REDLINE | VERLAG

Franz Kotteder

DIE WISSEN ALLES ÜBER SIE

Wie Staat und Wirtschaft Ihre Daten ausspionieren – und wie Sie sich davor schützen

Für Nine und Jakob

Franz Kotteder

Die wissen alles über Sie

Wie Staat und Wirtschaft Ihre Daten
ausspionieren – und wie Sie sich davor schützen

REDLINE | VERLAG

Impressum

Bibliografische Information der Deutschen Nationalbibliothek: Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://d-nb.de abrufbar.

Für Fragen und Anregungen:
kotteder@redline-verlag.de

1. Auflage 2011

Nymphenburger Straße 86
D-80636 München
Tel.: 089 651285-0
Fax: 089 652096

Umschlaggestaltung: Jarzina Kommunikations-Design, Holzkirchen
Umschlagabbildung: © Ed Bock/CORBIS
Satz: HJR, Jürgen Echter, Landsberg am Lech
EPUB-Produktion: Grafikstudio Foerster, Belgern

ISBN 978-3-86414-218-5

Weitere Infos zum Thema
www.redline-verlag.de
Gerne übersenden wir Ihnen unser aktuelles Verlagsprogramm.

Inhalt

Finger weg von meinen Daten: Der Schutz der Privatsphäre ist kein Geschenk

»Wo waren Sie am 21. September zwischen acht und zehn Uhr morgens?« Eine solche Frage des Kommissars in einem Fernsehkrimi dürfte in nicht allzu ferner Zukunft nur noch auf Unverständnis stoßen: Wie kann es sein, dass die Polizei so etwas nicht weiß? Was ist denn das für ein Polizist, der vor dem Verhör nicht einmal die Handydaten seines Kontrahenten checkt oder nachsieht, was der Biometrie-Check der Videoüberwachungskameras ergeben hat und ob die Lokalisierungsdaten aus dem PC etwas aufzeigen? In ein paar Jahren schon wird diese Frage obsolet werden, wenn alles nach dem Willen der Sicherheitsfanatiker in den Behörden und Parlamenten geht.

»Where do you want to go today?« Auch diese Frage, einst vom Software-Riesen Microsoft für die Werbung verwendet, wird einem schon bald komisch vorkommen: Denn natürlich weiß ja fast jeder, wohin man gehen will, wenn man den Computer einschaltet und im Internet surft: der Provider, der Browserhersteller, die Suchmaschine, die man benützt, der Betreiber des Netzwerks, das man in aller Regel besucht, möglicherweise auch der Staat, der einem den Trojaner unbemerkt auf die Festplatte geschickt hat, und so weiter. Im Netz ist man nie allein, man steht ständig unter Beobachtung. Diese Erkenntnis hat sich noch nicht überall durchgesetzt, noch immer glauben viele an die Mär, das Internet sei ein »rechtsfreier Raum«, dezentral organisiert,

in dem jeder sich unbehelligt herumtreiben kann. Aber langsam beginnt auch der gewöhnliche »User« zu ahnen, dass das Netz seine Tücken haben kann.

Lange Zeit schien es so, als wären die Debatten der Siebziger- und Achtzigerjahre nur noch brauchbar für Comedians, die sich über die Eltern- und Lehrergeneration lustig machen wollten, weil die noch mit selbstgemalten Transparenten und hektografierten Flugblättern auf die Straße ging, wenn ihr was nicht passte. Etwa die für 1983 geplante Volkszählung, gegen die sich zahlreiche Aktionsgruppen bildeten, die bis vors Bundesverfassungsgericht zogen. Das Zeitalter des Egoismus und des Individualismus sah dergleichen nicht mehr vor, so konnte man schon denken, und die Frage, was mit ihren Daten passiert, bewegt die Menschen des 21. Jahrhunderts so gut wie gar nicht mehr: Denn schließlich haben sie ja nichts zu verbergen.

Bei der Fülle an Daten, die beinahe tagtäglich jedem von uns am Arbeitsplatz, beim Einkaufen, im Internet und nicht zuletzt immer wieder auch von Ämtern und Behörden abverlangt werden, erscheint der einzelne Vorgang fast unerheblich: Was macht es schon, wenn jetzt noch einmal jemand ein weiteres, vermutlich eher unscheinbares Detail von uns wissen will?

