USA-Kolumne 3/2003

Inhalt

I. Das elektronische Panopticon – Auf dem Weg in eine neue „Sicherheitskultur“

Ein Tourist, der durch eine unbekannte Stadt schlendert, kommt an einem Sex-Shop vorbei und bleibt kurz vor dem Schaufenster stehen, bevor er weiter geht. Eine Woche später erhält er einen Werbebrief von dem Laden, der sich auf seinen „Kurzbesuch“ bezieht – zur großen Überraschung seiner Familie. Ein neues „Kunden-Identifikationssystem“ hatte mit Hilfe eines Signals von dem in seiner Fahrerlaubnis eingebetteten Micro-Chip die Adresse des Mannes ermittelt.

Dieses Szenario aus einem Bericht der American Civil Liberties Union (ACLU), einer gemeinnützigen Organisation, die sich für die Verteidigung der Bürgerrechte in den USA einsetzt, könnte bald Wirklichkeit werden, sollten sich derzeit sichtbare Trends fortsetzen. In ihrem Bericht „Bigger Monster, Weaker Chains“ (größeres Monster, schwächere Ketten) vom Januar diesen Jahres beschreibt die Organisation, wie die Kombination neuer Überwachungstechnologien mit der Lockerung der gesetzlichen Bestimmungen zum Schutz personenbezogener Daten sich zu einer ernsten Bedrohung des Privatlebens der U.S.-Bürger auswachsen könnte.

Im Jahr 1949 stellte sich der weltbekannte britische Autor George Orwell eine Welt vor, in der das Wort „Privatsphäre“ seine Bedeutung verloren hatte. Es gab keinen Ort, an dem man sich unbeobachtet aufhalten konnte. Aber selbst jemand, der Orwells Roman „1984“ in jenem Jahr las, mag diese Vorstellung noch für ein reines Hirngespinst gehalten haben. Inzwischen hat jedoch die Realität diese Vision schon beinahe eingeholt – dank gravierender Fortschritte bei der Entwicklung von Überwachungstechnologien.

Technologien, die eine solche Überwachung möglich machen, gibt es schon lange. Bisher waren sie wegen der hohen Kosten kaum bezahlbar. Inzwischen kosten sie jedoch so wenig, dass ihrer massenhaften Anwendung nichts mehr im Weg steht. Damit entsteht eine Infrastruktur, die unter bestimmten Voraussetzungen leicht missbraucht werden kann. Einige Experten sehen voraus, dass die Verbindung individueller Überwachungssysteme zu großen Netzwerken, die von privaten Firmen oder staatlichen Einrichtungen verwaltet werden, letztendlich unvermeidlich ist. Deshalb müssen jetzt

Rahmenbedingungen dafür geschaffen werden, die einen solchen Missbrauch auch in Zukunft möglichst unterbinden.

Am Zukunfts-Horizont erscheint die Möglichkeit der total überwachten Gesellschaft. Die technologischen Voraussetzungen sind zum Teil schon geschaffen oder im Entstehen begriffen. Und: Offensichtlich scheint es immer mehr „gute Gründe" zu geben, sich auf Schritt und Tritt beobachten lassen zu müssen. In den USA schreitet der gesellschaftliche Alltag einer neuen „Sicherheitskultur" entgegen.

II. Die Zukunft hat begonnen

Ob am Arbeitsplatz oder zu Hause, am Bankautomaten oder im Supermarkt, am Flughafen oder im Hotel, im Auto auf der Straße oder auf dem Parkplatz – die Wahrscheinlichkeit, dass eine Videokamera sich von den ganz alltäglichen Verrichtungen der U.S.-Amerikaner ein Bild macht, ist groß und wächst ständig. Ebenso die Zahl der gerechtfertigten Gründe für eine solche Überwachungstechnik.

Der Staat will Verbrechen verhüten und hofft auf höhere Aufklärungsquoten von Straftaten. Unternehmen wollen ihr Eigentum schützen und Sicherheit für Kunden und Mitarbeiter garantieren. Banken und Kreditkartenfirmen setzen sich gegen Betrüger zur Wehr. Städte und Gemeinden wollen einen möglichst reibungslosen Verkehrsfluss auf den Straßen. Öffentliche Einrichtungen wie Schulen, Krankenhäuser und Kirchen wollen die Sicherheit ihrer Schüler, Patienten und Mitglieder, ebenso wie die ihres Personals gewährleisten und den Zugriff Unbefugter auf sensible Informationen verhindern. Im Namen der öffentlichen Sicherheit wird das Gepäck von Flugpassagieren ohne deren Wissen durchsucht.

Die Überwachung der Telefon- und Internet-Benutzung ist in vielen großen U.S.-Unternehmen bereits alltäglich. Die American Management Association berichtete, dass sich unter den großen Arbeitgebern in den Vereinigten Staaten die Zahl derer, die auf irgendeine Weise die Aktivitäten ihrer Angestellten überwachten, sich in nur fünf Jahren, zwischen 1997 und 2001, auf 77,7 Prozent verdoppelt hat. Im Jahr 2001 kontrollierten 46,5 Prozent dieser Arbeitgeber gespeicherte E-mails; 37,7 Prozent hatten Videokameras aus Sicherheitsgründen installiert; 15,2 Prozent nutzten Videoaufzeichnungen zur Leistungsbewertung von Angestellten; 11,9 Prozent zeichneten Telefongespräche auf.

