragen mindestens den Rücken stärkte, ist kaum leugbar.


Die Enthüllungen und Vorwürfe betrafen nicht nur die NSA. Ebenso war der britische Geheimdienst involviert, und auch der deutsche Bundesnachrichten-



dienst arbeitete, wie sich nach und nach herausstellte, eng mit der NSA zusammen, was nicht erstaunen sollte, immerhin kam ein Teil der Attentäter des 11. September 2001 aus Hamburg. Dass dieses Schockdatum des neuen Jahrtausends seitdem für viele staatliche Datenschutzverletzungen und Einschränkungen bürgerlicher Freiheiten herhielt, war allgemein bekannt und weithin akzeptiert. Sicherheit gegen den internationalen Terrorismus ist ohne Abstriche beim Datenschutz nicht zu haben. Das war nicht nur die Überzeugung Obamas und vieler anderer Politiker, sondern auch des Moralphilosophen Peter Singer, der Mitte 2011 in seinem Essay *The Visible Man. Ethics in a World Without Secrets* den Gewinn an Sicherheit über den Verlust an Datenschutz gestellt und Privacy als junges, vor allem westliches Phänomen in der Menschheitsgeschichte in seiner Bedeutsamkeit für das Individuum relativiert hatte. So einfach ließ sich damals mit Angst und historischem Wissen der Weg ebnen für den Transfer von einer demokratischen Gesellschaft zum Überwachungsstaat.



Wenn der zukünftige Bericht aus deutscher Feder stammt, wird er an dieser Stelle vielleicht auf Christian Heller verweisen, der zeitgleich zu Singer und unabhängig von diesem mit seinem Buch *Post-Privacy. Prima leben ohne Privatsphäre* eine Art Ratgeber für das Unvermeidliche vorlegte und damit das geschichtliche Trauma der Überwachung überwand, unter dem das kollektive Gedächtnis seiner Nation seit dem Dritten Reich und der DDR stand. Denkbar, dass der Bericht in diesem Buch die Initialzündung für die Grün-



dingung der Bürgerbewegung *Die gläsernen 90 Prozent* sehen wird, die in der zweiten Hälfte der 2010er Jahre mit immer mehr Zulauf für intensivere Sicherheitskontrollen demonstrierte, nicht bereit, das eigene Leben für das überzogene Demokratieverständnis einiger weniger zu gefährden. Die Anhänger dieser Bewegung, so wird zu lesen sein, benutzten keine Verschlüsselung in ihrer digitalen Kommunikation, installierten freiwillig den Bundestrojaner auf Computer und Smartphone und erhielten dafür einen biometrischen Sicherheitspass, der zur Benutzung spezieller Flugzeuge, U-Bahnen und Autobusse berechtigte.

Wie auch immer die Berichte aus der Zukunft ausfallen, eine solche Bürgerbewegung würde sich auf die Aussage des damaligen deutschen Innenministers Hans-Peter Friedrich (CSU) berufen können, wonach Sicherheit ein »Supergrundrecht« sei, oder auch auf den vormaligen Innenminister Otto Schily, den »roten Sheriff« der SPD, der, gerade als seine Parteigenossen sich Wahlkampfvorteile aus der NSA-Affäre erhofften, erklärte: Law und Order sind sozialdemokratische Werte und die größte Gefahr geht nicht vom Staat und seinem Geheimdienst aus, sondern vom Terrorismus und der organisierten Kriminalität.

Innenminister sind naturgemäß parteiisch über Parteilinien hinweg, wenn es um die Arbeit der Nachrichtendienste geht. Immerhin erhielten diese Dienste vom Souverän den Auftrag, genau das zu tun, wofür sie nun in der Öffentlichkeit gerügt wurden: mittels verdeckter Erkundung möglicher Risiken die Gefährdung der inneren Sicherheit abzuwehren. Dass

der Geheimdienst dazu die jeweils neuesten Technologien einsetzt – was technisch möglich ist, wird benutzt, so Innenminister Friedrich im Kontext der NSA-Affäre –, sollte niemanden überraschen oder aufregen: Der Geheimdienst will seine Effektivität ebenso sichern und verbessern wie jedes andere Funktionssystem der Gesellschaft. Spätestens seit dem 11. September träumte er deswegen vom »full take« aller Daten von allen Bürgern. Was bisher an mangelhaften finanziellen und technischen Ressourcen scheiterte, wurde mit der zunehmenden Digitalisierung der Gesellschaft reale Option, sodass manche Geheimdienstler fröhlich Hölderlin zitierten: Wo aber Gefahr ist, wächst das Rettende auch. Wer die neuen Möglichkeiten der Datensammlung und -auswertung nicht nutzt, das war Konsens in diesem Funktionssystem, begeht eine Dienstpflichtverletzung, die bei dieser Art von Arbeit im Grunde an Landesverrat grenzt.

Dass dies nicht mit dem Staatssicherheitsdienst der DDR zu vergleichen sei, wurde politisch betont: In der Bundesrepublik sei der Geheimdienst rechtsstaatlich legitimiert und parlamentarisch kontrolliert, auch wenn das nicht alle Parlamentarier so sehen und manche vom Geheimdienst mehr Transparenz fordern. Das stärkere Argument war technischer Art: Die Überwachung erfolge nicht mehr durch einen Geheimdienstler, der die Briefe und Gespräche einer Person genau liest oder anhört, sondern durch eine Software, die nur nach bestimmten Stichworten sucht. Die Überwachung sei durch die modernen Technologien zwar

flächendeckend, aber auch anonym und zudem demokratisch, indem sie nicht nur ausgewählte Personen treffe, sondern die ganze Gesellschaft, einschließlich Geheimdienstler. Für viele, so könnte der Bericht schließen, war das die perfekte Lösung des internen Widerspruchs jeder Demokratie: Während die Arbeit ihres Geheimdienstes effektiver und kostengünstiger wurde, war die Privatsphäre ihrer Bürger im *distant reading* der Maschine zusätzlich geschützt.

2. Doppelte Gleichgültigkeit

Der Skandal der NSA-Affäre lag nur vordergründig in der aufgedeckten globalen Schnüffelei des amerikanischen Geheimdienstes und in der Unterstützung, die er dabei von anderen Geheimdiensten erhielt. Skandalöser war die Hilflosigkeit der Politik und das Desinteresse, mit der sie den Fall anging. Der Bundespräsident, der als einstiger Chef der Stasi-Aufklärungsbehörde für das Thema besonders sensibilisiert sein sollte, meldete sich in dieser Sache nicht zu Wort. Die Bundeskanzlerin sprach vom Internet als »Neuland für uns alle« und versicherte, dass auf deutschem Boden deutsches Recht gelten müsse, als ließe sich das Internet mit mehr Nachdruck der nationalen Exekutive von seiner medialen Eigenlogik abbringen. Die SPD verlangte lückenlose Aufklärung, als seien die Weichen für eine effektive Zusammenarbeit mit der NSA und für Vorratsdatenspeicherungsgesetze nicht in ihrer eigenen Regierungszeit gestellt worden. An-

dere ermahnten die Bürger zu bewussterem Selbst-
datenschutz, als ginge es nur um Daten, die man frei-
willig auf Facebook und Twitter präsentiert, und als
wäre alles wieder gut, wenn Cookies blockiert, Emails
verschlüsselt und jeden Abend die Browser-Chronik
gelöscht wird. Wer sich Sorgen um seine Daten macht,
kann kaum eine App benutzen, deren Nutzungs-
bestimmungen bekanntlich keine Verhandlungssache
sind, sondern triumphal im Binärmodus des *take it or
leave it* auftreten. Selbstschutz verbaut da den
Zugang zu einer Unzahl hilfreicher, interessanter oder
einfach nur unterhaltsamer Programme. Es mag Hel-
den des Alltags geben, die sich hartnäckig weigern,
»accept« zu klicken, wenn ihnen der Hunger einer
App auf »user data« und »usage data« zu weit geht.
Wer dies standhaft hundertmal getan hat, wird sich
allerdings fragen, wozu er überhaupt ein Smartphone
besitzt, wenn er es nur zum Telefonieren benutzt.