Ein weiteres, unscheinbares Detail: Natürlich täuscht das. Denn es gibt keine unscheinbaren Details mehr in der schönen, neuen Datenwelt. Die verschiedenen Bereiche, in denen wir uns bewegen, wachsen immer mehr zusammen zu einer einzigen, großen elektronischen Welt. Telekommunikation und Computer werden mit iPhone und Smartphone nahezu austauschbar, die verschiedenen Datenbanken sind immer leichter zu vernetzen und tauschen ihre Inhalte immer schneller aus. Zugleich sind die gesammelten, riesigen Datenberge mit immer

leistungsstärkeren Programmen immer noch schneller zu durchforsten nach jenen Informationen, die von den jeweils Interessierten wirklich benötigt werden. Der Einzelne kann sich jedenfalls nicht mehr darauf verlassen, wie es noch vor einigen Jahren der Fall gewesen sein mag, dass seine Angaben, seine Äußerungen im virtuellen Raum in der Überfülle des Materials einfach untergehen wie die sprichwörtliche Stecknadel im Heuhaufen. Und Suchprogramme, die den Heuhaufen Cyberspace höchst effektiv durchkämmen, gibt es bereits jede Menge.

So ganz unbedeutend ist also nichts mehr, was an Daten und Informationen über uns auf staatlichen Servern unterwegs ist oder durchs Internet geistert. Das aber ist schon viel mehr Menschen bewusst, als es auf den ersten Blick den Anschein haben mag. Sind nicht die meisten von uns recht bedenkenlos im Internet unterwegs, betreiben Online-Banking, bezahlen mit der Kreditkarte und werfen mit unseren persönlichen Meinungen auf Facebook oder StudiVZ nur so um sich? Mag sein, aber das hält sehr viele nicht davon ab, nachdenklich zu werden und auch ein bisschen misstrauisch zu sein. »Ausgerechnet der Erfolg durch Datensammeln ist die Schwachstelle der Netzwerkseite«, schreibt die *Süddeutsche Zeitung* zum Beispiel Ende 2010, »weltweit werden Nutzer immer kritischer gegenüber den großen Sammlern und immer sensibler, wenn es um ihre persönlichen Daten geht.«[1]

Diese Entwicklung betrifft aber auch staatliche Stellen. Wenn man sieht, wie vorsichtig die Bundesregierung mit dem Zensus 2011 umgeht, wie behutsam man sich an einen möglichen Protest aus den Reihen der Bürger herantastet, so kann man darin immerhin einen Fortschritt erkennen im Vergleich zur großen Volkszählung 1987, als die staatlichen Institutionen eher die Brechstange ansetzten.

Das ist andererseits aber nur das Mindeste, was man erwarten darf als Staatsbürger einer Demokratie. Eingriffe in Persönlichkeitsrechte – und allein die Frage nach persönlichen Daten ist ein solcher – müssen in einer Demokratie gut begründet sein, und es gibt eine ganze Reihe von Dingen, die weder den Staat noch die Regierung etwas angehen. Das betont das Bundesverfassungsgericht schon 1969 im sogenannten »Mikrozensus-Urteil«, einer der ersten Grundsatzentscheidungen zum Datenschutz. Es sei unzulässig, heißt es dort, »einen Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren«, um ihn so »einer Bestandsaufnahme in jeder Beziehung zugänglich« zu machen. Und die Demokratie, so der ehemalige hessische Datenschutzbeauftragte und große Theoretiker des Datenschutzes in Deutschland, Spiros Simitis, »zeichnet sich durch Informationsverzicht aus«.[2]

Diese Erkenntnisse haben sich zweifellos noch nicht überall durchgesetzt. Denn allein die staatlichen Stellen, die Ämter und Behörden, wollen immer mehr von ihren Bürgern wissen, insbesondere dann, wenn diese Bürger Leistungen des Staates in Anspruch nehmen wollen. Und so gibt es elektronische Reisepässe und Personalausweise, angeblich bald auch eine elektronische Gesundheitskarte, wenn man zum Arzt muss, und irgendwann dann wohl auch eine »Jobcard«. Immer sollen wir damit geschützt werden vor Gefahren – sei es nun der internationale Terrorismus, auch wenn der beispielsweise so gut wie nie mit gefälschten Reisepässen arbeitet –, seien es die sogenannten »Sozialschmarotzer« und »Hartz-IV-Betrüger«, die sich anscheinend äußerst üppige staatliche Transferleistungen erschleichen.

Bei näherer Betrachtung erweisen sich die meisten dieser Gefahren zwar als äußerst geringfügig oder

unwahrscheinlich – zum Beispiel wurde der biometrische Reisepass eingeführt, weil der alte angeblich nicht fälschungssicher genug war. Tatsächlich aber, das musste die Bundesregierung in ihrer Antwort auf eine förmliche Anfrage einiger Bundestagsabgeordneter zugeben, waren in den Jahren zwischen 2001 und 2006 nachweislich lediglich sechs gefälschte Passdokumente im Umlauf gewesen. Verglichen damit ist der Aufwand für den neuen, elektronischen Reisepass nicht sehr verhältnismäßig gewesen, sieht man einmal davon ab, dass er auch auf politischen Druck der Amerikaner und auf Anordnung der EU eingeführt wurde.

