

+
Während über George Orwells düstere Utopie „1984“ die Zeit hinweggegangen ist, zeichnet sich am Horizont ein ganz anderer, ein digitaler Überwachungsstaat ab. In ihm sammeln Staatsorgane und Unternehmen gleichermaßen Daten über Bürger und Konsumenten. Die liefern nicht selten frei Haus: mittels Handy, Internet und E-Mail, beim Online-Shopping ebenso wie an videoüberwachten öffentlichen Orten. Gleichzeitig nehmen die Befugnisse der Behörden zu, im Namen der Terrorabwehr diesen Datenschatten auch ohne konkreten Verdacht auszuspionieren. Auf dem Spiel stehen nach Ansicht von Datenschützern Freiheit und Privatsphäre im demokratischen Rechtsstaat.

+

Das Geschäft mit der Angst

Staat und Sicherheitsindustrie arbeiten Hand in Hand, um den Bürgern unbemerkt Daten zu entlocken. Noch stößt deren Auswertung an technische und juristische Grenzen – doch die Zentralisierung der Datenbestände schreitet unaufhaltsam voran

VON NIELS BOEING

Noch nicht einmal ein Vierteljahrhundert ist es her, als die Ankunft eines Orwell'schen Überwachungsstaates befürchtet wurde: 1983 versetzte die bevorstehende Volkszählung Deutschland in Aufruhr, das Bundesverfassungsgericht wurde angerufen – und Apple porträtierte IBM in einem Werbespot als Big Brother. George Orwells Negativvision, die er in seinem Roman „1984“ entwarf, war allerdings eine analoge. Die Überwachung besorgte eine Gedankenpolizei, die auf klassische Bespitzelung durch Menschen setzte. Ihr einziges Hightech-Instrument war ein zum Televisor mutiertes Fernsehgerät, mit dem die Partei in die Wohnungen der Bürger spähen konnte. Den gibt es bis heute nicht.

Er ist auch nicht mehr nötig – denn in den letzten Jahren ist eine neue Dystopie denkbar geworden: der digitale Überwachungsstaat. Wozu Spitzel mühsam Informationen zusammenklauben lassen, wenn die Menschen sie ahnungslos von selbst liefern – in Form eines stetig wachsenden digitalen Datenschattens? Wer heute Bürger bespitzeln will, muss lediglich ihre Daten analy-

sieren. Gespeist werden die Datenbanken dabei längst nicht allein von misstrauischen Staatsorganen, sondern vor allem von aufmerksamen Unternehmen, die für ihre Kunden nur das Beste wollen. Die gute Nachricht: Noch arbeiten alle Beteiligten mehr neben- als miteinander – der eine untersucht die Beine des Datenschattens, während der andere sich für den Kopf interessiert – und noch gehen die Beteiligten nicht effizient vor. Aber das könnte sich ändern. Eine Phalanx von vielen kleinen Brüdern könnte schaffen, was Orwell nur einem Big Brother zuge-
traut hatte. Die Technologien dafür sind vorhanden.

Statt Televisoren breiten sich Kameraaugen aus. „Der Bedarf hat seit den Anschlägen von New York und Madrid merklich zugenommen“, sagt Bruno Jentner, Marketingleiter der fränkischen Firma Funkwerk plettac electronic GmbH, die unter anderem Videoüberwachungssysteme für die Winterolympiade in Turin geliefert hat. Waren es anfangs hauptsächlich private Auftraggeber, die Überwachungskameras in Bahnhöfen, auf Flughäfen und in Bankgebäuden installierten, folgen nun

Für Staat und Sicherheitsindustrie geht es beim Einsatz der neuen Überwachungstechnologien nicht nur um die nationale Sicherheit, sondern auch um die Förderung des Hightech-Standorts

Wachsamer Blick auf den Rotlichtbezirk: Auf der Hamburger Reeperbahn läuft seit diesem März eine Anlage zur Videoüberwachung. Kosten: 620 000 Euro



MARCO HERR, POLIZEI HAMBURG, P042

staatliche Organe. Mitte März zum Beispiel wurde in Hamburg eine Kamerakette auf der Vergnügungsmeile Reeperbahn installiert. Begründung von Innensenator Udo Nagel: Hamburg wolle dem Sicherheitsbedürfnis von Bürgern und Gästen entgegenkommen.