Dennoch: Auch die Gleichgültigkeit des Großteils
der Bevölkerung war skandalös. Zwar demonstrierten
einige gegen die Überwachung durch Geheimdienste,
aber angesichts der Schwere des Vorfalls muss man
eher von einer radikalen Diskussionsverweigerung
auch auf Seiten der Bevölkerung sprechen. Die meis-
ten derer, die nicht für Überwachung waren, taten
trotzdem nichts dagegen, weil sie ja nichts zu ver-
bergen hätten. Diese populäre Beschwichtigungs-
formel ist nicht nur naiv, sondern auch unmoralisch,
wie schon eine Nachricht jener Tage über die erste
Trauung zweier Männer in einer evangelischen Kirche
zeigt. Was vor wenigen Jahrzehnten noch verboten

oder verpönt gewesen war, wurde nun gesellschaftlich anerkannt und sogar kirchlich gesegnet. Das heißt, viele, die gestern etwas verbergen – und dazu zählten vorgestern auch die Mediziner, die illegal Leichen seziierten –, waren aus heutiger Sicht schon damals keine schlechten Menschen.

Wer pauschal auf Transparenz setzt, riskiert, sich mit den geltenden Moralvorstellungen gegen die Ansprüche von Minderheiten – oder medizinische Erkenntnisse – zu verbünden. In einer demokratischen Gesellschaft, die sich der partiellen Rückständigkeit ihrer geschriebenen und ungeschriebenen Gesetze bewusst ist, sollte es Pflicht aller Bürger – eine ›Supergrundpflicht‹ – sein, das Recht des Verbergens zu schützen, indem man selbst dann darauf besteht, wenn man nichts zu verbergen hat. Nur so tritt man schon heute Verdächtigungen entgegen, die künftig jene treffen könnten, die sich – und sei es nur durch Abschaltung des GPS – der Kontrolle ihres Verhaltens entziehen. Denn auch dies gilt es zu bedenken: Die Gesetze einer Demokratie sind nie auf dem letztem Stand der Dinge und sie sind auch nie in Stein gemeißelt. Deutschlands Geschichte ist ein beängstigendes Beispiel dafür: Als deutsche Bürger einst freizügig mit ihren Daten umgingen und keinen ihrer jüdischen Vorfahren verschwiegen, ahnten sie nicht, dass sie dies einmal in den Tod führen könnte. Wissen wir, welche unserer heute unverfänglichen Daten unter künftigen Machtverhältnissen Anstoß erregen?

Naiv ist die Erklärung »Ich habe nichts zu verbergen« aber bereits unter den gegebenen Umständen.

Selbst wenn einem egal ist, ob die GPS-Daten verraten, wo man mit wem übernachtet hat, man sollte nicht glauben, die eigene Kommunikation vollends unter Kontrolle zu haben. So wie im physischen Umgang mit anderen unsere Mimik und Gestik nicht-intentional Informationen über uns vermittelt, so ist online der Mensch mehr als die Summe seiner Daten. Die verborgenen Erkenntnisse liegen in der Quersumme und im Vergleich, in den Erkenntnissen der Statistik und der Bildung von Verhaltensmustern. Die Informatiker sprechen von »virtuellen Informationen«, die sich aus der Verknüpfung physikalisch festgehaltener Informationen ergeben: »Data finds Data«. ⁵ Ein berühmtes Beispiel ist der viel zitierte Vater aus Minneapolis, der sich beim Einzelhändler Target über die Werbung für Babyartikel beschwerte, die seiner minderjährigen Tochter geschickt wurde. Target hatte eine Schwangerschaft angenommen, weil das Kaufverhalten dieser Frau den statistisch erstellten Konsummustern von Schwangeren entsprach. Wie sich zeigte, wusste Target dadurch wirklich mehr über seine Kundin als der Vater über seine Tochter. Was für den Urheber einer Information unverfänglich sein mag – die Buchbestellung bei Amazon, der Kommentar auf YouTube, die Suche nach bestimmten Begriffen mit Google oder eben der Kauf bestimmter Artikel –, ist für Big Data-Analysten der Mosaikstein eines komplexen Profils, das am Ende mehr über uns aussagen kann, als wir wissen und wollen. Der Algorithmus ist der Psychoanalytiker des 21. Jahrhunderts, der Verhaltensmuster feststellt, die bisher im Verborgenen lagen.

Ganz in diesem Sinne lautet die Werbung für den Sportschuh Nike+ mit dem eingebauten Schrittzähler: »See all your activity in rich graphs and charts. Spot trends, get insights and discover things about yourself you never knew before.«⁶ Wie kann man sein Grundrecht auf informationelle Selbstbestimmung ausüben, wenn der Analytiker Dinge ans Licht bringt, die einem selbst gar nicht bewusst waren, und dann nicht fragt, ob er diese Einsichten anderswo verwenden darf?

Wie auch immer man die Gefahrensensibilität der Bevölkerung einschätzen und bewerten mag, die Vorschläge der Gefahrenabwehr brachten nicht nur nationale oder europäische Gesetze gegen die mediale Kolonialmacht USA in Anschlag, sondern auch europäische Technologien.⁷ Auf Whistle.im, einer verschlüsselten Alternative zum populären, datenhungrigen WhatsApp-Messenger, hieß der inzwischen gelöschte Willkommensspruch im September 2013 noch: »Sichere Sofortnachrichten. Made in Germany.« Nationales Recht als Standortvorteil im Internet. Was für eine Wende gegenüber der einstigen Frontstellung des Internets gegen staatliche Institutionen! Wie selbstbewusst und ruppig begann damals John Perry Barlows *Declaration of the Independence of Cyberspace* (1996): »Regierungen der Industriellen Welt, ihr müden Riesen aus Fleisch und Stahl, ich komme aus dem Cyberspace, dem neuen Zuhause des Geistes. Als Vertreter der Zukunft bitte ich euch aus der Vergangenheit, lasst uns in Ruhe.« Nun aber erhoffte man sich Hilfe beim guten alten Nationalstaat gegen die Konzerne im Silicon Valley.

Das Thema selbst war natürlich keineswegs neu. Das Internet wird lange schon als Form des Neokolonialismus diskutiert, verschafft es doch der Technophilie des Westens und seinen Kommunikations- und Wahrnehmungsformen weltweit Geltung. So wird Langeweile, die diesseits des Carpe Diem-Dogmas kaum existierte, durch das Prinzip der permanenten Kommunikation der mobilen Medien auch anderswo zu einer Zivilisationskrankheit, und so sehen sich Gemeinschaften, die in traditionalistischen Kulturen das Leben der Individuen maßgebend bestimmen, plötzlich mit den flexiblen Freundschaftskonzepten der sozialen Netzwerke konfrontiert. Dieser mediale Neokolonialismus wird im Kontext der NSA-Debatte nun auch innerhalb der westlichen Welt lokalisiert, als Konflikt zum Beispiel zwischen deutscher Kultur und amerikanischen Technologien. Aber die Konfliktlinie verläuft nur scheinbar entlang nationaler Werte, denn es sind vorrangig die »digital immigrants«, denen deutsche Technologien mit deutschen Datenschutzbestimmungen am Herzen liegen. Die jüngere Generation wird WhatsApp mehrheitlich weiter benutzen, selbst oder erst recht, nachdem Transparenz-Apostel und Datenkrake Facebook sie Anfang 2014 für 19 Milliarden Dollar erwarb. Die Kolonialisierung, vor der im Kontext der NSA-Debatte gewarnt wird, ist – und das bezeugt nicht zuletzt ihren immensen Erfolg – im Grunde schon ein Generationskonflikt.