Wie auch immer: Je mehr man über den Staatsbürger, den Kunden, den Arbeitnehmer oder auch nur den Bekannten weiß, desto leichter ist der Umgang mit ihm. So lautet das Credo derer, die das möglichst umfassende Sammeln von Daten verteidigen. Das ist so falsch nicht. Aber die Sache hat ein Janusgesicht: Wer immer noch mehr Sicherheit haben will, muss irgendwann die Freiheit aufgeben. Die Abwägung zwischen beiden Extremen ist eine schwierige Aufgabe – und zwar nicht nur für Experten, sondern schlicht für alle, die davon betroffen sind.

Eines ist klar: Wer weiß, dass er unter Beobachtung steht, verhält sich anders als jemand, der ganz unbefangen unterwegs ist. Wer Nachteile befürchtet, verzichtet gern einmal darauf, seine Rechte wahrzunehmen, weil er auffallen könnte. Mit verängstigten Bürgern ist jedoch kein Staat zu machen, jedenfalls kein demokratischer. Und deshalb ist es für jeden von uns gutes Recht und auch Pflicht, sich im Kleinen wie im Großen um seine Persönlichkeitsrechte zu kümmern, ohne deshalb befürchten zu müssen, als »Querulant« abgestempelt zu werden.

Gleiches gilt auch für unser Handeln im Wirtschafts- und Privatleben. Da gibt es eine Reihe von Personen, die sagen,

Privatsphäre wäre etwas von gestern, darauf könne man getrost verzichten. Von einer gewissen Offenherzigkeit habe man schließlich nur Vorteile. Man muss aber darauf nicht hören und sollte es auch nicht. Es gibt keinen Grund, auf seine Privatsphäre zu verzichten. Man darf wollen, dass man in Ruhe gelassen wird. Man hat sogar ein Recht darauf. Und es gibt keinen vernünftigen Grund dafür, nicht selbst zu bestimmen, was man von sich an eine wie auch immer geartete Öffentlichkeit herausgeben will. Insofern ist dieses Buch auch ein entschiedenes Plädoyer für die Verteidigung der Privatsphäre – auch wenn das nicht in jeder Zeile explizit ausgesprochen wird.

Dieses Buch befasst sich mit den Fragen, wo die großen Datensammler sitzen, welche Daten sie sammeln, was sie mit diesen Daten wollen und was man tun kann, wenn man sie nicht hergeben will – so man nicht dazu gezwungen ist. Es versteht sich keineswegs als »abgeschlossene Enzyklopädie der Datenklauer«: Vielmehr geht es darum, an möglichst aktuellen Beispielfällen die Problematik des Datensammelns und der Schutzmöglichkeiten aufzuzeigen. Eine ohnehin gar nicht mehr erreichbare Vollständigkeit ist dazu nicht nötig. Man kann selbst aus vermeintlich höchst harmlosen Dingen wie Online-Spielen bei Facebook schnell erkennen, worum es geht und welche Absichten sich wirklich dahinter verbergen – nämlich schlicht die, den Anwendern persönliche Daten zu entlocken und damit Geschäfte zu machen, ohne dass diese es gleich merken.

Das Buch ist unterteilt in drei Hauptteile. Im ersten und umfangreichsten geht es um die staatlichen Datensammler: Ihnen kann man einerseits kaum ausweichen, weil gesetzliche Bestimmungen die Erhebung der Daten vorschreiben und eine Auskunftsverweigerung meist mit Sanktionen belegen. Andererseits aber haben wir als Staatsbürger auch Einfluss auf das Vorgehen des Staates:

indem wir die Regierung wählen, etwa. Oder indem wir die demokratischen Möglichkeiten nutzen, die uns zur Verfügung stehen, um gegen unserer Ansicht nach unsinnige Maßnahmen einzuschreiten.

Im zweiten Teil geht es um jene Daten, die von uns mehr oder weniger automatisch erhoben werden, wenn wir einkaufen oder zur Arbeit gehen. Hier geht es oft nur darum, Bescheid zu wissen, um sich gegen den großen Datenklau zu wehren. Es ist aber zugleich auch wichtig zu wissen, was möglicherweise geschehen kann mit den Informationen, die man hergibt.

Gleiches gilt für den dritten Teil, der sich mit unserem Verhalten im Internet beschäftigt. Hier handelt es sich um Daten, die man zum großen Teil freiwillig oder zumindest fast freiwillig offenbart. Oft ohne das auch nur zu ahnen.