Die werden nicht nur beobachtet, sondern auch gespeichert: „In den letzten zwei, drei Jahren ist mit dem Übergang zu digitalen Network-Recordern die Aufzeichnungsrates stark gestiegen“, sagt Funkwerk-Marketier Jentner. Bis 2002 habe der Anteil vernetzter Systeme am Videoüberwachungsmarkt bei etwa zehn Prozent gelegen, seitdem sei er auf 30 bis 40 Prozent gestiegen. Existieren aber erst einmal digitale Bilddaten von Bürgern, lassen sie sich im Prinzip auch ihrem Datenschatten hinzufügen.

Jentner versichert, dass die Kameras im Einklang mit geltendem Datenschutzrecht installiert werden: „Es gibt klare Voraussetzungen vom Gesetzgeber.“ Eine davon ist das so genannte Privacy Masking. Vor der Inbetriebnahme werden in der Software der um 360

Grad schwenkbaren Kameras die Neigungswinkel eingegeben, unter denen das Objektiv auf Wohnungsfenster zeigt. Schwenkt die Kamera in diesen Bereich, wird im späteren Betrieb der Bildschirm in der Polizeizentrale automatisch geschwärzt. Dieses Privacy Masking wird schon mal vergessen: Bundeskanzlerin Merkels Berliner Wohnung wurde jahrelang von einer Kamera auf dem nahe gelegenen Pergamon-Museum erfasst – der Sicherheitsdienst dürfte seinen Spaß gehabt haben.

Vorreiter in der Videoüberwachung ist Großbritannien, wo schätzungsweise vier Millionen Überwachungskameras installiert sind. Aber Deutschland holt auf. 2002 beklagte der Vorsitzende des ZVEI-Fachverbandes Sicherheitssysteme, Bernd Seibt, noch die „unbefriedigende Nutzung“ der Videoüberwachung hierzulande. Seitdem hat sich einiges getan: Die meisten Bundesländer haben nach den Anschlägen vom 11. September in Neufassungen ihrer Polizeigesetze die rechtlichen Grundlagen dafür geschaffen. Da ist es nicht verwunderlich, dass die Branche kräftig wächst: Die auf Sicherheits-

technologien spezialisierte Mario Fischer Unternehmensberatung erwartet, dass das Marktvolumen für Videoüberwachungssysteme in Deutschland von 327 Millionen Euro im vergangenen Jahr auf 455 Millionen Euro 2010 wachsen wird. Weltweit prognostizieren Marktforscher von Frost & Sullivan ein jährliches Wachstum von 11,3 Prozent für den Videoüberwachungsmarkt. Das Marktvolumen würde sich bis 2010 auf 8,64 Milliarden Dollar gegenüber 2003 mehr als verdoppeln.

Die Installation von Videoüberwachungssystemen genügt der Sicherheitsindustrie noch nicht: Die digitalen Bilddaten sollen mit Hilfe biometrischer Analyseverfahren auch ausgewertet werden. Dass die deutschen Stadionbetreiber bei der Fußball-WM hier nicht mit gutem Beispiel vorangehen wollen – nach Auskunft des WM-Organisationskomitees ist keine biometrische Auswertung geplant –, versteht Verbandsmann Seibt nicht: „Der Verzicht auf Biometrie bei der WM 2006 wäre nicht nur von Nachteil für die innere Sicherheit, sondern auch eine verpasste Chance für das Image Deutschlands als Hochtechnologiestandort.“

Dafür konnte die Sicherheitsindustrie auf einem anderen Biometriefeld punkten: Der neue Reisepass „e-Pass“, der im November vergangenen Jahres eingeführt worden ist, speichert auf einem Chip ein frontal aufgenommenes Bild, das an Grenzübergängen mittels Gesichtserkennungssoftware mit Digitalporträts gesuchter Straftäter und Terroristen verglichen werden kann. Ab 2007 soll auf dem Chip auch ein digitalisierter Fingerabdruck hinterlegt werden. Das Beratungsunternehmen International Biometric Group erwartet angesichts dieser Möglichkeiten einen Boom im weltweiten Biometriemarkt: Der Jahresumsatz, so schätzen die Experten, werde von derzeit 2,1 Milliarden Dollar bis 2010 auf 5,7 Milliarden Dollar steigen.

