Hans G. Zeger[1],

Big Brother is watching You

(Herbstkonferenz Katholische Aktion Österreich, 1.10.2004, Tainach/Kärnten)

Das Konzept der Privatsphäre ist in der Informationsgesellschaft noch immer unverstanden. Die bestehenden Regelungen zum Datenschutz sind zu sehr mit bürokratischen Mechanismen belastet und für die Durchsetzung der Betroffenenrechte nicht effizient genug. Durch die fortschreitende Vernetzung von Daten werden die Handlungsmöglichkeiten des Menschen im politischen, privaten und beruflichen Leben, aber auch als Konsument, zusehens eingeengt und kontrolliert. Nicht ein großer Bruder, sondern viele gläserne Mauern sind die aktuelle Bedrohung unserer Freiheit.

WER IST DER BIG BROTHER?

Das seit Orwell geflügelte Wort muss seit einigen Jahren neu hinterfragt werden. Stand bei George Orwell "Big Brother" als Chiffre für den totalitären Staat schlechthin, finden sich heute - zumindest in Europa - keine derartigen Staatsgebilde.

Warum genießt die "Big Brother"-Chiffre noch immer derartige, wenn nicht sogar steigende Anziehungskraft? Nicht nur Gegner des Überwachungstaates, sondern Voyeure und Befürworter totaler Überwachung berufen sich auf ihn, wie das bekannte Sendeformat zeigt oder die Namensgebung eines Spyware-Produzenten, der sein Produkt sinnigerweise 'Orvell' nannte.

Unsere Gesellschaft akzeptiert also ein Leben mit dem "Big Brother", machen wir uns auf die Spurensuche nach ihm.

SCHUTZ DER PRIVATSPHÄRE EIN HOHES GUT?

Die Idee, das Menschen Privatsphäre haben, ist ein modernes Konstrukt und wurde 1890 erstmals öffentlich formuliert . Samuel D. Warren und Lois D. Brandeis, zwei Bostoner Anwälte veröffentlichten in der Harald Law Review den Artikel "The Right of Privacy".

Kern der Argumentation ist das Recht "allein gelassen zu sein" ("the right to be let alone"). Lange vor dem Computereinsatz, aber auch lange nach den durch französiche Revolution und Aufklärung formulierten Prinzipien, wie Meinungs- und Versammlungsfreiheit, Gerechtigkeit und Solidarität, entstand die Idee einer individuellen Privatsphäre.

Aufgenommen wurde dieser Gedanke auch in der Europäischen Menschenrechtskonvention, 1950 verabschiedet und in Österreich seit 1958 in Kraft. Im Artikel 8[2] wird dieser Anspruch auf Privatsphäre formuliert:

---

[1] Der Autor ist Geschäftsführer der "e-commerce monitoring GmbH", Lektor an der TU-Wien, Mitglied des Datenschutzrates im Bundeskanzleramt und Obmann der "ARGE DATEN - Österreichische Gesellschaft für Datenschutz" (http://www.zeger.at)

[2] Der MRK-Artikel komplett: 'Artikel 8 - Recht auf Achtung des Privat- und Familienlebens
(1) Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs.
(2) Der Eingriff einer öffentlichen Behörde in die Ausübung dieses Rechts ist nur statthaft, insoweit dieser Eingriff gesetzlich vorgesehen ist und eine Maßnahme darstellt, die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung

'Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs.'

Freilich mit einem umfassenden und für die heutige Diskussion entscheidenden Gesetzesvorbehalt. Kurz gesagt, der Staat behält sich das Recht vor, in diese Rechte einzugreifen, wenn der Eingriff gesetzlich vorgesehen und wesentlich ist. Nicht nur autoritäre Staaten interpretieren diesen Gesetzesvorbehalt so, dass jeder gesetzlich vorgesehene Eingriff in die Privatsphäre gerechtfertigt ist, da ja der Gesetzgeber (= Nationalrat) nur wesentliches beschließt.

Diese Konstruktion bereitete bis Anfang der 70er-Jahre kaum Schwierigkeiten. Eingriffe in die Privatsphäre wurden als physische Übergriffe staatlicher Organe, ungerechtfertigte Hausdurchsuchungen, Zensurmaßnahmen und persönliche Überwachung abgehandelt. Die Erhaltung der Privatsphäre war eine mehr oder minder persönliche Auseinandersetzung von Individuen mit greifbaren Staatsorganen.