In den einzelnen Teilen wird man immer wieder einmal Unterkapitel finden, denen das Wort »Schlimmstenfalls« vorangestellt ist, oder die heißen: »Was man tun kann«. Hier wird unter »Schlimmstenfalls« dargestellt, was im ungünstigsten Fall eintreten könnte, nach den Szenarien der Kritiker. Und unter »Was man tun kann«, gibt es ganz pragmatische Handlungsvorschläge, wie man mit den möglichen Gefahren umgehen und verhindern kann, dass Informationen öffentlich werden, die man gar nicht weitergeben möchte.

Das Unbehagen an der IT: Die Sammelwut verunsichert viele Menschen

Wenn Journalisten besonders eindrucksvoll darlegen wollen, welche Daten von einem einzelnen Menschen mittlerweile im Internet so kursieren, dann googeln sie. Entweder sich selbst oder eine andere Person. Die französische Zeitschrift *Le Tigre* trieb diesen Versuch auf die Spitze und veröffentlichte Anfang 2009 die detaillierte Lebensgeschichte eines jungen Architekten aus Bordeaux. Die Fakten dafür stammten allesamt aus öffentlich im Netz zugänglichen Quellen, und weil der Mann ein sehr aktiver Nutzer der verschiedensten Dienste war – so hatte er allein 17.000 Fotos auf die Datenbank Flickr gestellt –, fiel die Lebensbeschreibung äußerst umfangreich aus. Der Betroffene kündigte einen Prozess wegen Verletzung der Privatsphäre gegen das Magazin an, ließ das dann aber schnell wieder bleiben: Er hätte vor Gericht nicht den Hauch einer Chance gehabt, schließlich hatte er aus freiem Willen all das verwendete Material ins Netz gestellt, aus dem dann später seine öffentliche und veröffentlichte Biografie wurde.

Manche Leser mögen über den Vorfall geschmunzelt haben und sich gesagt haben: selber schuld! Vielen dürfte aber auch klargeworden sein, dass auch über sie viel mehr Informationen im Netz vorhanden sind, als sie sich so bewusst machen. Auch wenn sie nicht zu den »Freaks« zählen, die pausenlos ihre Fotos hochladen oder ihren Senf zu den Äußerungen von Freunden und

Bekannten in ihrem sozialen Netzwerk geben müssen. Ein gewisses Unbehagen kann jedenfalls kaum einer verleugnen, der im virtuellen Raum unterwegs ist: Was passiert denn da eigentlich so genau?

Immer häufiger formuliert sich in letzter Zeit dieses Unbehagen auch in den Medien. Das Magazin der *Süddeutschen Zeitung* etwa stellte im Juli 2009 fest: »Die Datenaskese der Bürgerrechtler wird vom Datenhedonismus der Nutzer sozialer Netzwerke und Tracking-Dienste weggespült.«[3] Grund dafür, so der Autor, sei ein neues Menschenbild, das die Selbstinszenierung und die Zurschaustellung der eigenen Biografie zu Mitteln im sozialen Überlebenskampf gemacht habe: »Arbeit und Freizeit, berufliche und persönliche Kontakte sind eins, angetrieben von demselben Talent zum ›Networking‹.« Dies gehe einher mit einer Unbedenklichkeit, Hilfsmittel wie GPS oder Handy-Ortung im Namen der »Community-Bildung« zu akzeptieren, die zuvor nicht denkbar gewesen wäre: »Im Vergleich zu den Achtzigerjahren, in denen die Reden vom ›Überwachungsstaat‹ allgegenwärtig waren, leben wir in einer auffällig paranoialosen Zeit.«

Diese Feststellungen waren zu diesem Zeitpunkt durchaus zutreffend. Bereits ein gutes Jahr später aber sehen die Analysen schon wieder anders aus. Aus Anlass der Google-Street-View-Debatte etwa erscheint im Nachrichtenmagazin *Spiegel* ein Plädoyer für den Kampf um die Privatsphäre.[4] »Freiheit ist auch die Freiheit, sich zu verweigern«, heißt es darin, »es sollte darum gehen, dass wir vor allem bei privatesten Daten erlauben müssen, was damit geschieht.« Es gehe auch nicht um das Abfotografieren von Häuserfassaden, sondern im Kern »um den digitalen Um- und Neubau der Wesen dahinter und darum, dass wir das selbst bereits als Währung anerkennen. Es geht nicht um Egos, sondern um Identität.«