Aber nicht nur Organisationen aller Art springen auf das High-Tech Überwachungs-Karussell. Auch Privatleute geben immer mehr Geld aus, um ihr Eigentum und sich selbst besser zu schützen. Die Überwachungstechnik-Firma CCS International in New Rochelle im Bundesstaat New York schätzt, dass in den USA private Verbraucher bereits Überwachungstechnik im Wert von 6 Millionen U.S.-Dollar pro Tag kaufen, die nicht unbedingt immer legal ist.

Eltern wollen, dass ihre Kinder während ihrer Abwesenheit gut behandelt werden. Sie installieren sogenannte „Nanny Cams", kleine digitale Videokameras zur Überwachung von Kindern oder Haustieren, die sich leicht irgendwo im Kinderzimmer verstecken lassen, um so den Tagesmüttern bei der Betreuung ihrer Kinder auf die Finger schauen zu können. Ein Hersteller solcher Kameras ist die Firma Nanny Check, Inc. im Bundesstaat New York.

III. Digitale Augen

Die Marktforschungsfirma J.P. Freeman in Newton, Connecticut, berichtete im Januar 2003, dass in den USA bereits über 11 Millionen Überwachungskameras installiert sind, 42 Prozent der weltweiten Gesamtzahl. Der Markt hat schon jetzt ein Jahresvolumen von 150 Mio. US$ erreicht. Für die nächsten zehn Jahre sagt J.P. Freeman ein Wachstum von 40 bis 50 Prozent für digitale Überwachungskameras voraus. Der Markt für andere Formen der Überwachung (siehe unten) soll noch schneller wachsen.

Ein Haupt-Anwendungsbereich ist die Verbrechensbekämpfung. Polizeibeamte wollen Netzwerke von Videokameras nutzen, um hinterhältige Todesschützen, die zum Beispiel im Oktober 2002 die Bevölkerung in und um die Bundeshauptstadt Washington D.C. drei Wochen lang in Angst und Schrecken versetzten und 10 Menschen töteten, schneller ausfindig und unschädlich machen zu können. Der Fall machte auch private Unternehmen kooperationswillig. Im Stadtteil Georgetown von Washington D.C. verbinden nun Ladenbesitzer ihre Video-Überwachungsanlagen zu einem Netzwerk und stellen die Aufzeichnungen bei Bedarf der Polizei zur Verfügung. In einem neuen, zentralen Überwachungszentrum kann die Polizei der Stadt Videoaufnahmen aus öffentlichen Gebäuden, Straßen, U-Bahn Stationen und Schulen in Echtzeit verfolgen und sich die Gesichter von Menschen auf den Bildschirm zoomen.

Moderne Kameras können problemlos Gesichter aus 90 Meter Entfernung aufnehmen. Unbemannte, mit hochauflösenden Kameras ausgestattete Spionageflugzeuge, sogenannte „Drones", die bisher nur im Ausland zum Einsatz kamen, sollen in Zukunft auch im eigenen Land benutzt werden.

Digitale Videokameras werden auch zur Verkehrsüberwachung benutzt. Als im Sommer 2001 die Rekonstruktion einer Autobahnbrücke nahe Northampton, einer kleinen Stadt im Bundesstaat Massachusetts, monatelang erhebliche Rückstaus verursachte, startete die nahegelegene Universität, die University of Massachusetts, ein Versuchsprojekt, das die Frustration der Betroffenen verringern sollte. Ein System von digitalen Kameras, die auf Dächer oder Leitungsmasten nahe der Brückenauf- und -abfahrt angebracht wurden, zeichnet die Bilder der Autos auf, die auf die Brücke fahren und sie wieder verlassen. Die Nummernschilder werden maschinell identifiziert und so die zum Passieren der Brücke benötigte Zeit berechnet. Interessierte Autofahrer können sich nun jederzeit über das Internet informieren, wie lange sie voraussichtlich zum Überqueren der Brücke brauchen werden. Zwar werden die aufgezeichneten Daten sofort wieder gelöscht. Aber das könnte auch jederzeit geändert werden. Laufende Kosten des Systems: 600,00 US$ pro Monat.

Die Coolidge Brücke ist nur eins von vielen Tausend Beispielen wo Bürger – mit oder ohne ihre Einwilligung – überwacht werden. Nach Recherchen des New Yorker Aktivisten Bill Brown sind allein um Manhattan's Times Square herum, im Karree zwischen Fifth und Eight Avenue sowie zwischen der 42. und 50. Straße, mehr als 260 Überwachungskameras installiert.

Die Firma Axis Communications erwartet den größten Nachfrageschub für Kameras, die Bildaufzeichnungen über Computer und Internet zugänglich machen, nicht von großen sondern von kleinen Organisationen: Mietwohnungsverwaltungen, Kirchengruppen oder kleineren Ladenbesitzern, die ihre Gebäude und Innenräume ununterbrochen überwachen möchten.

IV. Mobilfunk-Lotsen

Videoüberwachung macht immer noch einen verschwindend geringen Teil aller Überwachungstechnologien aus. Andere werden zum Beispiel für den Mobilfunk entwickelt. Bis zum Jahr 2006 müssen in den USA alle Mobiltelefone so konstruiert sein, dass beim Anwählen der Nummer 911 für Notfälle der genaue Aufenthaltsort des Anrufers automatisch übermittelt wird. Damit soll zum Beispiel die Hilfeleistung bei Verkehrsunfällen, medizinischen Notfällen und Bränden verbessert werden.

Mobiltelefon-Anbieter wollen mit der gleichen Technologie dem jeweiligen Aufenthaltsort angepasste Dienstleistungen entwickeln. So soll ein Reisender zum Beispiel unterwegs durch zielgerichtete Werbung auf Restaurants vor Ort aufmerksam gemacht werden, die seinen kulinarischen Vorlieben entsprechen.