Erst mit der Ausbreitung der EDV Anfang der 70er-Jahre wurde die Idee der Privatsphäre neu hinterfragt. Die scheinbar grenzenlosen Speichermöglichkeiten der Computer ließen die Idee aufkommen, dass es einmal möglich sein müsste, alles über einen Menschen zu wissen oder - wie es ein deutscher Innenminister Ende der 70er-Jahre formulierte - vor dem Täter am Tatort zu sein.

Ein Erhebung des statistischen Zentralamts brachte 1975 223 personenbezogene Datenverarbeitungen zutage, mit der Prognose, in Zukunft würde die Zahl - auf Grund der massiven Zentralisierungsgewinne - noch weiter absinken.

Wir wissen, dass nicht nur diese Prognose falsch ist. Auch der Versuch vor dem Täter am Tatort zu sein, hat sich als Illusion erwiesen.

Mit der Idee des "Datenschutzes" sollte diesen monströsen Datenverarbeitungen ein Gegengewicht entgegengesetzt werden. Mehrere Länder, voran Deutschland, relativ spät Österreich, hatten bis 1984 Datenschutzgesetze erlassen.

Auch in der OECD und im Europarat war zu Beginn der 80er-Jahre Datenschutz ein Thema und relativ ähnliche Bestimmungen und Empfehlungen wurden von diesen Gremien verabschiedet. Erstaunlich und vermutlich nur Zufall, dass nach 1984 der Elan zur Entwicklung eines Privatsphärekonzepts im Informationszeitalter deutlich nachließ.

Waren die Fundamente des Datenschutzgedankens schon mit falschen Erwartungen und Befürchtungen auf Sand gebaut, so ist das Konzept "Datenschutz" selbst reichlich verunglückt. Statt zu hinterfragen, was Privatsphäre im Informationszeitalter mit tendenziell unbegrenzten Informationsströmen bedeuten kann, wie mit den Freiheiten und Bedrohungen von Anonymität umzugehen ist, wurde eine technokratische Richtung eingeschlagen.

Aus dem "Recht auf Privatsphäre" wurde "Datenschutz", aus "Datenschutz" "Datensicherheit" und "Datensicherheit" wurde zur Angelegenheit der EDV-Techniker.

Österreich legte noch ein unrühmliches Schäuferl nach, indem das Konzept mit bürokratischen Registerbestimmungen, die niemand exekutieren konnte, belastet wurde. Jeder Datenverarbeiter hatte zu melden, was er mit seinen Daten macht. Das funktioniert bei 223 Verarbeitern, nicht jedoch bei 50.000 oder derzeit 300.000 Datenverarbeitern allein in Österreich.

---

der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist.'

Der Hauptverband der Sozialversicherungsträger, das Innenministerium oder ein Krankenhaus wurden denselben bürokratischen Abläufen unterworfen, wie tausende Kegelklubs und Tennisvereine.

Erst 1987 wurde in Deutschland durch das Volkszählungsurteil das bisherige Konzept "Datenschutz" hinterfragt und durch den Begriff der "informationellen Selbstbestimmung" ersetzt. Der Einzelne soll entscheiden dürfen, wer welche Informationen über ihn hat, 87 Jahre nach "The Right of Privacy" wurde das Recht "allein zu sein" für das Informationszeitalter thematisiert. Leider blieb dieser Gedanke isoliert und ohne großen Nachhall.

Erst 1995 erfolgte durch die EU-Richtlinie Datenschutz (95/46/EG[3]) zumindest auf europäischer Ebene ein Innovationsschub, wenn auch aus einem erstaunlichen Beweggrund. Nicht die Sicherung der Einhaltung der Menschenrechte war Triebfeder für die EU-Richtlinie, sondern (privat)wirtschaftliche Überlegungen. Da mittlerweile zu jeder Wirtschaftstransaktion auch enorme Datenmengen verarbeitet wurden, bestand die Gefahr, dass einzelne Länder mit Hilfe des Arguments "Datenschutz der Bürger" Handelshemmnisse errichten. Die Gefährdung der vier Grundfreiheiten ("freier Warenverkehr", "freier Dienstleistungsverkehr", "freier Personenverkehr" und "freier Kapitalverkehr") war Anlaß für diese Richtlinie, die auch im Titel sowohl den Schutz der Bürger als auch den freien Datenverkehr zitiert.

Ein Spagat mit dramatischen Folgen für die Durchsetzung der Persönlichkeitsrechte.

MÜSSEN PERSÖNLICHKEITSRECHTE INDIVIDUELL EINGEKLAGT WERDEN?