Dies ist eine interessante Fortschreibung des vorausgegangen Textes, und es handelt sich dabei keineswegs um einen Einzelfall. Wurden bis vor kurzem Skeptiker noch belächelt als gestrig daherkommende Maschinenstürmer, die halt noch nicht so recht hineingefunden haben in die Welt des Web 2.0, so hat sich binnen kürzester Zeit eben diese Skepsis durchgesetzt in den Köpfen gerade auch der sogenannten »digitalen Bohème«. In bürgerlichen Kreisen war dieses Thema ohnehin schon verankert, oft durch eine lange Protestgeschichte aus den Achtzigerjahren, aber auch durch Diskussionen innerhalb der intellektuellen Elite der Republik. 2009 etwa erschien die Streitschrift »Angriff auf die Freiheit – Sicherheitswahn, Überwachungsstaat und der Abbau bürgerlicher Rechte«, mit der sich die beiden Schriftsteller Ilija Trojanow und Juli Zeh engagiert und sehr konkret in die politische Debatte einmischten. Ihnen ging es dabei vor allem um die sogenannten Sicherheitsgesetze, die als Allheilmittel gegen »Terrornetzwerke« gepriesen werden. »Netzwerke sind die Drachen des 21. Jahrhunderts«, sagen die beiden dagegen. Es stehe nichts weniger als »ein Kampf um unsere Freiheit und unsere Privatsphäre« bevor, »ein Kampf, der sofort beginnen muss, denn die Zukunft unserer Gesellschaft wird gegenwärtig verhandelt, ohne dass unsere Meinung gehört wird«.[5] Zeh und Trojanow bezogen ihre Kritik in erster Linie auf staatliche Maßnahmen, entließen aber auch die Privatwirtschaft und im Speziellen die großen Internetkonzerne nicht aus der Verantwortung. Tatsächlich zeigte sich da schon, dass Datenschutz keineswegs eine überkommene Problematik für Alt-Linke und Alt-Grüne ist, die eben ein hoffnungslos gestörtes Verhältnis zum Staat haben, sondern dass er alle angeht. Vor allem, weil sich aus vielen kleinen Einzelinformationen heutzutage problemlos ein Gesamtbild zusammenstellen lässt, das wir von uns möglicherweise gar nicht machen lassen wollen. Die Technik aber macht bereits vieles möglich. »Die rasanten

Fortschritte hinsichtlich der Rechenleistung und der Auswertungsalgorithmen moderner Computer«, schreibt etwa der Chaos Computer Club (CCC), »machen neue Analysemethoden zugänglich, die das Erkennen von menschlichen Beziehungsgeflechten, Absichten und Vorlieben aus Verkehrsdaten möglich machen.«[6] Es kann jedoch gut sein, dass man das gar nicht will …

Der Untergang der Privatsphäre?

Konzernführer wie Google-Chef Eric Schmidt verstehen so etwas überhaupt nicht. Privatsphäre und Datenschutz – das passt nicht ins Geschäftsmodell. Und deshalb tun sie gerne so, als wäre Privatsphäre so ungefähr das Hinterletzte, was sich ein moderner Mensch vorstellen kann. Scott McNealy, einer der Gründer von Sun Microsystems, brachte das in entwaffnender Offenheit schon 1999 auf den Punkt: »Sie haben keine Privatsphäre mehr. Finden Sie sich damit ab.« Und Marc Zuckerberg, der Chef des größten sozialen Netzwerks überhaupt, nämlich Facebook, hat ein ganz besonderes Sendungsbewusstsein. Er vertritt die These der »radical transparency«, der grundsätzlichen Transparenz. In einer »offenen und transparenten Welt«, so glaubt er, seien die Menschen verantwortungsvoller und toleranter, weil sie zu den Konsequenzen ihres Handelns stehen müssten. Und weil jeder einmal etwas Falsches oder Lächerliches mache. Zuckerberg: »Die Menschen zu dieser Offenheit zu bewegen – das ist eine große Herausforderung, aber ich glaube, wir schaffen das. Es kostet nur Zeit.«

Mag sein, dass diese Menschen wirklich glauben, was sie sagen, und es nicht nur behaupten, weil es am besten zu ihren Geschäftsinteressen passt. Wenn dem so ist, dann hat man es jedenfalls mit einem doch eher einfachen Weltbild

zu tun. Dass eine ständige soziale Kontrolle und Aufsicht durch die Community – um einmal das Wort »Überwachung« zu vermeiden – zu einer besseren Welt führt, dieser Gedanke in all seiner Schlichtheit könnte auch von einem George W. Bush jun. stammen.