Mit dem Übergang zu digitalen Network-Recordern ist die Aufzeichnungsrate gestiegen

Einhundertprozentige Sicherheit bei der Erkennung bieten Biometrie-Systeme bislang nicht. Die Raten von falscher Identifizierung oder Ablehnung liegen bei zwei Prozent: Das trifft statistisch 20 000 von einer Million Grenzgängern. Bei standardisierten Bildern seien Maschinen zwar bereits besser als Menschen, sagt der Neuroinformatiker Christoph von der Malsburg, der mit seiner Firma ZN Vision Technologies eines der weltweit führenden Gesichtserkennungssysteme entwickelte. Die Analyse von Bewegtbildern aus Videodaten stecke aber „noch sehr in den Kinderschuhen, sowohl was die Erkennung von Personen angeht – wegen schlechter Auflösung sowie variabler Beleuchtung und Pose – als auch im Sinne der Charakterisierung der Vorgänge.“

Der Biometrie-Pass hat noch mehr Zweifelhafes zu bieten: die so genannten RFID-Tags (Radio Frequency



PICTURE-ALLIANCE/DP

Das Auge des Gesetzes in der Bahnhofshalle: Bahnhöfe und Flughäfen waren die ersten öffentlichen Einsatzorte bei der Videoüberwachung, nun folgen Plätze und Straßen

Identification). Sie werden nicht per Computer ausgelesen, sondern mittels elektromagnetischer Induktion. Das Lesegerät erzeugt damit berührungslos in der Spule des Tags einen Strom, der dessen Chip zum Senden der gespeicherten Personendaten veranlasst. Die sind verschlüsselt und sollen so Pässe endlich fälschungssicher machen, hoffen die Behörden in den Industrieländern. Doch schon im Juli 2005 gelang es dem niederländischen Sicherheitslabor Riscure, den Schutz mit einem normalen PC binnen zwei Stunden zu knacken.

Lückenloses Konsumentenprofil

Vorangetrieben wird die RFID-Technologie vor allem von der Warenwirtschaft, die sie als Revolution in der Logistik preist. Denn jeder RFID-Chip hat eine weltweit einmalige Nummer, die im so genannten Object Name System (ONS) abgelegt ist. Damit wird zum einen der Weg jeder einzelnen RFID-getaggten Ware lückenlos nachvollziehbar. Zum anderen sollen die RFID-Chips in Supermärkten und Kaufhäusern die Kassenabrechnung vollends automatisieren. Im Einkaufswagen vorbeigeschobene, getaggte Waren werden automatisch erkannt und die entsprechenden Preise zusammengerechnet – so jedenfalls die Theorie. Als Mitarbeiter der Metro – der Konzern gehört zu den treibenden Kräften der Technologie – Anfang März auf der Cebit Bundeskanzlerin Merkel die Vorzüge der Technik präsentieren wollten, erlebten sie ein Desaster: Fünfmal mussten sie den vollgepackten Einkaufswagen am Scanner vorbeischieben – dann erst erkannte er den Wageninhalt korrekt. „Da müssen Sie noch mal drüber nachdenken“, soll die Kanzlerin trocken bemerkt haben.