Es erstaunt freilich nicht, dass die öffentliche Debatte sich trotzdem ans Nationale hielt und vor allem diskutierte, inwiefern die NSA Daten deutscher Bür-

ger ausspäht und inwiefern sie dies auf deutschem Boden tut. Der Nationalstaat kann sich besser gegenüber einem anderen Nationalstaat positionieren als gegenüber einer global und viral operierenden Technologie. Als im Herbst neue Enthüllungen und anschaulichere Bilder – das Handy der deutschen Kanzlerin, die amerikanische ›Spionagezentrale‹ im Herzen von Deutschlands Hauptstadt – die NSA-Debatte zurück auf die politische Tagesordnung brachte und zu einer Sonder-sitzung des Bundestags führte, ging es daher auch dort vor allem um Deutschlands Souveränität gegenüber den USA. Zweifellos ein wichtiges Thema – ebenso wie die Frage der parlamentarischen Kontrolle des Geheimdienstes und die Angemessenheit seiner Verfahren –, mit dem man sich aber der eigentlichen Debatte entzog: über die stattfindende radikale Digitalisierung der Gesellschaft, täglich praktiziert von immer neuen Kohorten vor allem der Digital Natives.

3. *Self Tracking und Smart Things*

Wenn der Netzkritiker Evgeny Morozov in der FAZ in einem Kommentar zur NSA-Affäre die »amerikanischen Schnüffler« als »Dataholics« bezeichnet und ihre Einlieferung in eine »Big Data-Entzugsklinik« fordert, ist dies nicht mehr als ein rhetorischer Schachzug, den er selbst im Verlauf seines Artikels abschwächt und gleichzeitig radikalisiert.⁸ Morozov weiß sehr wohl, dass Snowdens Asylgeber Russland in diesem Falle den Verräter mehr liebt als den Verrat,

denn was dieser über die NSA offenbart, gilt ähnlich auch für den russischen Geheimdienst.⁹ Allerdings sind der grenzenlosen Data Love längst nicht mehr nur die Geheimdienste verfallen. Das Begehren des »full take« findet – und darin liegt das paradoxe Ver-söhnungspotenzial der Gesellschaft mit ihrem Geheimdienst – sein Pendant – und seinen Freispruch – in der Gesellschaft selbst: als eine Art Bürgerbewegung in Gestalt des Self Tracking sowie als Technologie der Zukunft in Gestalt der Smart Things.

Die Kultur des Self Tracking hat sich seit Jahren unter dem Begriff »Quantified Self« entwickelt und Produkte wie Fitbit, Digfit, Jawbones Wristband und Nike+ zur Kontrolle der Schritt- und Pulsfrequenz sowie des Bewegungs-, Schlaf- und Essverhaltens hervorgebracht. Das Gebot der absoluten Transparenz wechselt hier das Vorzeichen, indem Überwachung Selbsterkenntnis verspricht. Bemerkenswert ist zunächst der Selbstbetrug des Self Tracking-Diskurses in seiner populistischen Gestalt. »If you can measure it, you can learn to improve it«, lautet eine Auskunft zum technologiegestützten Zusammenhang von Selbstbeobachtung und Selbstoptimierung.¹⁰ Eine andere sieht zwar den Zusammenhang von Technologie und Überwachung – »If you can measure it, someone will« –, suggeriert im Anschluss – »and that somebody should be you« – jedoch irrigerweise, dass Freiwilligkeit vor Kontrolle schützt.¹¹ Man behält seine persönliche Datenhoheit natürlich nicht, indem man sich selbst vermisst und die Ergebnisse ins System auf dem Server der Anbieter einspeist. Vielmehr bestätigt diese Aus-

sage das, was Zygmunt Bauman als »zweite Revolution der Manager« beschreibt: die Beobachtung der Verwalteten wird von diesen selbst übernommen, Disziplinierung wird durch Selbstdisziplinierung ersetzt.¹² Irreführend ist auch, wenn sich Self Tracker in der Tradition des »Erkenne dich selbst!«-Orakels am Tempel von Delphi sehen,¹³ das Selbsterkenntnis als Einsicht in die eigene Unvollkommenheit und Begrenztheit meinte und keineswegs als optimierendes »Living by numbers«.

Jenseits unmittelbarer Selbstoptimierungsziele ließe sich das Self Tracking auch als Data Love der unbedingten Art beschreiben: ohne finanzielles Interesse und unmittelbaren Sinn. Was ein junger Self Tracker – »who tracks everything from his mercury levels to his vitamin D consumption« – im Jahr 2008 verkündete, gilt für andere auch und heute um so mehr: »There's so much info that it'd be a shame not to track it.«¹⁴ Wahre Liebe, um bei der Metapher zu bleiben, überwindet die Konventionen der Vernunft und entflammt selbst für abwegige Fragen – wie zum Beispiel, ob man schneller einschläft, wenn man vorher einige Minuten auf beiden Beinen steht, oder wie oft man jeden Buchstaben des Alphabets auf seiner Computertastatur tippt.¹⁵

Trotzdem wäre das Urteil, Self Tracker liebten Daten mehr als sich selbst, übereilt. Denn die »bedingungslose« Liebe für Daten jeglicher Art steht immer im Zeichen der Hoffnung auf nachträgliche Rationalisierung, wenn neue wissenschaftliche Methoden aus scheinbar nutzlosen Daten wichtige Erkenntnisse

über ihre Produzenten und die Gesellschaft generieren. Es ist diese vorbehaltliche Unbedingtheit, die dafür spricht, die kaum zu leugnende Obsession der Self Tracker nicht als bloßen Narzissmus abzutun. Ihr Datenfetischismus hat eine soziale Komponente, die sich zunächst darin ausdrückt, dass sie ihr persönliches Data Mining öffentlich machen und anderen – Mitbürgern, Soziologen, Medizinerinnen, Verkehrsplanern etc. – helfen, Mensch und Gesellschaft besser zu verstehen.¹⁶ So gesehen sind Self Tracker die Avantgarde einer außerakademischen Sozialstudie. Sie produzieren kontextspezifisch und problembezogenes Wissen jenseits bestehender Wissenshierarchien und modifizieren damit das Verhältnis zwischen Wissenschaft und Gesellschaft so wie es Wissenssoziologen seit Anfang des Jahrhunderts – selbst ohne Bezug auf Wikipedia und Self Tracking – konstatieren: Während in der Moderne bisher immer die Wissenschaft zur Gesellschaft gesprochen hat, »antwortet« nun die Gesellschaft, in Gestalt von »Laienexperten«, der Wissenschaft.¹⁷

Die andere Aussicht auf Versöhnung der Geheimdienste mit ihrer Bevölkerung sind die Smart Things bzw. das Internet der Dinge. Auch dieses Stichwort fiel – unter anderem durch Morozov – in der Debatte zu Datenschutz und Privacy im Umfeld des NSA-Skandals, hatte aber kaum eine Chance gegen neue Enthüllungen, persönliche Schicksale und zertrümmerte Festplatten. Dabei enthält das Szenario der softwareschweren Alltagsobjekte, die untereinander kommunizieren und programmierte Entscheidungen

treffen, durchaus medienwirksames Spektakelpotenzial: der Swimmingpool, der sich aufheizt, wenn im Kalender ein Barbecue eingetragen ist; der Kühlschrank, der Bestellungen aufgibt, wenn die Milch ihr Verfallsdatum erreicht hat; das Auto-GPS, das Stau-meldungen und Baustellenverzeichnisse konsultiert und automatisch die Fahrtroute anpasst. Das Internet der Dinge befreit die menschliche Intelligenz von den niederen Tätigkeiten der Situationsanalyse und Verfahrensregelung, die der Computer viel schneller und verlässlicher erledigen kann als der Mensch. Eine Befreiung für höhere Zwecke, wie es oft enthusiastisch heißt, ohne Hinweis, worin diese heutzutage liegen könnten.


Es ist eine Befreiung, die zugleich paralyisiert. Marshall McLuhan, einer der Urväter der Medienwissenschaft, nannte die Medien einst »extension of man« bzw. Organverlängerung: Erweiterung der Arme (Hammer, Pistole), der Beine (Rad, Auto), des Auges (Fernrohr, Mikroskop), des Gedächtnisses (Schrift, Fotografie). Mit dem Internet der Dinge übernimmt der Computer nun nicht mehr nur das Rechnen für uns, sondern auch das Beobachten und Auswerten unserer Umwelt (Denken). Dass die Schattenseite der Organverlängerung für McLuhan die Amputation war, wird niemanden überraschen. Wir wissen, dass die Schrift unser Gedächtnis nicht trainiert und dass unsere Beine beim Autofahren keine Muskeln entwickeln. Das Internet der Dinge hat gleich *zwei* Schattenseiten: Es macht unser Denken weniger elastisch und es arbeitet umso besser, je mehr es über uns weiß.