V. Biometrische Erkennung

Eine noch im Entwicklungsstadium befindliche Gruppe von Technologien beschäftigt sich mit der Identifikation von Personen durch einzigartige Körpermerkmale. Diese reichen von Fingerabdrücken über Augenbeschaffenheit zur Gesichtsgeometrie, die durch Kameras oder Sensoren aufgezeichnet und digitalisiert werden. Einige U.S.-Firmen arbeiten fieberhaft an sogenannten „DNA-Chips", die an Ort und Stelle den für jeden Menschen einmaligen „genetischen Fingerabdruck" erkennen sollen. Auch an Verfahren zur Erkennung der Stimme und des Körpergeruchs wird gearbeitet.

Konventionelle Fingerabdruck-Scanner werden in den USA bereits als Sicherheitsmechanismus in Bürogebäuden eingesetzt, aber auch zunehmend bei der Bezahlung in Supermärkten oder Schnellrestaurants sowie bei Sozialhilfeempfängern, um Leistungs-Missbrauch zu unterbinden.

Auch Gesichtserkennungsverfahren mit Hilfe von Videokameras befinden sich im Teststadium. In den letzten Jahren wurde ein solches Verfahren zum Beispiel in einem großen Sportstadion sowie in Flughäfen getestet. Dabei werden die von einer digitalen Videokamera aufgenommenen Bilder mit in einer Datenbank gespeicherten Fotos verglichen, zum Beispiel denen von bekannten und gesuchten Straftätern. Bisher waren die Testergebnisse unzureichend. Aber es steht außer Frage, dass in den kommenden Jahren entscheidende Fortschritte erreicht werden können.

Zu den Hauptinvestoren in biometrische Technologien gehören Banken und Kreditkartenfirmen sowie Spielcasinos, die Betrügern auf die Spur kommen wollen. Aber auch Behörden, die für die Sicherheit von Flughäfen verantwortlich sind, haben großes Interesse.

VI. Sprechende Produkte

Eine weitere vielversprechende Technologie sind winzige Mikrochips, die miteinander kommunizieren und an beliebiger Stelle angebracht werden können. Nach Angaben

der Automotive Industry Action Group, einer Denkfabrik der Autoindustrie, planen die drei großen U.S.-Autohersteller, die Reifen ihrer Fahrzeuge mit winzigen Funksendern (radio transponders) auszustatten. Diese können bei einer Fahrgeschwindigkeit bis zu 160 km/h identifiziert werden. Auch elektronische Straßen-Maut-Zahlungsautomatenm, wie sie zum Beispiel die Firma SAMSys Technologies in Richmond Hill, Ontario, anbietet, registrieren die genauen Merkmale des jeweiligen Fahrzeugs. Die sogenannten „radio frequency identification tags", auch RFID-Chips genannt, werden auch bereits für andere kommerzielle Anwendungen getestet.

Der U.S.-amerikanische Rasierklingenhersteller Gillette stattete in diesem Jahr bereits 500 Millionen „Mach 3 Turbo" Rasierer mit solchen „Identifikatons-Etiketten" aus. Im Zusammenspiel mit sogenannten „intelligenten Regalen" wird automatisch registriert, wenn ein Produkt aus dem Regal entnommen wird. Somit weiß das Verkaufspersonal genau, wann das entsprechende Regal neu bestückt werden muss. Aber auch Ladendiebstahl könnte auf diese Weise unterbunden werden. Gleichzeitig werden Verbraucher, ohne es zu wissen, zu mobilen Funksendern gemacht.

Weitere Anwendungen für die Chips sind geplant: Sie sollen Patienten in Krankenhäusern überwachen, die unter Quarantäne stehen, und verhindern, dass sich Besucher von Firmen Zugang zu geheim gehaltenen Unterlagen von Klienten oder aus der eigenen Entwicklungsabteilung verschaffen. In jedes nur denkbare Objekt integriert, könnten es die Chips möglich machen, zum Beispiel den gesamten Inhalt einer Handtasche oder eines Koffers zu identifizieren. Prinzipiell könnten die RFID-Chips auch unter die Haut implantiert werden.

Nach Angaben von ACLU hat eine Autovermietungsfirma bereits den Versuch unternommen, einen Kunden wegen überhöhter Geschwindigkeit zur Kasse zu bitten. Die Firma hatte in dem Mietwagen ein Gerät angebracht, das mit Hilfe des weltumspannenden Global Positioning Systems (GPS) die Verkehrssünde registriert hatte. Auf die gleiche Art und Weise könnten Unternehmen die Benutzung von Firmenfahrzeugen durch ihre Angestellten überwachen.

Eine ganze Reihe von Firmen entwickelt tragbare Geräte, die es Eltern ermöglichen sollen – zum Beispiel auf ein Armband montiert – mit Hilfe von Satelliten-gestützter Datenübertragung, vom Arbeitsplatz aus den jeweiligen Aufenthaltsort ihrer Kinder zu überwachen.

VII. Digitale Spürhunde

Im Zeitalter von Computer und Internet wächst die Zahl der „Datenspuren", die wir hinterlassen, täglich. Das Internet ist bereits heute die größte öffentlich zugängliche Datenbank für persönliche Informationen. Und seit Unternehmen in personenbezogenen Informationen einen Schlüssel zum Marketing-Erfolg sehen, und neue Technologien das Sammeln und Speichern solcher Daten möglich machen, boomt der Markt für solche „Ware". Eine ganze Reihe von Firmen, so zum Beispiel Acxiom und Choice Point, haben aus dem Sammeln von personenbezogenen Informationen ein einträgliches Geschäft gemacht. Auch gibt es Firmen, die ihre Kunden-Informationen in Gemeinschafts-Datenbanken einbringen, um so ein umfassenderes Bild ihrer eigenen Kundschaft zu erhalten.