Nachdenken sollten RFID-Verfechter auch über zwei potenziell hässliche Konsequenzen. In Verbindung mit Kundenkarten, von denen allein in Deutschland rund



JULSTEIN

Vorreiter Großbritannien: Im Vereinigten Königreich sind vier Millionen Überwachungskameras installiert. Bis Jahresende soll es eine landesweite Kfz-Kennzeichen-Erfassung geben

100 Millionen ausgegeben sind, kann aus der detaillierten Einkaufsliste ein perfektes Konsumentenprofil erstellt werden. Damit kann der Handel endlich zur Online-Wirtschaft aufschließen, die dank Cookies solche Profile schon seit langem anlegen kann. Der Datenschatten des Verbrauchers könnte dann etwa einer angeschlossenen Fluglinie mitteilen, dass er zuletzt Unmengen Rum gekauft hat und Sonderangebote für Kubareisen gebrauchen könnte. Das mag noch praktisch sein – heikel wird es, wenn etwa Arbeitgeber oder Versicherungen Zugang zu solchen Daten bekommen sollten. Und: Jedes unbefugte Lesegerät kann die Daten abgreifen, wenn es weniger als zehn Meter an den Chip herangebracht wird. Damit können im Prinzip auch Dritte unmittelbar einen Teil vom individuellen Datenschatten erbeuten.

Diese Befürchtungen weisen die Akteure der RFID-Revolution zwar als Schwarzmalerei von sich. Tatsächlich ist ihnen diese Konsequenz der Technologie aber seit langem bewusst, wie interne Dokumente des Auto-ID Lab, einer internationalen RFID-Industrieplattform, zeigen. „Die beste Kommunikationsstrategie ist, die Technologie schlicht als verbesserten Strichcode zu positionieren“, hieß es 2001 in einer vertraulichen Präsentation. Denn Befragungen hatten schon damals gezeigt, dass 78 Prozent der über RFID Aufgeklärten Bedenken und teilweise explizit Big-Brother-Assoziationen hatten. Dass die Strichcode-Strategie bislang nicht aufging, ist Datenschutzorganisationen wie dem unabhängigen Bielefelder Verein Foebud zu verdanken. Sie entlarvten nicht nur das von Metro im Versuchsmarkt „Future Store“ bereitgestellte RFID-Deaktivierungsgerät als unzulänglich: Die gespeicherten Daten wurden nachweislich nicht vollständig gelöscht – ausgerechnet die weltweit einmalige Seriennummer blieb erhalten. Foebud sorgte auch dafür,

dass die Technik bisher nicht übereilt eingeführt wurde. „Wir wollen keine Abschaffung von RFID, sondern Gesetze und technische Vorkehrungen, die die Privatsphäre der Bürgerinnen und Bürger schützen“, sagt Rena Tangens, Mitgründerin von Foebud. „RFID ist in Ordnung für Paletten in der Logistik, aber Menschen sind keine Versandpakete.“

Unzulässige Bewertung des Datenschattens

Diese Auffassung scheint der Deutsche Fußball-Bund nur begrenzt zu teilen. Dass die RFID-Chips nun auf den WM-Tickets eingesetzt werden und dort die Ausweisnummer speichern, begründet der DFB damit, dass es dann bei den Einlasskontrollen in den Stadien keine Sprachprobleme mit ausländischen Fans gebe. Eine eindeutige Identifizierung wäre aber auch mit anderen Verfahren möglich gewesen. Die eigentliche Motivation ist nach Ansicht von Rena Tangens viel schlichter: Die WM ist für Sponsor Philips – einen der führenden RFID-Hersteller – eine gute Gelegenheit, die Technologie endlich an den Datenschutzdebatten vorbei als Faktum zu etablieren. Immerhin kommt sie auf über drei Millionen WM-Tickets zum Einsatz.

Aber auch ohne massive Vernetzung von Sensoren ist das Erstellen von Kundenprofilen schon jetzt ein Problem, wie das so genannte Scoring im Versandhandel oder bei der Kreditvergabe zeigt. Aus einem Mix öffentlich zugänglicher statistischer und bei Adresshändlern beziehbaren Daten wird ein Wert für die Bonität des Kunden errechnet. Ein reales Beispiel: Wer bei einer Online-Bestellung über die Postleitzahl erkennbar Hamburg St. Georg – berüchtigt für seine Drogenszene – als Wohnort eingibt, bekommt als Zahlungsmodus Vorkasse angezeigt. Ein Wohnort wie Blankenese ermöglicht hingegen eine Bezahlung auf Rechnung. Ein glat-

Aus einem Mix verschiedener Daten lässt sich ein Wert für die Bonität von Kunden ermitteln

ter Bruch des Datenschutzgesetzes: Es verbietet eine automatisierte Bewertung von Kunden. Nur ist denen wegen der Intransparenz des Verfahrens kaum bewusst, dass sich hier Unternehmen unrechtmäßig ihres Datenschattens bedienen.