Der Swimmingpool bleibt kalt, wenn wir ihn nicht in unseren Kalender schauen lassen; GPS hilft wenig, wenn wir unsere Ziele verschweigen. Die Smart Things können einander nur mitteilen, was sie über uns wissen; sie können uns nur so viel an Bequemlichkeit liefern, wie wir ihnen an Informationen über uns.


Deswegen werden wir die Daten, die wir nicht beim Geheimdienst wissen wollen, den Global Player des Internets trotzdem geben. Denn schon heute klingt es für die meisten nicht wie eine Bedrohung, sondern wie ein Versprechen, wenn Google bemüht ist, immer genauer unsere Verhältnisse, Interessen und Aufenthaltsorte zu wissen, um jederzeit passende Empfehlungen über Restaurants, Geschäfte, Sehenswürdigkeiten und potenzielle Lebenspartner in der Nähe aufs Handy spielen zu können. Mit der Aussicht auf bequemeres Informationsmanagement wird schließlich auch eine Überwachungstechnologie wie Google Glass gesellschaftlich salonfähig werden. Das Problem der Überwachung ist nicht vorrangig ein politisches oder ökonomisches (das ist es auch), sondern ein technologisches, philosophisches und anthropologisches. Morozov nennt es die »Ideologie des Datenkonsums«. Diese Ideologie – das ist der eigentliche Skandal – hat über die Geheimdienste hinaus alle erfasst.

4. Datenumweltkatastrophe

Der Paradigmenwechsel von der Verborgenheit zur absoluten Transparenz des individuellen Lebens, so




wird es in den Geschichts-→Büchern der Zukunft heißen, vollzog sich nicht nur im Zeichen der Vermessung, sondern auch der Vernetzung. Das Internet der Dinge, so wird man lesen, war der Triumph künstlicher Intelligenz und menschlicher Bequemlichkeit über die verbliebenen Datenschutzbemühungen des frühen 21. Jahrhundert. Es zog die Dinge und Aktionen zusammen und erleichterte durch Kontrolle das Leben der Menschen. Seine immense Datenakkumulation war ein Paradies für all jene, die sich für menschliches Verhalten im großen Stile interessieren: Soziologen, Werbefachleute, Versicherungen, Mediziner, Verkehrsregler, Stadtplaner, Polizisten und andere Sicherheitsbeamte. Das beunruhigte zwar die Datenschützer, aber die Mehrheit kooperierte längst mit den staatlichen und kommerziellen Datensammlern. So wie sie für wenige Cent im Supermarkt per Rabattkarte Einblick in ihr Kaufverhalten erlaubt hatte, so ›verkaufte‹ sie nun ihre digitale Kommunikation. Und zwar nicht nur, wenn es dafür Online-Dienste gratis gab. Auch auf GPS wollte man nicht mehr verzichten. Auch nicht, als es Geld kostete. Selbst Google Glass war ein großer Erfolg, vielleicht weil es jeden in das Zentrum einer kleinen Überwachungszentrale setzte und vergessen ließ, dass dies vor allem geschah, um das Überwachen überwachen zu können. Irgendwann hatten sich die meisten sogar den »intelligenten Mülleimer« angeschafft, der nicht mehr im Zeichen der Selbstoptimierung oder des Informationsmanagements stand, sondern der gouvernementalen Kontrolle ordentlichen Recyclens diente.¹⁸





Die Distanz der Geschichtsschreibung wird die historischen Etappen der Entwicklung erkennen und der eigenen Zeit gutschreiben. Sie wird auf den Holländer Alex van Es verweisen, einem Vordenker des Self Tracking, der schon 1998 den Inhalt seines Mülleimers mittels Barcode-Scanner auf der Website icepick.com veröffentlichte; ein Beleg dafür, dass keine Obsession des Data Minings absurd genug sein kann, um nicht alsbald kommerziell umgesetzt zu werden. Man wird zugleich daran erinnern, dass die Idee der Überwachung noch vor ihrer Hollywood-Version in Peter Weirs *Truman Show* (1998) von der künstlerischen Avantgarde angedacht worden war, in Fernand Légers Idee für einen Film, der 24 Stunden lang das Alltagsleben eines Mannes und einer Frau ohne deren Wissen aufnimmt (1931), und in Dan Grahams Projekt *Alteration of a Suburban House* (1978), das die Wand eines Einfamilienhauses durch Glas ersetzen und somit das Leben dieser Familie auf die Bühne der Nachbarschaft bringen sollte. Ein Beleg dafür, wie sehr Kunst, Kommerz und Kontrolle miteinander verquickt sind. Dass die Benutzer des intelligenten Mülleimers, der sich in den 2020er Jahren allgemein durchsetzte, einen Discount für die Müllabfuhr bekamen, wird die Geschichtsschreibung ebenso erwähnen wie den Antrag der *90 Prozent*-Bewegung, den Nichtteilnehmern am »Smart Bins Save City«-Programm den Sicherheitspass zu entziehen.

Vor dem Hintergrund dieser kulturhistorischen Tatbestände ist Morozov wohl zuzustimmen, dass die Kommerzialisierung von Daten sich nicht durch ein




Gesetz verhindern lässt, wenn sie im Einklang mit dem Wunsch der Bürger geschieht. Die Debatte nach Snowdens Enthüllungen umkreiste entsprechend die Frage, wie sich verhindern lässt, dass Internet-Unternehmen und Geheimdienste zusammenarbeiten. Morozov nannte dies den Griff nach den »niedrig hängenden Trauben«: Ein Verblendungsmanöver der Politik, das unterstellt, der kommerziell gesammelte Datenvorrat könne dem Zugriff staatlicher Institutionen entzogen werden. Kaum zu glauben, dass die Politik diese Selbstentmachtung gegenüber dem Kommerziellen zulassen würde. Immerhin garantieren ihr intime Kenntnisse über das Leben der Bürger eine effizientere Erfüllung ureigener Aufgaben: Senkung der Ausgaben im Gesundheitswesen durch Früherkennung von Krankheitsmustern und Präventivmaßnahmen bei offensichtlichem Fehlverhalten, Bekämpfung von Steuerhinterziehungen und Sozialleistungsbetrug durch Detailwissen über das Kaufverhalten der Bürger, bessere Verkehrsflusssteuerung durch Analyse von Bewegungsmustern, bessere Stadtplanung durch genauere Kenntnis der Raumnutzung, besseres Energiemanagement durch Auswertung von Energieverbrauchsmustern, selbst die Bildungspolitik lässt sich besser koordinieren mit Einblicken in individuelle Interessen- und Verhaltensmuster.




Kein Staat hat etwas dagegen, mehr über seine Bürger zu wissen. Im Gegenteil, jeder Staat wird von den Daten profitieren wollen, die durch kommerzielles oder idealistisches Tracking und Data Mining zur Verfügung stehen. Wie wenig man von seiner Regie-






rung in Sachen Datenschutz erwarten kann, zeigte nicht zuletzt der 28. Juni 2012, als im Deutschen Bundestag das neue Meldegesetz beschlossen wurde, das dem Staat erlaubte, die Daten seiner Bürger an Unternehmen in der Werbe- und Auskunfteibranche zu verkaufen, wenn diese keinen ausdrücklichen Widerspruch einlegten. Der Beschluss wurde in einem fast leeren Saal des Parlaments als Tagesordnungspunkt 21 kurz vor 21 Uhr gefasst – also kurz nach Beginn des EM-Halbfinals Deutschland–Italien. Die Entscheidung fiel zwar knapp aus und wurde nach dem Protest von Datenschützern später annulliert. Dass eine Mehrheit von zwei, drei Politikern ein solches Gesetz auf den Weg bringen kann, tröstet aber keineswegs, und es bleibt die Frage: Was, wenn der Staat beim nächsten Versuch die Bürger am Geschäft beteiligt?