Laut ACLU macht auch der Staat regen Gebrauch von dem in kommerziellen Datenbanken gesammelten Material. Viele Regierungsstellen pflegen auch riesige eigene Datenbestände. Das FBI verwaltet Millionen digitalisierter Fingerabdrücke. Das Department of Health and Human Services unterhält eine Datenbank über jede neu eingestellte Arbeitskraft im gesamten Land. Das Bildungsministerium sammelt Angaben zur Schulausbildung von Millionen U.S.-Amerikanern. Die Fahrerlaubnisstellen der Bundesstaaten sammeln Fotos aller Einwohner, die eine Fahrerlaubnis besitzen.

Nicht einmal vor den intimsten Informationen machen die Datensammler halt. Die Vertraulichkeit der Beziehung zwischen Arzt und Patient wird zum Relikt der Vergangenheit. Inzwischen lassen Arztpraxen, Kliniken und Krankenhäuser private Versicherer, Arbeitgeber und andere „Interessenten" in ihre elektronischen Akten schauen. Das Medical Information Bureau hat sogar eine zentrale Datenbank für seine Mitglieder aus der Versicherungswirtschaft angelegt, die personenbezogene medizinische Informationen von über 15 Millionen Patienten enthält. Die Firma Genelex, die genetische Tests durchführt, hat nach Angaben von ACLU bereits rund 50.000 DNA-Proben in ihrer Datenbank gesammelt.

Unterstützt durch die Centers for Disease Control and Prevention, eine Abteilung des U.S.-Gesundheitsministeriums, will eine Forschergruppe an der medizinischen Fakultät der Harvard Universität die Akten von 20 Millionen Patienten in U.S.-Krankenhäusern nach gehäuft auftretenden Symptomen untersuchen, die durch Bioterror verursacht sein könnten.

Von Seiten der Wirtschaft versuchen private Firmen, sich möglichst Informationen über potentielle Kunden und Geschäftspartner zu beschaffen. Ein Beispiel ist die Regulatory Data Corporation, die von 19 weltweit agierenden Unternehmen im Finanzbereich im Juli 2002 gegründet wurde. Das Konsortium will Kundendaten der betreffenden Unternehmen zusammenführen, um Geldwäsche, Betrug, Korruption und organisiertes Verbrechen zu bekämpfen. Dabei will das Unternehmen Informationen aus rund 20.000 öffentlich zugänglichen Quellen, darunter Veröffentlichungen in den Medien, in einer riesigen Datenbank zusammenfassen, der sogenannten Global Regulatory Information Database.

Auch kleinere Banken in den USA bieten inzwischen Informationen über ihre Kunden, einschließlich solcher Details wie Kontenbewegungen und Kreditkartenkäufe zum Verkauf an andere Firmen feil.

Sieben der zehn größten Supermarkt-Ketten in den USA registrieren mit Hilfe von Rabattkarten die Einkaufsgewohnheiten ihrer Kunden. Für die entsprechende Mitgliedschaft, die der Kunde beantragt, kann er zu günstigeren Konditionen einkaufen, wenn er dabei seine Plastikkarte benutzt, die dann alle Einkäufe an der Kasse registriert.

VIII. Technische Hürden

Zum Orwell'schen Szenario gibt es kaum noch technische Barrieren. Vor allem die Kombination von mehreren Überwachsungstechnologien mit Mikroelektronik und winzigen optischen Bauelementen, Satelliten-unterstützten Netzwerken für drahtlose Datenübertragung, digitalen Datenspeichern mit enormer Kapazität, immer leistungsfähigeren Mikroprozessoren und Computern und Datenbank-Software macht die „totale Überwachungsgesellschaft" theoretisch bereits heute möglich.

Sollten sich die Leistungsparameter von Prozessoren, Datenspeichern und Übertragungsmedien weiter in so hohem Tempo steigern wie bisher, dann könnte in 20 Jahren ein dem heutigen Personalcomputer ähnliches Gerät ausreichen, um jeden U.S.-Einwohner zu überwachen.

Die Kombination von Überwachungstechnik und computergestützten, vernetzten Datenbanken bildet die Basis für eine universelle Überwachungs-Infrastruktur. So wird zum Beispiel Software entwickelt, die von verschiedenen digitalen Videokameras aufgenommene Bilder zu Panorama-Aufnahmen eines ganzen Raumes verschmilzt.

Während die Größe der Bauteile schrumpft, werden die zu verarbeitenden Datenberge immer größer. Dabei gibt es allerdings noch einige technische Herausforderungen zu meistern. Die großen zu bewältigenden Datenmengen bereiten dabei weniger Probleme als deren sinnvolle Auswertung.

Erfahrungen mit großen Datenmengen gibt es bereits aus der biotechnologischen Forschung. Biometrische Informationen wie zum Beispiel Fingerabdrücke, und andere Bildaufzeichnungen können heute auf wenige Kilobyte Speicherplatz komprimiert werden, was etwa der Länge einer einfachen E-mail-Nachricht entspricht.