Von Sicherheitsorganen wird der schon länger angezapft. Der US-Geheimdienst NSA wertet seit Jahren im großen Stil mit Hilfe des weltumspannenden digitalen Überwachungssystems Echelon den Internetdatenverkehr aus, wenn auch im Verborgenen. Offiziell müssen sich die Strafverfolger bislang noch mit dem Belauschen des E-Mail-Verkehrs begnügen. In den USA ist dies mit dem Patriot Act von 2001 legalisiert worden. Das FBI setzt dabei kommerzielle Programme zum so genannten Packet Sniffing ein. Anders als beim 2003 eingestellten Carnivore-System zum Abfangen von E-Mails muss es

inzwischen darüber nicht mehr Bericht an den US-Kongress erstatten. Mittlerweile nutzt das FBI andere Technologien, die nicht mehr kontrolliert werden.

So drastisch sind die deutschen Verhältnisse noch nicht. Aber auch hier können Ermittler mit richterlichem Bescheid seit dem 1. Januar 2005, als die Telekommunikations-Überwachungsverordnung (TKÜV) in Kraft trat, E-Mail-Konten filzen. Die Provider mussten dafür ein eigenes Terminal und das Kryptogerät SINA-Box installieren, das die von den Behörden angeforderten Daten verschlüsselt. „Seit der TKÜV ist die Anzahl der Überwachungen nach oben gegangen“, sagt Andreas Maurer, Sprecher des Providers I&I Internet AG.

Der Lauschangriff auf die E-Post war nur der Anfang. Die nächste Ausbaustufe in Europa ist bereits geplant: die Vorratsdatenspeicherung. Hinter diesem Wortungelum verbirgt sich die Aufzeichnung aller wichtigen Nutzungsdaten durch Provider und Telekommunikationsunternehmen: Telefonnummern, IP-Adressen, User-IDs, Verbindungszeiten, Verbindungsadressaten und einiges mehr.

Damit lässt sich detailliert festhalten, wann und wie Nutzer online waren oder telefonierten. Strittig ist noch, ob die Datenmengen sechs oder gar bis zu 24 Monate aufbewahrt werden müssen. Der Bundestag hat im Februar mit Koalitionsmehrheit erklärt, die im Dezember 2005 beschlossene EU-Richtlinie umsetzen zu wollen.

EU-Bürger unter Generalverdacht

Für diese Daten interessiert sich nicht nur der Staat, auch Musik- und Filmindustrie frohlocken. Denn die könnten dann die IP-Adressen von Tauschbörsennutzern, die sie der Urheberrechtsverletzung verdächtigen, bequem mit den Nutzerdaten der Provider abgleichen – wenn auch nur mit richterlichem Beschluss. Der dürfte aber eine Formsache sein, nachdem im verabschiedeten Entwurf der Richtlinie die von EU-Parlamentariern geforderte Einschränkung gestrichen wurde, Daten nur bei schweren Straftaten anfordern zu können.

„Das ist Big Business“

Der schwedische Überwachungsexperte Pär Ström über die Unzulänglichkeiten und die Zweckentfremdung von Sicherheitstechnologie

Technology Review: Wer ist die treibende Kraft beim Einsatz von Überwachungstechnologien – die Industrie oder der Staat?

Pär Ström: Das politische Establishment ergreift jede Möglichkeit, die eigene Macht auf Kosten der Bürger auszubauen. Zumindest, solange eine Atmosphäre der Angst herrscht. Dafür werden jedes Mal Hard- und Softwareprodukte benötigt, und die müssen irgendwo bezogen werden. Das ist Big Business. Die Unternehmen wollen etwas verkaufen. Dabei schlagen die Systeme etwa zur Kontrolle von Flugpassagieren immer wieder falschen Alarm. Die echten Terroristen treten in so verschwindend geringer Zahl auf, dass sie in den Fehlermeldungen völlig untergehen. Außerdem wissen Terroristen von der Überwachung und stellen sich darauf ein. Die schicken dann erst mal Neulinge auf einen Testflug ohne Waffen, um zu sehen, ob ihre Leute erfasst sind.