Ist der Datenschutz besser aufgehoben im Bereich der Wirtschaft? Es mag so erscheinen, weil hier das primäre Ziel nicht Kontrolle oder moralische Wertung ist, sondern der Verkauf – ganz gleich welche seltsamen Bedürfnisse der genaue Blick zu Tage führt. Genau aus diesem Grund ist die Wirtschaft auch neugieriger als der Geheimdienst, der sich nur für Gefahrenpotenziale interessiert. Auf jeden Fall ist sie genauso wie er an Echtzeitanalysen der sozialen Medien, der Online-Kommunikation insgesamt sowie des Offline-Verhaltens interessiert. Das Marketing schwärmt im Zeitalter der totalen Überwachung ebenso wie der Geheimdienst vom »full take« und träumt von der Vernetzung zwischen Produkt und Konsument: Der Supermarkt weiß durch GPS-Datenauswertung nicht



nur, welche Wege ich zwischen den Regalen nehme, er weiß durch biometrische Erfassung auch, dass ich den einen Käse für einen anderen, fettreduzierten, wieder zurück ins Regal gelegt habe, und lenkt fortan durch entsprechende Beleuchtung die Aufmerksamkeit auf kalorienarme Produkte, deren elektronisch angezeigte Preise nach Erkenntnis meiner Diätproduktaffinität natürlich jeweils nach oben korrigiert werden. Marketingspezialisten lieben Big Data und das Internet der Dinge, weil so das Konzept der Segmentierung zur radikalen Personalisierung verfeinert werden kann, denn was sind schon Adressenanbieter gegen die Möglichkeit des gläsernen Kunden: »Der Daten-Imperativ lautet: Wisse vieles, besser alles über deine aktuellen und potenziellen Kunden, dann kannst du bessere Angebote machen, die attraktiver sind und exakter passen. Die Folge: mehr Absatz, mehr Umsatz, mehr Gewinn.«¹⁹

Der gläserne Kunde ist immer auch ein gläserner Bürger. Aus dieser Einsicht resultiert Morozovs Sorge, die Wirtschaft könne vom Staat zur Kooperation gezwungen werden. Deswegen setzt Morozov auf mehr als staatliche Gesetze zur Regulierung von IT-Unternehmen. Ihm geht es um das Bewusstsein des Einzelnen. Vergleichbar mit der Umweltbewegung gelte es, die »Datenkatastrophe« zu vermeiden: Denn so, wie es irgendwann keine Privatsache mehr war, dass man eine hohe Energierechnung problemlos bezahlen kann, da der Energieverbrauch ökologische Folgen für alle hat, so habe unser Umgang mit persönlichen Daten eine ethische Dimension. Morozov denkt da-

bei gar nicht an die extrospektive Variante des Self Tracking, wenn Daten gesichert und bereitgestellt werden, die auch andere betreffen (per Kamera, Audio-recording oder Personentagging in sozialen Netzwerken). Schon die introspektive Form – die Bereitstellung persönlicher Daten für Versicherungen: Autofahrstil, Konsumgewohnheiten, körperliche Bewegung etc. – sei keine Privatsache: Sie hat einen Effekt auch für jene, die unter dem mit diesen Daten errechenbaren Durchschnitt liegen oder den Nachweis ihrer Durchschnittlichkeit nicht erbringen wollen, und deswegen keinen Discount erhalten oder eben künftig mehr zahlen müssen. Jeder Kauf eines intelligenten Mülleimers setzt jene unter Druck, die noch nicht mit der städtischen Müllabfuhr kooperieren. Die persönliche Freizügigkeit mit Daten, so Morozovs Warnung, setzt Maßstäbe, denen sich andere nicht entziehen können.

Diese Perspektivierung liegt nahe an jener »Ethik der Fernverantwortung«, die der Technikphilosoph Hans Jonas 1979 gefordert hatte: ein Bedenken der Folgen meiner Handlungen, selbst wenn sie nicht mehr mich oder mein unmittelbares Umfeld betreffen sollten.²⁰ Zugleich zeigt Morozovs Zugriff auf das Überwachungsproblem, wie kompliziert das Thema ist, wenn man sich wirklich darauf einlässt.²¹ Denn diese Perspektive macht Opfer zu Tätern und lässt wenig Spielraum für den üblichen Ruf nach Gesetzen. Kein Wunder also, dass andere Morozovs Hinweis auf ein strukturelles Problem der Informationsgesellschaft lauthals ins Politische entschärfen: Die Totalüber-

wachung sei eine Kränkung der Demokratie, mündige Bürger würden behandelt wie unmündige Kinder, der Protest solle sich nicht an der Umweltbewegung orientieren, sondern am Widerstand gegen die Notstandsgesetze in den 1960er Jahren. Diese politische Gewichtung wiederholt der einstige FDP-Innenminister Gerhart Baum: »Es fehlt eine Bürgerbewegung zum Schutz auf Privatheit, so wie es eine solche zum Schutz der natürlichen Lebensgrundlagen gab und gibt.«²² FAZ-Herausgeber Frank Schirrmacher hingegen bestand darauf, dass der Schrecken der Snowden-Affäre nicht aus »geheimen technologischen Überwachungsunikaten« resultiert, »sondern daraus, dass sie die gleichen Logiken, Systeme, Formeln und Maschinen benutzen, die unseren Alltag und unsere Arbeitswelt bestimmen«. Die Verschmelzung zwischen den Silicon Valley-Giganten und dem Geheimdienst, so Schirrmacher an anderer Stelle mit Verweis auf GPS, kommt nicht als Orwell, sondern »über Dinge, die uns sogar Freude machen«.²³ Diese Verquickung zwischen dem, was wir fürchten, und dem, was wir wollen, ist das eigentliche Problem, das Politik und Bevölkerung aporetisch lähmt.


Aus diesem Grund ist allerdings Morozovs Vergleich zwischen Umwelt- und Datenkatastrophe letztlich methodisch unsauber. Diesen Vergleich ziehen zwar auch andere, indem sie die Rolle der Daten in der Informationsgesellschaft nicht wie die eingangs zitierte *Data Love*-Konferenz mit der Funktion der Elektrizität für das industrielle Zeitalter beschreiben, sondern mit der viel inflationärer Formel, dass Da-

ten das neue Öl seien. Diese Metapher ist so schlecht wie die der Elektrizität – Daten verbrauchen sich nicht durch Gebrauch – und zugleich ehrlicher, weil sie auf zwei Probleme im Umgang mit dem Rohstoff Öl hinweist: die Verschmutzung der Umwelt durch Unfälle und normale Nutzung. Diese beiden Probleme lassen sich ebenso für den Rohstoff Daten annonciieren: Daten können ungewollt in die Umwelt austreten (zumeist durch Hacks, mitunter durch Achtlosigkeit) und sie beeinflussen die Umwelt negativ schon durch Verwendung (so Morozov und andere). Zum Schutz der Umwelt vor Ölverschmutzung wurden Regeln erlassen, die es nun gegen Datenverschmutzung zu schaffen gelte: Wie der Oil Pollution Act Schiffen hohe Sicherheitsvorkehrungen abverlangt, so könnte dies auch Unternehmen auferlegt werden, die mit Daten handeln – der neue Schlüsselbegriff lautet »clean data technologies«.²⁴ Das methodische Problem dieser Analogie liegt in ihrer Voraussetzung, dass eine Umweltkatastrophe mit einer kulturellen Revolution vergleichbar sei.

Denn das Prinzip der *Shifting Baseline*, das aus dem Diskurs der Umweltkatastrophe kommt, bedeutet im Kontext der Datenkatastrophe nicht die Zerstörung der Lebensgrundlage künftiger Generationen, sondern deren Veränderung. Diese Veränderung stellt zwar viele der bisher geltenden Werte des gesellschaftlichen Zusammenlebens infrage, ihr Katastrophenswert aber bleibt – anders als bei Klimaerwärmung und Luftverschmutzung durch den Gebrauch fossiler Brennstoffe – ungeklärt. Während man dem Nein der

Umweltbewegung zum (biologischen) Nichtsein des Menschen kaum widersprechen kann (Streitpunkt ist nur die Dringlichkeit des Appells), entkommt das Nein zum (kulturellen) Anderssein nicht dem Verdacht, die kommende Generation auf die eigene (kulturpessimistische) Weltsicht verpflichten zu wollen.²⁵ Bewahrungsethik steht, wenn sie kulturell ausgerichtet ist, unter stärkerem Legitimationsdruck als im Falle der Umweltkatastrophe. Sie hat dann nicht nur die Realität der Bedrohung nachzuweisen, sondern auch deren Bedrohlichkeit – und gegen das Argument zu bestehen, dass radikale Umbrüche der Kultur unverzichtbarer Teil der Kultur der Moderne sind.