Der deutsche Medientheoretiker Norbert Bolz von der Technischen Universität Berlin ist der Ansicht: »Der schwerste Angriff auf die Privatsphäre geht dabei übrigens nicht von Regierungen und Unternehmen aus, sondern von den sozialen Netzwerken.«[7] Womit er auf andere Weise das Gleiche sagt wie Zuckerberg. Nur sieht Bolz im ständigen Einblick, den die Community Gleichgesinnter auf das Individuum hat, nichts Positives. Es handele sich, beispielsweise bei Google Street View, um einen Angriff auf den »Geheimniszustand«, der für die bürgerliche Privatsphäre wesentlich sei. Ob dieser Angriff abgewehrt werden kann? Bolz zeigt sich skeptisch: »Die Freiheit der Information hat ihre traditionellen Grenzen an der Privatsphäre des Individuums und der Sicherheit des Staates. Aber es gibt immer mehr Menschen, denen beides gleichgültig ist.«

Man könnte aber mit genauso gutem Recht ebenso sagen: Es gibt inzwischen immer Menschen, denen das nicht mehr gleichgültig ist. Der Kampf um die Privatsphäre ist noch lange nicht entschieden, auch wenn wir alle schon unsere Datenspuren im Netz hinterlassen haben und das Internet keinen Radiergummi kennt. Der Kampf um die Privatsphäre ist freilich nicht zu gewinnen ohne persönlichen Einsatz und ohne die entsprechende Politik in den einzelnen Staaten.

Die Hilflosigkeit der Politik

Was die Politik angeht, gibt es allerdings auch gute Gründe, sich Sorgen zu machen. Denn die Regierungen und die Sicherheitsbehörden zählen ja selbst zu den großen Datensammlern und häufen Informationen an, von deren Notwendigkeit man nicht immer überzeugt sein kann. Obendrein kommt es ja immer wieder zu Datenpannen – und ganz besonders oft anscheinend in Großbritannien, jenem Land innerhalb der Europäischen Union, das führend ist, was Überwachung und Erfassung seiner Bürger angeht. So kamen dort im November 2007 Informationen über 25 Millionen Briten, die Kindergeld beziehen, abhanden, weil sie mit der Post verschickt worden waren und nie ankamen. Im Dezember 2007 verschwanden in britischen Gesundheitszentren Patienteninformationen von mehr als 100.000 Menschen spurlos. Im selben Monat wurde auch der Verlust einer CD mit Informationen über drei Millionen Kandidaten für den theoretischen Teil der Führerscheinprüfung bekannt. Und im Januar 2008 wurden aus dem Auto eines Offiziers der Kriegsmarine Datenträger mit Informationen gestohlen, die über mehr als 600.000 potenzielle Rekruten angelegt worden waren.

Derlei Sicherheitspannen seien bei uns gar nicht möglich, heißt es zum Beispiel aus den Oberfinanzdirektionen. Hierzulande würden solch brisante Informationen nicht auf CDs mit der Post verschickt, sondern lagerten auf mehrfach abgesicherten Servern. Dennoch gibt es immer wieder kleinere Beispiele für das Versagen von Behörden: Mal landen versehentlich Ermittlungsergebnisse der Polizei vorübergehend im Internet (wie es im Januar 2007 etwa dem Polizeipräsidium Südhessen widerfuhr), mal sind es Daten über Verstorbene, die im Krankenhausmüll landen, mal werden Festplatten auf dem Second-Hand-Markt angeboten, aus denen Informatiker höchst sensible Daten noch herauslesen können, weil diese nicht sauber gelöscht worden sind.

Das zugrundeliegende Problem ist: Es werden einfach viel zu viele Daten gesammelt, und es wird viel zu wenig Wert darauf gelegt, sie sicher zu verwahren. »Wer den Daten-Gau vermeiden will«, fordert der Bundesdatenschutzbeauftragte Peter Schaar, »muss für Datensparsamkeit sorgen.«[8] Eine Aussage, die nun freilich nicht nur für staatliche Stellen gilt, sondern auch für den Privatmenschen. Der kann nämlich, beispielsweise im Internet, durchaus bestimmen, welche Informationen er über sich preisgeben will und welche nicht. Sofern er sich überlegt, was ihm seine Privatsphäre wirklich wert ist.

Von der Politik allein ist jedenfalls erst einmal wenig Hilfe zu erwarten. Da hat man nämlich den Eindruck: Selbst wenn sie guten Willens ist – es fehlt ihr meist schlichtweg die Ahnung von der Materie, um mit den Gefährdungen des Internets und des Web 2.0 fertigzuwerden. Von »politischer Hilflosigkeit der Bundesregierung« im Umgang mit neuen Internet-Techniken und -Formaten spricht etwa die Wochenzeitung *Die Zeit*, wenn sie im Sommer 2010 feststellt: »Es fehlt nicht nur an Konzepten für den Umgang mit den Netzmultis, es fehlt an einer Sprache, die den Bürgern ihre Sorgen zu nehmen weiß. Und es fehlt weithin an juristischen Instrumenten, um den völlig neuen Problemen, die durch die private Datenvermassung für Individuen und den Staat entstehen, halbwegs gerecht zu werden.«[9] Daran scheint sich nur langsam etwas zu ändern. Immerhin haben die Verantwortlichen das Problem erkannt und inzwischen sind wenigstens Ansätze festzustellen, den sich wandelnden technischen Bedingungen einigermaßen gerecht zu werden – oder doch wenigstens etwas schneller hinterherzuhinken als bisher.