Die USA implementieren ja gewaltige Systeme zur Erstellung von Profilen von Reisenden wie „CAPPS-2“ oder „Secure Flight“. Bringen diese Systeme mehr Sicherheit?

Das bezweifle ich, weil es das Problem einer Vielzahl so genannter „falscher Positivtreffer“ gibt. Das heißt, dass die Systeme jeden Tag Personen markieren, obwohl die in Wirklichkeit keine Bedrohung darstellen. Selbst US-Senator Edward Kennedy, der Bruder des ehemaligen Präsidenten John F. Kennedy, ist von einem derartigen



Mahrer: Pär Ström schrieb 2005 das Buch „Die Überwachungsmafia“

System schon als Verdächtiger herausgepickt worden – sein Name wurde von jemand anderem als Deckname benutzt.

Treten diese Pannen auch bei anderen Systemen auf?

Ja. Kürzlich wurde bekannt, dass die Software zur Erkennung betrügerischer Steuererklärungen der US-amerikanischen Behörden viele berechnete Ansprüche als vermeintliche Tricks ausgewiesen hat. Viele ehrliche Bürger werden folglich durch ihre Regierung drangsaliert.

Werden Sicherheitssysteme zweckentfremdet?

Schauen Sie sich das Verkehrsüberwachungssystem an, das Großbritannien gerade aufbaut. Videokameras an den Straßen, in Städten und an Tankstellen werden mit einer Software für die automatische Nummernschilderkennung ausgestattet. Jede Bewegung eines Fahrzeugs wird automatisch registriert und in Echtzeit mit einer Reihe von Datenbanken abgeglichen. Damit werden unversicherte Fahrzeuge erfasst und solche, die zur Fahndung ausgeschrieben worden sind. In diesem Fall wird dann ein Alarm ausgelöst. Darüber hinaus werden die Daten aber auch zwei Jahre lang im nationalen Polizeisystem gespeichert, die Frist soll sogar auf fünf Jahre ausgedehnt werden. Die Philosophie dahinter: Für den Fall, dass die Polizei im Nachhinein an einer bestimmten Person oder Gegend interessiert sein könnte, sollen die aufgezeichneten Spuren verfügbar sein. **INTERVIEW: STEFAN KREMPLE**



PICTURE-ALLIANCE/DPA

Verschärfte Grenzkontrollen: Wer in die USA einreist, muss das Kontrollprogramm „US Visit“ über sich ergehen lassen – Foto und Fingerabdrücke zur biometrischen Auswertung

Die Provider rechnen damit, dass sie der Aufbau der nötigen Technik für eine sechsmonatige Speicherung rund eine Million Euro kosten wird. Hinzu kämen noch die Betriebskosten. Ob das Geld gut ausgegeben ist, wird bezweifelt. „Wie bei der TKÜV stellt sich hier die Frage, ob da nicht mit Kanonen auf Spatzen geschossen wird“, sagt I&I-Sprecher Maurer. Im Prinzip stünden mit der Richtlinie 450 Millionen EU-Bürger unter Generalverdacht. Der Informatiker Hannes Federrath, der die Entwicklungsgruppe von JAP – einem Tool zum anonymen Websurfen – leitet, hält die Speicherung der Internetdaten für sinnlos. „Sie führt nur dazu, dass die Dummen gefangen werden. Die Cleveren benutzen internationale Datenrouten, die weiterhin Anonymität gewährleisten“, vermutet er.

In ihrer geplanten Form soll die Vorratsdatenspeicherung auch eine Ermittlung potenzieller Straftäter ermöglichen. Luc De Raedt, Data-Mining-Spezialist an der Uni Freiburg, hält dies für noch nicht machbar: „In den gespeicherten Daten ein Muster zu entdecken, das ein ernstlich kriminelles Verhalten charakterisiert, ist meines Erachtens jenseits des Standes der Technik im Data-Mining.“ Es sei unklar, ob die Kommunikation von Kriminellen andere Muster aufweise als diejenige unbescholtener Bürger. Hinzu komme, sagt De Raedt, dass kriminelle Aktivitäten so selten sind, dass sie auch dann schwer zu analysieren wären, wenn ihr Muster bekannt wäre.