Aber Projekte wie SETI@Home, welches das Weltall mit Hilfe von Radioteleskopen nach Zeichen intelligenten Lebens durchforstet, haben gezeigt, dass die sinnvolle Auswertung von Datenbanken um so schwerer wird, je komplexer das Datenmaterial ist. Oft sind die Ergebnisse solcher Untersuchungen nutzlos.

Eine der größten Herausforderungen entsteht durch die Tatsache, dass es in jeder Datenbank falsche Daten gibt. Angefangen bei Rechtschreibfehlern oder falsch gesetzten Kommas, bis hin zu falschen Zuordnungen von Informationen – Fehlerquellen lauern überall. Werden verschiedene Datenbanken verschmolzen, kommt es auf Grund unterschiedlicher Datenformate oder durch andere Ursachen oft dazu, dass sich die Zahl falscher Informationen vervielfacht.

Die Datenbank-Spezialisten der U.S.-Firma Information Impact schätzen den Anteil falscher Einträge mit mindestens einem gravierenden Fehler in großen Kunden-Datenbanken auf mindestens 20 bis 35 Prozent. Dazu kommt noch die relativ unausgereifte Technologie „intelligenter Suchmaschinen". Bei einer Fehlerquote von nur einem Prozent würde ein nationales Terrorismus-Überwachungssystem bereits Tausende falscher Alarms auslösen und unschuldige Menschen zu Verdächtigen machen.

IX. Rechtliche Fesseln gelockert

In Sachen Datenschutz gelten die USA seit langem als rückständig. Schon vor dem 11. September 2001 waren die Einwohner der Vereinigten Staaten schlechter vor unerwünschten Datensammlern geschützt als die Bevölkerung anderer Industriestaaten. Ein umfassendes Datenschutzgesetz zum Schutz der Privatsphäre, wie zum Beispiel in Deutschland, gibt es nicht, dafür viele einzelne Rechtsvorschriften auf Bundes- und Landesebene.

Oft zum Vorteil der privaten Wirtschaft, erlauben diese Vorschriften kommerziellen Datensammlern den Zugriff auf zum Teil höchst sensible personenbezogene Daten. Pri-

vate Krankenversicherungen haben Einsicht in Patienten-Akten. Lebensversicherer verlangen in ihren Antragsformularen Angaben zur persönlichen Krankheitsgeschichte. Banken, Kreditkarten-Firmen und Supermarktketten, zeichnen die Kaufgewohnheiten ihrer Kunden auf.

Andererseits gibt es eine lange angelsächsische Rechtstradition, die staatlichen Behörden vor allem bei der Verfolgung von Verdächtigen hohe Hürden aufbaut, um die Rechte des Individuums auf Freiheit und faire Behandlung zu wahren. U.S.-Bürger sind gegen unverhältnismäßige Verfolgung verfassungsrechtlich geschützt. Durchsuchungen und Überwachungen sind grundsätzlich nur dann zulässig, wenn ein auf einem konkreten Verdacht zum Rechtsbruch beruhender richterlicher Durchsuchungsbefehl vorliegt, welcher genau beschreiben muss, wonach an welchem Ort gesucht werden soll.

Ein wegweisendes Urteil des U.S.-amerikanischen Bundesverfassungsgerichts schloss im Jahr 1967 auch elektronische Überwachungsmethoden in diese Regelung ein. Der Staat, so die Meinung der Richter, habe nicht das Recht, Menschen uneingeschränkt an Orten zu überwachen, wo diese sich in angemessener Sicherheit wähnten – so zum Beispiel in einer Telefonzelle.

Die folgenschweren Terroranschläge vor 18 Monaten haben ein öffentliches Klima der Angst und des Misstrauens geschaffen, welches es der U.S.-Regierung ermöglichte, die rechtlichen Beschränkungen zur Überwachung von Personen innerhalb der Vereinigten Staaten, vor allem auch der eigenen Bürger, gravierend zu schwächen.

Nur sechs Wochen nach den Anschlägen, als das Land noch in einem schweren Schockzustand war, schaffte es die Administration unter George W. Bush, eine entsprechende Gesetzesvorlage als das sogenannte „USA PATRIOT Act" durch das Parlament bestätigen zu lassen.

Das Gesetz gibt staatlichen Behörden ein bisher ungekanntes Maß an Freiheit beim Sammeln von personenbezogenen Informationen. Behörden, Universitäten, Bibliotheken, Arztpraxen und Internet-Firmen müssen bei Bedarf ihre Datenbanken und Archive öffnen, ohne dass ein hinreichender Verdacht auf kriminelle Aktivitäten vorliegen muss. Häuser oder Büros können in Abwesenheit des Eigentümers durchsucht werden, ohne dass der Betreffende unmittelbar vor- oder nachher darüber informiert werden muss. Ähnliches gilt für das Überwachen von Telefongesprächen und Korrespondenz per E-Mail.

Das U.S. Verteidigungsministerium will Informationen über Millionen von Menschen durchforsten, um Kriminelle und Terroristen ausfindig zu machen. Das „Total Information Awareness" Projekt (TIA) soll der Behörde unkompliziert Zugriff auf alle weltweit verfügbaren Datenbanken verschaffen und könnte die Zusammenstellung eines persönlichen digitalen Dossiers für jeden Einwohner der Vereinigten Staaten zur Folge haben. Personenbezogene Daten aus staatlichen, medizinischen, kommerziellen und anderen Quellen sollen einen riesigen Informationspool über U.S.-Bürger und Ausländer mit Kontakten in die Vereinigten Staaten schaffen. Erklärtes Ziel sind das Aufspüren, Klassifizieren, und Identifizieren von Terroristen und die Verhinderung von Terroranschlägen.