Denn das, was in dieser Hinsicht bisher geschah, war bisweilen nur noch lächerlich. Die frühere Familienministerin Ursula von der Leyen (CDU) verblüffte etwa die Fachwelt mit

dem Vorschlag ihres Ministeriums, der Kinderpornografie im Internet dadurch entgegenzuwirken, dass man vor einschlägigen Seiten im Netz Stoppschilder schalten wollte. Das brachte ihr von denen, die sich mit den Voraussetzungen und Gepflogenheiten des Internets und seiner Gemeinde ein wenig auskannten, kaum Beifall, dafür aber den schönen Spottnamen »Zensursula« ein. Amtsnachfolgerin Ilse Aigner (CSU) war schon ein bisschen näher an der Realität, als sie aus Protest gegen die Laxheit im Umgang mit privaten Daten ihr Facebook-Konto öffentlichkeitswirksam kündigte. Praktische Folgen hatte das für Facebook natürlich nicht.

Wohin es tatsächlich gehen muss, wenn man eine Veränderung anstrebt und die großen Datensammler zur Vernunft bringen will, das zeigen etwa die Verfahren, die von der Europäischen Union in der Vergangenheit gegen Microsoft und jetzt aktuell gegen Google angestrengt wurden. Oder auch das gerichtliche Vorgehen von Verbraucherschützern gegen Facebook. Da zeigen die vorsichtigen, fast schon devoten Reaktionen der Netzmultis, was sie wirklich beeinflussen kann. Nämlich das selbstbewusste Auftreten staatlicher und überstaatlicher Institutionen, die auch die Macht haben, Sanktionen durchzusetzen. Und so gibt es genau genommen eigentlich keinen Grund, nur pessimistisch in die Zukunft zu blicken, wenn es um den Schutz unserer Daten und unserer Privatsphäre geht. Der Kampf ist noch lange nicht verloren. Es kommt aber darauf an, sich ihm überhaupt zu stellen.

Teil 1:
Vater Staat will alles wissen

Wie Ämter und Behörden uns (fast) ganz legal ausspionieren

Was darf der Staat? Die Rechte des Bürgers und andere Interessen

Nein, diese Volkszählung ist nicht besonders beliebt in Deutschland. Mehr als 1.100 Bürgerinitiativen im ganzen Land rufen zum Boykott auf, ihre Parolen lauten: »Nur Schafe lassen sich zählen!« und »Kein Staat mit diesem Staat!« Die Regierung droht mit Zwangsgeldern, in einzelnen Bundesländern nimmt der Verfassungsschutz gar die Jugendorganisation der SPD, die Jungsozialisten, die Grünen und die Bürgerrechtsorganisation Humanistische Union unter Beobachtung, weil einzelne Landesgliederungen den Boykott unterstützen. Bundesweit finden mehr als 100 Hausdurchsuchungen bei Volkszählungsgegnern statt. Und eines Tages prangt auf dem Rasen der Dortmunder Fußballarena vor einem wichtigen Bundesligaspiel in breiten Lettern die Aufforderung: »Boykottiert und sabotiert die Volkszählung«. Nach Rücksprache mit dem Bundespräsidialamt ergänzen die Verantwortlichen des

Vereins den Satz, der sich so schnell nicht entfernen lässt, um ein »nicht!« dahinter und um ein »Der Bundespräsident:« davor, um die Fernsehübertragung nicht zu gefährden.

Das alles geschah vor ungefähr 25 Jahren, zwischen Herbst 1986 und dem 25. Mai 1987, dem Stichtag für die Volkszählung. Ursprünglich war sie schon für das Frühjahr 1983 vorgesehen gewesen, war aber dann wegen einer ausstehenden Entscheidung des Bundesverfassungsgerichts aufgeschoben worden. Die Verfassungsrichter fällten dann auch im Dezember 1983 ein aufsehenerregendes Urteil und erklärten das damalige Volkszählungsgesetz für grundgesetzwidrig, weil es das Recht der Bürger auf »informationelle Selbstbestimmung« nicht beachte.

Im Frühjahr 2011 steht nun wieder eine Volkszählung an, zum Stichtag 9. Mai. Ein Verein und ein Arbeitskreis, hinter denen nach eigenen Angaben rund 13.000 Menschen stehen, haben dagegen Verfassungsbeschwerde eingelegt, sind damit aber gescheitert. Die Entscheidung des Bundesverfassungsgerichts erregte kein besonderes Aufsehen, landete nicht einmal automatisch auf den Titelseiten der Tageszeitungen. Die Bürger des Landes scheinen andere Sorgen zu haben im Herbst 2010.