Die Datenkatastrophe verlangt eine Diskussion, die zum einen tiefer greift als auf die Frage, wie sich das Briefgeheimnis unter den Bedingungen der Digitalisierung aufrechterhalten lässt, und zum anderen nicht durch naheliegende Analogien von weitergehenden Aspekten des Problems absieht. Man muss diese ›Katastrophe‹ verstehen als Indikator eines gesellschaftlichen Mentalitätswechsels, der vor allem von den Digital Natives getragen wird. Dass diese so wenig Anstoß nehmen am Verlust der Privatsphäre, mag für viele – und vor allem für Vertreter der älteren Generation – als Ausdruck von Ignoranz und Gleichgültigkeit erscheinen. Aus sozialpsychologischer Perspektive ließe sich der mangelnde Protest aber auch als Emanzipationsversuch verstehen. Als Sehnsucht nach einem Raum, der Privates und Öffentliches nicht mehr unterscheidet. Als Rebellion gegen die Eltern und Großeltern, deren einstige Kulturrevolution der Ver-



öffentlichung des Privaten mithilfe der neuen Medien radikal weitergeführt wird. Diese Rebellion ist zum einen sehr erfolgreich, wie die Klage der Älteren über die Gleichgültigkeit der Jungen zeigt. Zum anderen kann sich diese Sehnsucht auf historische Vorbilder berufen, denn im frühen 20. Jahrhundert wurde der gläserne Mensch nicht nur von kommunistischer Seite gegen die bürgerliche Kultur ins Feld geführt, sondern auch von der westlichen Avantgarde.²⁶ Die Leitsätze dieser Kultur – Georg Simmels Erklärung »Das Geheimnis ist eine der größten Errungenschaften der Menschheit«, aber auch Peter Handkes Bekenntnis »Von dem, was die anderen nicht von mir wissen, lebe ich« – verlieren unter dem Transparenz- und Mitteilungsgebot der digitalen Kultur ihre Geltung. Ganz zu schweigen davon, dass sie sich als unpraktikabel erweisen, wenn es um die Versprechen der intelligenten Gegenstände und Umgebungen geht. Überwachung und Kontrolle sind aus dieser Perspektive nur die gesellschaftliche Nutzbarmachung der radikalen Transparenz, die auf sozialen Netzwerken seit langem propagiert und praktiziert wird.

Festzuhalten bleibt: Die Datenkatastrophe ist – so sehr sie auch über das reduzierte Problembewusstsein des Abhörskandals hinausgeht – als existenzielles Thema weniger bedrohlich und als ethisches weniger eindeutig als die Umweltkatastrophe. Vielleicht verpuffte deswegen Morozovs Appell, die moralischen Konsequenzen unserer datenspezifischen Ignoranz, Vorteilsbeschaffung und Selbstlosigkeit zu bedenken. Vielleicht schickte man deswegen lieber den mün-



digen Bürger gegen den unterdrückenden Staat in den Ring, was umso plausibler war, nachdem die britische Regierung ihren Geheimdienst in die Büros des *Guardians* gesandt hatte, um dort Festplatten mit Snowdens Informationen zu zerstören. Mit diesem rein symbolischen Machtakt – kein Geheimdienst, der den Namen verdient, glaubt, im Zeitalter der digitalen Kopierbarkeit ließen sich unerwünschte Daten durch materielle Gewalt vernichten – schloss sich der Kreis medienstrategisch dort, wo alles begonnen hatte: Bei Edward Snowdens ›Verrat‹. Den haben viele zwar zu Recht eher als Erweckung und Anstoß einer notwendigen Debatte betrachtet, zumeist aber nicht über die Tragweite hinaus, die Snowden selbst seinen Enthüllungen zugestand. Es ist leicht zu verstehen, warum.



5. Kalter Bürgerkrieg

Der Bericht, der aus der historischen Distanz die Vorfälle um die NSA-Affäre und Snowdens Verrat bezeugen würde, wird Snowden zu den ambivalenten Helden der Geschichte zählen. Ein ambivalenter Held, nicht, weil seine Tat selbst unter den Präsidenten der USA unterschiedlich bewertet wurde, sondern, weil sein für viele zweifelloses Heldentum von einem romantisch verklärten Gesellschaftsverständnis getragen war. Er habe der Welt Kunde von den Schnüffelprogrammen geben wollen, damit sie die Chance erhalte, etwas dagegen zu unternehmen. Ein Aufklärer und Wegbereiter für Change also, der keinen Zweifel



hat, dass sein moralisches Gewissen ihn von allen Amtseiden entbindet, die sich der Wahrheit in den Weg stellen. Ein Märtyrer, der im Dienst des öffentlichen Wohls das eigene Leben riskiert und dafür 2014 den ersten Positiv-Preis der vom Bielefelder Verein digitalcourage verteilten BigBrotherAwards erhielt. Und in der Tat: Snowden ist eine aktuelle Ergänzung zum David-gegen-Goliath-Mythus, ein Beleg für die Macht des Individuums gegenüber dem mächtigsten aller Staaten, ein Beispiel dafür, dass außerhalb des akademischen Systems Diskurse, an deren Gründung kritische Wissenschaftler seit Jahren eifrig und mit vergleichsweise geringem Erfolg arbeiten, viel nachdrücklicher etabliert werden können.


Die Ambivalenz von Snowdens Heldentum liegt nicht im Optimismus, mit dem Snowden an das Gute im Menschen glaubt, sondern im Besitzanspruch, mit dem er das Internet behandelt. Der Gestus zeigt sich schon im Titel seines TED-Talks im März 2014: »Here is how we take back the Internet.« Wer spricht da? Wie viele sind das? Woher nehmen sie das Recht, das Schicksal eines Mediums bestimmen zu wollen? Die Rückforderung mag plausibel klingen und die Nachfragen absurd, wenn man das Problem des Datenschutzes auf die Schnüffelei der Geheimdienste reduziert. Betrachtet man es im Kontext der »Ideologie des Datenkonsums« als Teil einer gesellschaftlichen Entwicklung, stellt sich aber die Frage, mit welchem Mandat – und welcher Aussicht auf Erfolg – einige Aktivist:innen die Entwicklungsrichtung eines Mediums, das ihnen nicht allein gehört, vorgeben wollen. Um Miss-

verständnis zu begegnen: Diese Frage zielt auf die Logik der Argumentation und steht nicht für die Ablehnung der vorgebrachten Forderungen. Im Gegenteil, der Wunsch ist, das Problem würde radikaler angegangen werden, mit der oben skizzierten Konsequenz, an seinen kulturellen und gesellschaftlichen Wurzeln anzusetzen. Dass dies nicht geschieht, dass der Diskurs an der Oberfläche bleibt und gar von denen Hilfe erwartet, die – als Softwareentwickler und Data Miner – die Ideologie des Datenkonsums verinnerlicht haben und mit ihren Produkten predigen, das macht die Ambivalenz von Snowdens Heldentum aus.

Man kann natürlich nicht ausschließen, dass einige Softwareentwickler durch den von Snowden angestoßenen Diskurs für Fragen des Datenschutzes sensibilisiert werden und bei der nächsten App, die sie schreiben, von der unnötigen Abfrage bestimmter Nutzerdaten absehen. Es ist durchaus möglich, dass auf diese Weise Privacy über geschäftliche Erwägungen der Datenakkumulation gestellt wird. Angesichts der Rolle, die Big Data als Wirtschaftsfaktor zunehmend spielt, ist jedoch nicht zu erwarten, dass viele Start-ups auf diese Weise freiwillig Nachteile gegenüber ihren Konkurrenten eingehen. Es sei denn, die Zurückhaltung in der Datenabfrage bringt Wettbewerbsvorteile bei den Kunden. Darin liegt das Potenzial des angestoßenen Diskurses: dass sich im Bereich der digitalen Medien ein Parallelmarkt entwickelt, der den Schutz der Daten seiner Kunden über die Gewinne stellt, die man mit diesen Daten machen könnte.