Dieses Vorhaben stieß auf massiven Widerstand von Bürgern und Abgeordneten. Im Februar dieses Jahres beschloss der U.S.-Kongreß, dass sich das Pentagon die Einführung dieses Projektes vom Parlament genehmigen lassen muss. Aber die U.S.-Regierung unter George W. Bush hatte innerhalb von drei Wochen ein ähnliches, vom Geheimdienst CIA gesteuertes Projekt auf den Weg gebracht: das „Terrorist Threat Integration

Center" (TIC). Ziel ist der Aufbau einer gigantischen Datenbank, die persönliche Daten von Einwohnern und Besuchern der USA speichern soll. Dabei sollen unter anderem die Kommunikationsströme im Internet überwacht werden. Anbieter von Internet-Zugängen sollen eine „Black Box" installieren, die die Überwachung der E-Mail-Kommunikation konkreter Personen ermöglicht. Dabei können aber auch alle E-Mails von anderen Nutzern dieses Anbieters aufgezeichnet werden.

Das U.S.-Außenministerium öffnete seine Datenbank mit 50 Millionen Visa-Anträgen den Polizeibehörden. Ein weiteres Projekt, welches dem Kampf gegen den Terrorismus dienen soll, ist das Computer Assisted Passenger Pre-Screening System II (CAPPS II) der U.S.-Behörde für Verkehrssicherheit, Transportation Security Agency. Persönliche Daten von Reisenden sollen gesammelt und gespeichert werden und jede Person dann in eine von drei Sicherheits-Kategorien eingestuft werden – ohne die Betreffenden davon in Kenntnis zu setzen.

Auch in anderen Fällen werden die Betroffenen ohne ihr Wissen überwacht. Aber es gibt auch Widerstand gegen derartige Praktiken. Am 27. Mai 2003 lehnte das Landesparlament des Bundesstaates Texas in zweiter Lesung einen Gesetzentwurf ab, der es den texanischen Sicherheitsbehörden erlauben sollte, eine Datenbank mit biometrischen Merkmalen aller Personen anzulegen, die im Besitz einer Fahrerlaubnis sind.

Die U.S.-Regierung schlug außerdem vor, Briefträger, Handwerker und andere Personen, die mit vielen Bürgern in ihren Häusern in Kontakt kommen, als Informanten anzuheuern. Auch diese Idee stieß auf massiven öffentlichen Widerspruch. Im November 2002 verbot das Parlament der Regierung die Umsetzung des so genannten „TIPS" Projektes. Im Juli 2003 verabschiedete das von den Republikanern kontrollierte Landesparlament des Bundesstaates Alaska eine Resolution, die das USA PATRIOT Act als Eingriff in die Freiheitsrechte der US-Bürger verurteilt.

X. Elektronisches Panopticon

Im Jahr 1791 hatte der britische Philosoph Jeremy Bentham die Vorstellung eines neuartiges Gefängnisses. In der Mitte des kuppelartigen Raumes, in dem alle Gefangenen verwahrt wurden, stand ein zentraler Kontrollturm, von dem aus die Gefängniswärter über die Insassen wachten. 38 Jahre später wurde das erste Panopticon der Welt in Philadelphia, an der Ostküste der Vereinigten Staaten gebaut. Während die einzige Verbindung jedes Gefangenen zur Außenwelt ein Blick zum Himmel aus dem Dachfenster seiner Einzelzelle war, hatten die Aufpasser - für die Gefangenen unsichtbar – einen Überblick über den gesamten Raum.

Die Panopticon-Studien des niederländischen Architekten Rem Koolhaas zeigten, dass Gefängnis-Insassen im Lauf der Zeit trotzdem Wege fanden, sich der Beobachtung durch die Wächter zu entziehen. Auch eine „elektronische Überwachungsgesellschaft" würde derartige „panoptische Effekte" mit sich bringen und damit die Zweckmäßigkeit eines solch gigantischen Systems in Frage stellen.

Inzwischen sind sich jedoch viele Experten in Wissenschaft und Forschung einig, dass die Elemente einer totalen Überwachungsgesellschaft in den USA schon vorhanden sind oder gerade entstehen. Und zwar, weil es die U.S.-Amerikaner so wollen. Die „totale Überwachungsgesellschaft" könnte aus dem Wunsch der Menschen nach Sicherheit, Kontrolle und Bequemlichkeit erwachsen. Jede Art von Überwachung mag vorteil-

haft für den jeweiligen Benutzer und Zweck sein. Ihre Kombination zu all-umfassenden Überwachungssystemen könnte allerdings unerwünschte Folgen haben: zum Beispiel das allmähliche Verschwinden der Privatsphäre.

Im Zusammenhang mit der Sammlung und Auswertung personenbezogener Daten ergeben sich zwei Haupt-Problempunkte. Der erste ist die Frage, wem gegenüber die Partei, die personenbezogene Daten sammelt, Rechenschaft schuldig ist, bzw. wie der Zugang zu solchen Daten kontrolliert wird. Auch die Veränderung solcher Daten muss genau überwacht und kontrolliert werden. Das zweite Hauptproblem ist, in welcher Weise zu einem bestimmten Zweck gesammelte und gespeicherte Daten später zu einem ganz anderen Zweck von Dritten ausgewertet werden können.

Tausende Datenbanken existieren bereits in Behörden und Unternehmen, Krankenhäusern und Arztpraxen. Diese noch isolierten Daten könnten in Zukunft verknüpft werden. Die Kombination der vorhandenen Video- und Datenaufzeichnungen in persönlichen Dossiers könnte in einem „hochauflösenden Bild des Privatlebens" der Menschen kombiniert werden.