Doch selbst wenn einige Attribute der Zielgruppe, ein Profil also, definiert wären – der Erfolg ist damit noch keineswegs sicher. Der New Yorker Polizeipräsident Raymond Kelly verdeutlichte dies kürzlich im Magazin „New Yorker“ am Beispiel der Londoner Bombenleger vom Juli 2005. Drei seien Briten pakistanischer Abstammung gewesen, einer Jamaikaner, und beim zweiten, vereitelten Anschlag habe man es mit drei Ostafrikanern zu tun

gehabt. Wonach hätte man da suchen sollen? Er hat nach seiner Amtsübernahme das „Racial Profiling“ sofort abgeschafft, weil es ineffektiv sei. „Ich glaube, Profiling ist einfach bekloppt“, wird Kelly zitiert.

Ein weiteres Problem von Hightech-Systemen, die unseren Datenschatten mehrten und verwalten: Obwohl sie die allgemeine Sicherheit erhöhen sollen, sind sie selbst nicht sicher vor Manipulation. Die Informatikerin Melanie Rieback von der Freien Universität Amsterdam demonstrierte Anfang des Jahres mit Kollegen, dass sich die Daten auf veränderbaren RFID-Chips so umschreiben lassen, dass sie die damit verknüpften Datenbanken durcheinander bringen oder gar einen Virus aktivieren. „Wir haben nur die Standardkonfiguration ausgenutzt“, sagt Melanie Rieback. Das zeige: „Kein System ist inhärent sicher.“

Der Übergang zum autoritären Sicherheitsstaat

Auch wenn die vorhandenen Überwachungssysteme noch in vieler Hinsicht unzulänglich sind und sich Staat und Wirtschaft noch schwer damit tun, den unaufhaltsam wachsenden Datenschatten des Bürgers detailliert auszuwerten: Die Daten liegen vor und sind kaum zu reduzieren. Zwar existieren Schutzwälle, die eine Verknüpfung bislang getrennter Datenbestände verhindern. Für die deutschen Sicherheitsorgane ist dies etwa die Trennung zwischen Geheimdiensten und Polizei. Doch mit jedem Anschlag wächst die Versuchung, diese Trennung aufzuheben. Für den Bremer Anwalt Rolf Gössner, der als Bürgerrechtler und Überwachungskritiker jahrelang illegal vom Verfassungsschutz bespitzelt wurde, ist die Zentralisierung deutscher Sicherheitsbehörden „bereits in vollem Gange“. „Wir gehen in die Richtung eines autoritären Sicherheitsstaates“, urteilt Gössner.

Die Mehrheit bemerkt den Übergang vom Rechtsstaat zum Unrechtsstaat gar nicht

Kritik kommt auch vom Bundesdatenschutzbeauftragten Peter Schaar. „In der Vergangenheit sind sowohl die polizeilichen als auch die nachrichtendienstlichen Befugnisse immer wieder erweitert worden“, sagt der Experte. Es sei nicht damit zu rechnen, dass diese in absehbarer Zeit revidiert werden. Dass viele Bürger sich über ihren Datenschatten kaum Gedanken machen, mag daran liegen, dass sie sich noch „wohl fühlen in der Orwellness“, wie es der Internetchronist Peter Glaser einmal ausgedrückt hat. Der digitale Datenabdruck ermöglicht ja erst all die neuen bequemen Online-Dienste. Ein allgegenwärtiger Big Brother ist nirgends zu entdecken. Genau das ist das Problem. Der ehemalige Düsseldorfer Polizeipräsident Hans Lisker hat es so formuliert: „An die Stelle des Freiheitsstaates wird der Kontrollstaat treten. Das alles wird rechtsstaatlich verlaufen, sodass die Mehrheit den Übergang vom Rechtsstaat zum Unrechtsstaat ... gar nicht bemerken wird.“