Ein ›Bio-Markt‹ des Internets gewissermaßen, dessen Produkte entsprechend teurer wären – so wie Gemüse ohne Pestizide und Fleisch von glücklichen Hühnern. Ein solcher Markt untergräbt die politisch heiß umkämpfte Netzneutralität – die Datenübertragung unabhängig von Form, Inhalt, Absender oder Ansehen und Kaufkraft des Empfängers – freilich von einer bisher nicht beachteten Seite und könnte deswegen wiederum Netzaktivisten gegen sich haben. Die Problematik, die in diesem Zweiklassen-Internet zweifellos liegt, übersteigt allerdings nicht den Problempegel des geteilten Lebensmittelmarktes. Im Gegenteil, während bei Lebensmitteln nur aus ökonomischen Zwängen nicht alle sich für die sichereren Produkte entscheiden, kann dies auf dem Markt der Applikationen auch aus Gleichgültigkeit oder Überzeugung geschehen. In jedem Falle müsste die Diskussion zu eben diesen ökonomischen und ideologischen Fragen vorstoßen, statt bei der von Snowden vorgegebenen rechtlichen Konfliktlage stehen zu bleiben.

Die Grenzen, in denen sich die angestoßene Debatte bewegt, illustriert eine Umfrage der *ZEIT* unter Netzspezialisten zur Frage »Ist das Internet noch zu retten?«²⁷ Die Antworten sind voller Kampfgeist und zeigen nur gelegentlich eine tiefere Einsicht in die eigentliche Problemlage. So erklärt Markus Beckedahl, Betreiber des Blogs *netzpolitik.org* und Mitveranstalter der wichtigen Konferenz *re:publica*: »Es geht um nichts Geringeres als unsere digitale Zukunft mit den Grundwerten und Grundrechten, die wir kennen und lieben gelernt haben.« Mit gleicher Ausrichtung



mahnt Anke Domscheit-Berg, Netzaktivistin und Spitzenkandidatin der Piratenpartei für die Bundestagswahl: »Wir können uns mehrheitlich weiter blind und taub stellen und uns dann in einer Welt wiederfinden, in der wir versuchen, unseren Kindern zu erklären, was ein freies Internet einmal bedeutete und wie mit seinem Ende auch viele andere Freiheiten für immer verschwanden. Wir können uns aber auch machtvoll erheben und das Internet – so wie wir es kannten – mit Zähnen und Klauen zurückerobern.« Liebe, Zähne, Klauen – ein ehrenwerter Protest gegen den Gang der Dinge, der allerdings ignoriert, wie sehr schon das frühe Internet mental seine aktuelle Struktur in sich trug. Die alte, inzwischen von den meisten Netztheoretikern aufgegebenene Hoffnung auf das Internet als Ort befreiter und befreiender Kommunikation beruhte von Anfang an auf dem Missverständnis, das Internet ohne den Computer zu denken. Man betonte die Möglichkeiten der Vernetzung und übersah das Postulat des Rechnens, das der Computer der Situation der Menschen auch und umso mehr aufdrängt, wenn er sich mit anderen Rechnern verbündet. Vernetzte Computer wollen genauso alles vermessen und berechnen, wie sie alles kopieren wollen. Was das Kopieren betrifft, heißt deswegen die Antwort für viele, und vor allem für die Netzaktivisten, sich von den Copyright-Regeln der analogen Welt zu verabschieden. Die Vermessung ist das O zum A; auch hier hilft es wenig, sich an bisherige Gepflogenheiten zu klammern.

Weit sachbezogener und resignierter fällt deswegen die Antwort von Viktor Mayer-Schönberger aus, Ko-

autor des Buches *Big Data: Die Revolution, die unser Leben verändern wird*: »Im Kern ist das die neue Aufgabe von Regierungen – die umfassende, auf Information basierende, voraussehende Steuerung der Gesellschaft. Dabei sind Regierungen Nachzügler. Sie folgen den Unternehmen wie Google und Facebook und Organisationen wie Wikipedia (und WikiLeaks!), die das längst erkannt haben. Das ist nicht das Ende, sondern erst der Anfang.« Kybernetik, da helfen auch Zähne und Klauen nicht, war schon immer das Tarnwort für Kontrolle, der das Internet – der Menschen und der Dinge – immer mehr Bereiche des menschlichen Lebens zuführt. Dass Regierungen zur effektiveren Erfüllung ihrer Aufgaben von den neuen Möglichkeiten Gebrauch machen, liegt auf der Hand und wird in der politischen Diskussion kaum infrage gestellt. Dort geht es zumeist nur noch darum, dass das Data Mining transparent und demokratisch erfolgt: Die Instrumente sollen gezeigt werden (mit dem willkommenen Nebeneffekt der Selbstdisziplinierung), und sie sollen jedem zugänglich sein (was angesichts der Kosten komplexer Datenanalysen kaum zu realisieren ist).²⁸

In seinem *Postskriptum über die Kontrollgesellschaften* illustriert der französische Philosoph Gilles Deleuze die künftige Stadt, »in der jeder seine Wohnung, seine Straße, sein Viertel dank seiner elektronischen (dividuellen) Karte verlassen kann, durch die diese oder jene Schranke sich öffnet«. Diese Prognose wird zwanzig Jahre später konkret durch Produkte wie den NFC-Ring, der als Schlüssel wirkt, oder das Nymi

Wristband, das die persönliche Pulsfrequenz als Identifikationsmittel nutzt. Konkret wird damit zugleich, was für Deleuze den dystopischen Teil seines Szenarios ausmacht: »Aber die Karte könnte auch an einem bestimmten Tag oder für bestimmte Stunden ungültig sein; was zählt, ist nicht die Barriere, sondern der Computer, der die – erlaubte oder unerlaubte – Position jedes einzelnen erfasst und eine universelle Modulation durchführt.«²⁹ Auch wenn IBM in Rio de Janeiro einen Kontrollraum gebildet hat, in dem alle Überwachungskameras zusammenkommen, und auch, wenn China ähnliche Kontrollräume für seine neuen Städte baut, man sollte die Zukunft nicht durch alte Feindbilder beschönigen. Es wird am Ende keine Big Brothers geben, die man aus ihrer Schaltzentrale zerrren könnte. Es wird keine Kontrolleure aus Fleisch und Blut geben, die die Karten freischalten oder sperren. Die Karten werden Algorithmen gehorchen, gefüttert mit Millionen von Daten, die wir selbst ihnen überlassen haben. Der Begriff dafür ist bereits auf dem Markt: *algorithmic regulation*. Sein Geistesverwandter ist *datafication*, die Transformation von Kommunikationen und Aktionen in tabellarisierbare, quantifizierbare Daten. Der in der politischen Philosophie annoncierte Übergang von der Disziplinar-gesellschaft zur Kontrollgesellschaft vollzieht sich durch die Digitalisierung der Gesellschaft, wobei die Datafication den effektiven Zugriff im Modus der Kybernetik garantiert.