In der Tat aber ist es ganz interessant, die Diskussionen von vor einem Vierteljahrhundert noch einmal nachzuvollziehen. Denn die Sorgen von damals erscheinen beinahe rührend, vergleicht man sie mit der heutigen Wirklichkeit. Da sah man die Visionen eines George Orwell in seinem Roman *1984* auf gespenstische Weise wahr werden, weil in Deutschland das Kabelfernsehen drohte, ja das ganze Land mit Glasfaserkabeln überzogen werden sollte. Die Digitalisierung des Telefonnetzes war die unmittelbare Vorstufe des Überwachungsstaates, weil Telefongespräche jederzeit und problemlos abgehört und aufgezeichnet

werden könnten, hieß es. Und die neue Technologie des Bildschirmtextes, abgekürzt Btx, würde ganz neue Kontrollmöglichkeiten schaffen – die Bürger holten sich damit den Großen Bruder quasi direkt ins Wohnzimmer, weil die Behörden jederzeit nachvollziehen könnten, welche Seiten die Nutzer aufrufen würden. Nahezu lückenlose Personaldossiers ließen sich so erstellen, wenn man auch noch den Abgleich verschiedener Datenbanken bei Ämtern, Behörden und Versicherungen gestatte.

Erst vorpreschen, dann zurückrudern

Die Ängste von damals waren so unberechtigt ja nun nicht – tatsächlich gab es alle diese Möglichkeiten damals schon. Es gibt sie heute noch viel mehr, nur scheinen sich, anders als in den Achtzigerjahren, längst nicht mehr so viele Menschen darüber aufzuregen. Der Datenabgleich aus verschiedensten Quellen ist durch Hartz IV längst salonfähig geworden, es trifft ja nur »die Richtigen«.

Aber damit ist natürlich noch lange nicht die Frage geklärt: Was darf der Staat eigentlich? Wie weit darf er in die Rechte seiner Bürger eingreifen? Eine klare, eindeutige Antwort wäre zwar schön, aber es gibt sie nicht. Sie muss jedes Mal wieder aufs Neue beantwortet werden, und es ist immer eine Auseinandersetzung und eine Abwägung zwischen verschiedenen Interessen. Regierung, Verwaltung und ganz besonders die Sicherheitsbehörden werden immer behaupten, diese und jene Maßnahme sei unbedingt notwendig, setze man sie nicht durch, so drohten Chaos und Verdammnis, das Land sei nicht mehr regierbar und inneren wie äußeren Feinden werde das Tor sperrangelweit aufgerissen. Diese Argumentation findet sich, mehr oder weniger abgeschwächt, praktisch immer, wenn es um die

Einschränkung von Bürgerrechten und insbesondere des Rechts auf Privatsphäre geht. Und stets lässt sich derselbe Mechanismus beobachten: Zuerst wird ein Schreckensbild an die Wand gemalt, dann folgt der Vorschlag mit drastischen Maßnahmen, die unbedingt umgesetzt werden müssen, damit aus dem Schreckensbild nicht Wirklichkeit würde. Ist die öffentliche Meinung allzu empört, macht man ein paar Abstriche und setzt das Paket dann trotzdem um.

Oder aber es kommt das Bundesverfassungsgericht und macht den Datensammlern einen Strich durch die Rechnung. Regelmäßig seit den Sechzigerjahren werden Deutschlands oberste Richter angerufen, um die Frage zu klären, wie weit der Staat in die Freiheitsrechte seiner Bürger eingreifen darf. Und fast immer fallen die Entscheidungen zugunsten der Bürgerrechte, fast immer werden die Hardliner zurückgepfiffen. Tatsächlich hat das Bundesverfassungsgericht den Datenschutz in Deutschland im Wesentlichen mitbegründet und faktisch in den Status eines Grundrechts erhoben.

Die Politik hat das freilich selten wirklich gewürdigt. Karlsruher Urteile, die umstrittene Maßnahmen aufhoben, wurden in aller Regel keineswegs als Hinweis darauf betrachtet, dass man einen Fehler gemacht habe. Sondern im Gegenteil fühlten sich die Regierenden umso mehr bemüßigt, die beanstandeten Rechtsmängel jetzt möglichst zu umgehen oder nur so weit zu beheben, als es unbedingt nötig war. Fast immer geht es der Politik nach solchen Entscheidungen des Bundesverfassungsgerichts lediglich darum, das ursprünglich beabsichtigte Ziel mit allen Mitteln doch noch zu erreichen, nach dem Motto: Vorne muss es so aussehen, als ob wir tun, was die Richter sagen, aber hintenrum machen wir doch, was wir wollen.

So ist über die Jahrzehnte hinweg ein recht dichtes Netz staatlicher Beobachtung entstanden. Manche Daten sind