Unter den beschriebenen Umständen wäre eine nicht mehr so „harmlose" Fortsetzungsgeschichte des eingangs erwähnten ACLU Szenarios denkbar: Gerade zu der Zeit, als der Mann sich in der Stadt X als Tourist aufhielt, wurde in dem Stadtviertel, in dem sich der Sex-Shop befand, ein Sexualverbrechen begangen. Die Polizei der Stadt X, die uneingeschränkten Zugang zu allen verfügbaren Datenbanken hat, nimmt den Mann in den Kreis der Verdächtigen auf. Eine Untersuchung seiner Internet-Gewohnheiten bringt zum Vorschein, dass der Mann einige Massen-E-mails mit pornografischem Inhalt geöffnet hat (‚die allesamt ungebeten in seiner Mailbox gelandet waren). Daraufhin wird der Mann auf die Liste der potentiellen Verdächtigen gesetzt…

Um einen Missbrauch personenbezogener Daten zu verhindern, sollte der Zugriff streng selektiv mit Hilfe von Autorisierungssystemen erfolgen, die auch alle Zugriffe auf Daten genau registrieren. Die Einführung wirksamer Kontrollmechanismen würde voraussetzen, dass die U.S.-Amerikaner sich die Gefahren vor Augen führen, die ein umfassendes Überwachungssystem langfristig mit sich bringen könnte. Dass unter den derzeitigen Bedingungen strikte Kontrollmechanismen in die entstehenden Überwachungssysteme eingebaut werden, scheint zweifelhaft. Zu sehr steht der Schutz vor weiteren Terroranschlägen im Vordergrund bei der inneren Sicherheitspolitik – jedenfalls in der öffentlichen Diskussion. Die Terroranschläge haben die Einstellung der U.S.-Amerikaner in Sachen Privatsphäre stark beeinflusst.

Sind Überwachungssysteme erst einmal eingeführt, werden sie auch benutzt werden – zu immer mehr Zwecken. Auf lange Sicht liegt die Gefahr darin, dass sich im Lauf der Zeit ein gewisser Gewöhnungseffekt einstellt. Kinder, die mit Videokameras im Kinderzimmer aufwachsen, werden sich daran später am Arbeitsplatz nicht stören. Letztendlich könnte die Überwachung allumfassend werden, so dass man sich nirgendwo im öffentlichen Raum mehr unbeobachtet bewegen kann.

XI. Transparente Zivilgesellschaft

Viele Experten glauben heute bereits, dass die universelle Verbreitung von vernetzten Überwachungssystemen nicht mehr aufzuhalten ist. Sie stellen deshalb die Frage, wie deren Missbrauch verhindert werden kann. Einer von ihnen ist Science Fiction Autor

David Brin, der in seinem 1998 veröffentlichten Buch voraussagte, dass die USA unaufhaltsam den Weg zur „transparenten Gesellschaft" beschritten hätten. Brin glaubt, dass der Verlust der Privatsphäre, zumindest außerhalb der eigenen vier Wände, unausweichlich ist und fordert deshalb seine Mitmenschen auf, aus der Not eine Tugend zu machen.

Anstatt eine all-umfassende Überwachungs-Infrastruktur ausschließlich als Gefahr für die Demokratie und für die Freiheit des Individuums anzusehen, sieht er darin auch ein mögliches Mittel zu deren Stärkung. Für Brin ist es entscheidend, ob die Macht, andere zu überwachen, nur in den Händen Weniger konzentriert ist, oder ob sie praktisch von allen gleichermaßen ausgeübt werden kann. Anstatt den seiner Meinung nach zum Scheitern verurteilten Versuch zu machen, die „öffentliche Privatsphäre" zu retten, sollten wir eine Gesellschaft gestalten, die für alle gleichermaßen durchschau- und kontrollierbar ist. Alle Organisationen, die Datenbanken mit personenbezogenen Informationen besitzen, müssten Betroffenen jederzeit Einsicht gewähren und genaue Aufzeichnungen darüber führen, an wen diese zu welchem Zweck herausgegeben wurden.

Lawrence Lessig, Rechtsprofessor an der renommierten Stanford University, kann sich ein System vorstellen, dass ähnlich funktioniert wie das der „credit reports", die Banken und Unternehmen Auskunft über die Kreditwürdigkeit einer Person geben. Aufgenommene Kredite und das Zahlungsverhalten, aber auch abgelehnte Kreditanträge werden dort von einer kleinen Zahl autorisierter Firmen registriert. Der Betreffende kann jederzeit Einsicht in die Eintragungen nehmen und fordern, dass falsche Daten wieder gelöscht werden. Der persönliche Kreditbericht gibt auch darüber Auskunft, wer sich Zugang zu diesen Informationen verschafft hat.

In der gleichen Weise sollten Bürger ihre Regierung und private Unternehmen bei der Überwachung von Bürgern und Verbrauchern kontrollieren und wenn nötig zur Verantwortung ziehen. Nur, wenn Überwachungstechnologien ausschließlich von bestimmten Eliten angewandt werden, ist die Demokratie in Gefahr. Der beste Weg, unsere individuelle Freiheit zu bewahren mag es sein, die Idee von einer Privatsphäre aufzugeben.