Ein anderer, älterer Zweig der politischen Philosophie hat die Umstellung der Gesellschaft auf die Lo-

gik der Kybernetik bereits vor über 45 Jahren unter dem Stichwort »technokratische Rationalität« problematisiert. Diese ersetze perspektivisch den autoritären Staat, was zugleich einen Wechsel in die Diskussionslosigkeit bedeute: Denn die normativen Regelungen der Gesellschaft werden dann nicht mehr in umgangssprachlicher Kommunikation verhandelt, sondern zweckrational und scheinbar ideologiefrei gesetzt. Die bürgerliche oder sozialistische Ideologie, die ihre Ziele zumindest begründen musste, weicht der »Ersatzideologie« von Technik und Wissenschaft als »Selbstverdinglichung der Menschen unter Kategorien zweckrationalen Handelns und adaptiven Verhaltens«. ³⁰ Das Problem, das Jürgen Habermas im Anschluss an Max Webers und Herbert Marcuses Rationalismuskritik sieht, ist die Entwicklung der Rationalität von einem Mittel der Emanzipation des Menschen zu einem Mittel seiner Verdinglichung. Diesen Aspekt des Modernisierungsprozesses haben unter anderem Max Horkheimer und Theodor W. Adorno in ihrer *Dialektik der Aufklärung* und Zygmunt Bauman in seiner *Dialektik der Ordnung* beschrieben. Jeweils schafft die instrumentelle Vernunft – wenn auch auf unterschiedlichen Grausamkeitsstufen – eine Situation ›moralischer Erbarmungslosigkeit‹, in der Menschen bestehende Regeln nicht mehr verantworten, aber auch nicht infrage stellen, sondern mit hehrem Pflichtgefühl befolgen und durchsetzen. Die Adia-phorisierung – so das Fachwort der Ethik, wenn Menschen sich für die Folgen ihrer Handlungen nicht zuständig fühlen – erübrigt sich (bzw. verbirgt sich am

Backend des Interface), wenn nicht mehr der Mensch, sondern der Algorithmus (als neuer, perfekter »Bruder Eichmann«) die Regeln aufstellt und durchsetzt.

Bauman hat die Gefahr angesprochen, moralische Zuständigkeit an technologische Entwicklungen auszulagern: »Heute entwickeln wir Technologien nicht mehr, ›um zu‹ tun, was wir tun wollen, sondern wir tun einfach das, was irgendeine inzwischen entwickelte (oder besser: zufällig oder ›glücklicherweise‹ entstandene) Technologie möglich macht.«³¹ Die Fragen, woher die Technologien kommen, die uns die Parameter unseres Handelns vorgeben, und welche Einheit dabei Erfindungsgeist und Gewinnstreben junger Programmierer bilden, werden uns noch beschäftigen. Zunächst sei nochmals auf Jonas hingewiesen, der drei Jahrzehnte vor Bauman vor der Macht des technisch Möglichen gewarnt hatte. Für ihn lag das Verhängnis des Menschen im »Triumph des *homo faber*«, der ihn zum »willenlosen Vollstrecker seines Könnens« macht: »Wenn nichts so gelingt wie das Gelingen, so nimmt auch nichts so gefangen, wie das Gelingen.«³² Diesem technischen Gelingen – und der moderne Begriff dafür heißt Computieren, Programmieren, Algorithmen – sind wir mehr denn je verfallen. Wenn im Kontext der NSA-Affäre auf Demonstrationen im Sommer 2013 »YES WE SCAN«-Plakate erschienen, drückten diese zum einen durch Verweis auf dessen Wahlkampfspruch YES WE CAN Enttäuschung über Präsident Obama aus. Die Überlappung beider Sprüche – we scan because we can – artikuliert zugleich genau jenen fatalistischen Aktivismus, der nicht nur

für Jonas und Bauman das Verhältnis der Moderne zur Technologie kennzeichnet: Ja, wir können alle möglichen Daten sammeln und auswerten, und also tun wir es auch. Der »full take«, auf den die Geheimdienste zielen, ist kein Widerspruch zur modernen Gesellschaft, sondern Teil ihrer Widersprüchlichkeit. Die Kontrollgesellschaft und die »Kultur der Kontrolle«³³ sind Konsequenzen des Modernisierungsprozesses, der alle verfügbaren Technologien nicht zuletzt im Dienste einer immer effektiveren Organisation und Kontrolle gesellschaftlicher Strukturen und Prozesse einsetzt.

In dieser Widersprüchlichkeit der Moderne sind auch ihre machtloseren Bewohner verfangen. Es wurde am Beispiel des Self Tracking und der Smart Things vermerkt, dass pragmatische Erwägungen im Zeichen der Bequemlichkeit und des Erkenntnisdranges zur freiwilligen Datenpreisgabe führen. Der mangelnde Aufschrei der Bevölkerung angesichts des NSA-Skandals findet aber auch andere Erklärungen: »Sehnsucht nach Überwachung« im Sinne der Fürsorge in einer unübersichtlich gewordenen Moderne und »Lust am Gesehenwerden« im Sinne eines »Ich werde gesehen (beobachtet, bemerkt, erfasst), also bin ich«.³⁴ Beide Motive – der Exhibitionismus als Selbstversicherung und der Ordnungswille als Komplexitätsreduktion – sind psychologisch nachvollziehbar und machen – ebenso wie Erkenntnisdrang und Bequemlichkeit – das Individuum potenziell zum Verbündeten seiner Überwachung bzw. Kontrolle.

Wenn im Kontext der NSA-Affäre vom »kalten Bürgerkrieg« die Rede ist,³⁵ sollte man den Konflikt

also nicht auf Bürger und Staat reduzieren oder als Krieg zwischen Digital Natives und Digital Immigrants verstehen bzw. zwischen jenen, die Daten kaufen und verkaufen oder sich unrechtmäßig beschaffen, und all den anderen. Der Bürgerkrieg findet nicht zwischen den Bürgern statt, sondern *in* den Bürgern: zwischen ihrem Interesse an technischem Fortschritt, Orientierung und Wahrgenommenwerden auf der einen Seite und ihrem gelegentlichen Unbehagen, dafür Objekt der Überwachung und Kontrolle zu sein, auf der anderen Seite. Dieser interne Bürgerkrieg steht allen Bemühungen im Wege, den Datenschutz durch Daten-Dezentralisierung – zum Beispiel mittels individueller Router und Server – zu stärken. Denn dies würde zwar, ganz im Sinne der eigentlichen, dezentralen Grundstruktur des Internets, die Datenkraken des Internets schwächen, aber eben auch die Bürger der vielfältigen Vorteile berauben, die sich aus Zentralisierung und Vernetzung der Daten ergeben. Die zu klärende Frage lautet: Wie weit kann sich die moderne Gesellschaft dem Gelingen neuer Erfindungen in dieser Hinsicht entziehen?

Gelingt der Entzug nicht, wird die künftige Geschichtsschreibung möglicherweise auch diesen Streitfall anzeigen: Im Jahr 2023 richtete das deutsche Internetministerium, das kurze Zeit nach Snowdens Enthüllungen gebildet worden war, eine Unterlassungsklage gegen die Vereinigung der Datenschutzaktivisten. Deren sogenannter »weißer Block« hatte schon lange Kommunikationslöcher zu erzeugen gefordert, zum Beispiel durch Deaktivierung des GPS

am Smartphone.³⁶ Die Deaktivierung war 2023 zwar nicht mehr möglich, aber der Besitz eines Smartphones mit Presence Tag noch keine Vorschrift. Das wollte das Internetministerium nun ändern. Denn das Verkehrsministerium beabsichtigte, Presence-Technologie (die mit der Präzision von fünf Zentimetern die Position ihres Trägers anzeigen kann) in der Verkehrsregelung einzusetzen. Kollisionen jeder Art ließen sich damit blind und taub vermeiden durch automatisch ausgelöste Warnsignale oder Bremsbefehle an zwei Presence Tag-Träger, deren Positionskordinaten das Abstandslimit unterschritten. Die Datenschutzaktivisten konnten dieses als sicher erachtete Verfahren kaum ablehnen, forderten aber eine Anonymisierung, da die Vermeidung der Kollision zwischen einem Auto und einem Fahrrad nicht die Identifizierung der Fahrer voraussetze. Dieser Perspektive schloss sich das Internetministerium nicht an, mit der Begründung, dass modernstes Data Mining aus der Kenntnis der physischen und psychischen Kondition der Fahrer, ihrer Alltagsroutinen, der Fahrzeugmodelle und vieler anderer verfügbarer Daten die Wahrscheinlichkeit einer Kollision errechnen und entsprechend früh Präventivmaßnahmen auslösen könne. Da Verkehrssicherheit keine Privatangelegenheit sei, dürfe sich kein Bürger der Identifizierung entziehen. Der Aufruf, Lücken in der kybernetischen Kommunikation zu schaffen, wurde daher als gefährlich, von manchen auch als terroristisch eingestuft und gerichtlich untersagt.