Zum Weiterlesen:

Amato, Ivan. Big Brother Logs On. Technology Review, September 2001. Siehe http://www.technologyreview.com/articles/amato0901.asp

Farmer, Dan; Mann, Charles C. Surveillance Nation: Part One. Technology Review, April 2003, 34-43. Siehe http://www.technologyreview.com/articles/farmer0403.asp

Farmer, Dan; Mann, Charles C. Surveillance Nation: Part Two. Technology Review, Mai 2003, 46-53. Siehe http://www.technologyreview.com/articles/farmer0503.asp

Garfinkel, Simson. I see you. Technology Review, 5. März 2003. Siehe http://www.technologyreview.com/articles/wo_garfinkel030503.asp

Givens, Beth. A Review of Current Privacy Issues. Privacy Rights Clearinghouse, San Diego, März 2001, aktualisiert Oktober 2002. Siehe http://www.privacyrights.org/ar/Privacy-IssuesList.htm

Hogan, Kevin. Will Spyware Work? Technology Review, September 2001. Siehe http://www.technologyreview.com/articles/hogan1201.asp

Safire, William. You Are A Suspect. New York Times, November 14, 2002.

Schmidt, Charlie. Beyond the Bar Code. Technology Review, März 2001. Siehe http://www.technologyreview.com/articles/schmidt0301.asp

Stanley, Jay; Steinhardt, Barry. Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society. American Civil Liberties Union, Januar 2003, 18 S. Siehe http://www.aclu.org/Privacy/Privacy.cfm?ID=11573&tc=39

Talbot, David. Tracking Trucking. Technology Review, 9. Januar, 2002. Siehe http://www.technologyreview.com/articles/wo_talbot010902.asp

Bücher zum Thema:

Agre, Phillip E.; Rotenberg, Marc. Technology and Privacy: The New Landscape. MIT Press, Juli 1998, 336 S.

Brin, David. The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom? Perseus Publishing, Mai 1998, 384 S.

Garfinkel, Simson. Database Nation: The Death of Privacy in the 21st Century. O'Reilly & Associates, Januar 2001, 336 S.

Monmonier, Mark S. Spying With Maps: Surveillance Technologies and the Future of Privacy. University of Chicago Press, November 2002, 264 S.

Whitaker, Reginald. The end of Privacy: How Total Surveillance Is Becoming a Reality. New Press, Februar 2000, 208 S.

Organisationen, die sich mit dem Thema „Überwachungs-Technologien und Privatsphäre“ beschäftigen:

American Civil Liberties Union (ACLU)
1920 gegründete gemeinnützige Organisation zur Verteidigung der Bürgerrechte in den USA mit Büros in den meisten Bundesstaaten, die von fast 300,000 Menschen finanziell unterstützt wird und rechtlich gegen die Verletzung von Bürgerrechten vorgeht. Siehe:
http://www.aclu.org, bzw. themenbezogen
http://www.aclu.org/Privacy/PrivacyMain.cfm

Center for Democracy and Technology (CDT)
Gemeinnützige Organisation, die sich für demokratische Werte und Verfassungsrechtliche Freiheiten im digitalen Zeitalter einsetzt. Siehe:
http://www.cdt.org

Electronic Privacy Information Center (EPIC)
1994 gegründetes Forschungszentrum in Washington, D.C., das die Öffentlichkeit über aufkommende Probleme im Zusammenhang mit verfassungsrechtlich garantierten Rechten und Freiheiten aufklärt. Siehe:
http://www.epic.org

Privacy Foundation
Untersucht Kommunikationstechnologien und Dienstleistungen, die die Privatsphäre von Bürgern beeinträchtigen können und veröffentlicht Projektberichte. Siehe:
http://www.privacyfoundation.org

Privacy Rights Clearinghouse, PRC
1992 gegründetes Projekt des Utility Consumers Action Network in San Diego, Kalifornien; Will das Bewußtsein von Konsumenten dafür schärfen, wie Technologie ihre Privatsphäre beeinflusst und setzt sich für deren Schutz ein. Siehe:
http://www.privacyrights.org

XII. Tipp (nicht nur) für Zukunftsforscher:

Jede Wirkung hat eine Gegenwirkung

Jede neue Technologie, jede Maßnahme, die Arbeitsabläufe in einer gewünschten Weise verändern soll, bringt auch – oft unerwünschte – Nebenwirkungen mit sich. Viele solcher negativen Effekte sind aber durchaus vorhersehbar, wenn sie nicht in der Planungsphase vernachlässigt werden.

Die American Management Association schätzt, dass in über drei Viertel der großen U.S.-Unternehmen Angestellte in irgendeiner Weise bei ihrer Arbeit elektronisch überwacht werden. Auch das führt zu unerwünschten Nebeneffekten. Mitarbeiter schränken den Informationsaustausch mit ihren Kollegen ein. Ein Angestellter, der gerne zu Hause anrufen würde, um sich danach zu erkundigen, wie es seinem kranken Kind geht, bleibt stattdessen gleich zu Hause.

Welche neuen Produkte, Technologien oder Abläufe werden in Ihrem Unternehmen eingeführt?
Welcher Nutzen soll damit erreicht werden?
Welche unerwünschten Nebenwirkungen könnte diese Maßnahme nach sich ziehen?
Wie könnte diesen Negativ-Wirkungen vorgebeugt werden?

E-mail: gimmethenews@att.net

Seit 1997 beschäftigt sich Evelyn Hauser als freie Autorin mit Zukunftsforschung in den USA und recherchiert Informationen über zukunftsrelevante gesellschaftliche, wirtschaftliche, und technologische Entwicklungen in den Vereinigten Staaten für deutsche und US-amerikanische Kunden.
Z_beiträge: USA-Kolumne 3/2003 – 01.08.03