Welche enormen Schwierigkeiten im Umgang mit Persönlchkeitsrechten bestehen, zeigte die TV-Diskussion zur letzten Bundespräsidentenwahl. Die Kandidatin stellte im Zuge der Diskussion um das Verhalten einzelner Mandatare in einer parlamentarischen Abstimmung das Recht der geheimen Wahl in Frage und meinte sinngemäß "Ich darf doch wohl jeden sagen, wen ich gewählt habe."

Übersehen wurde, dass das geheime Wahlrecht nichts mit der freien Äußerung der politischen Meinung zu tun hat, sondern mit dem Recht, Entscheidungen zu treffen, ohne sie begründen zu müssen. Es ist eine demokratische Verpflichtung für alle, in der Wahlzelle unbeobachtet zu wählen, um auch allen die Möglichkeit zu geben, abweichend zu wählen und Minderheiten zu bevorzugen. Der Gang in die Wahlzelle erfolgt nicht, weil man etwas zu verbergen hat oder weil man seine politische Meinung nicht deklarieren möchte, sondern zum Schutz jener Menschen, die sich nicht deklarieren wollen.

Ein individell durchzusetzendes Wahlrecht, genauso wie ein Recht auf Meinungsfreiheit oder auf Versammlungsfreiheit, wäre ein Widerspruch in sich. Nicht ohne Grund werden bei jeder Wahl Wahlbeobachter verschiedenster Gruppierungen herangezogen, die einen vom Individuum unabhängigen ordnungsgemäßen Ablauf garantieren.

Nicht so im Datenschutzbereich. Das heutige, durch die EU-Richtlinie verbreitete Konzept des "Datenschutzes" überträgt die gesamte Verantwortung zur Einhaltung des Datenschutzes den Bürgern. Der Bürger muss sich mit Hilfe seiner "subjektiven Rechte" um die Einhaltung in jedem Einzelfall kümmern, eine völlige Überforderung angesichts der Fülle der Datenbestände und der Geschwindigkeit der

[3] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr

Datenverbreitung. Wir schätzen, dass jeder Bürger im Schnitt in 400 Datenbanken gespeichert ist.

Kern des Konzeptes ist, dass Daten aus gesetzlichen Gründen verwendet werden dürfen, aus einer Reihe anderer Gründe, aber auch dann, wenn der Betroffene zugestimmt hat. Diese Zustimmung muss zwar ausdrücklich erfolgen, ist jedoch nicht Form gebunden und kann damit auch konkludent vereinbart werden.

Veröffentlicht etwa ein Veranstalter die Listen der Teilnehmer im Internet, dann ist das zulässig, wenn die Teilnehmer zugestimmt haben. Ist eine Veröffentlichung nicht erwünscht, dann muss jeder einzelne die Veröffentlichung untersagen, es gibt jedoch keine Mechanismen, die es etwa den Benutzer der Webseite ermöglichen würde, herauszufinden, ob tatsächliche Zustimmungen zur Veröffentlichung vorliegen.

Werden die Daten nicht veröffentlicht, sondern es wird "nur" damit gehandelt, wie dies bei Adressverlagen der Fall ist, sind die Chancen des Betroffenen noch weiter reduziert.

Natürlich bestehen theoretische Rechtsschutzinstrumente, die jedoch derartig langsam arbeiten, dass sie de facto nicht mehr wirken. Im Rahmen der Rechtshilfe hat die ARGE DATEN mittlerweile hunderte Fälle betreut und auch zur Datenschutzkommission gebracht. Wenn überhaupt entschieden wurde, dann im Durchschnitt nach einem Jahr, auch bei Bagatellfragen, die entsprechenden Daten waren dann längst schon an einer anderen Stelle oder "nicht mehr verfügbar".

Die grundlegenden subjektiven Rechte sind das Recht auf Auskunft, auf Information des Datenverarbeiters, auf Richtigstellung falscher Daten und Löschung nicht mehr benötigter Daten. Weiters kann der Verwendung bestimmter Daten, etwa in einem Adressbuch, widersprochen werden. Betrachtet man jedoch die Realität, etwa der Informationspflicht, dann wird dieses Recht - sanktionslos - täglich millionenfach gebrochen und ist für den Betroffenen nicht einforderbar.

Das Recht auf Information des Auftraggebers sieht vor, dass jeder Datenverarbeiter Betroffene davon in Kenntnis setzen muss, zu welchen Zweck er Daten verwertet. Informiert er den Betroffenen nicht, dann weiß dieser nichts davon und kann kein Rechtsmittel ergreifen. Weiß er von der Datenverarbeitung, dann ist er ja informiert und "braucht" kein Rechtsmittel zu ergreifen.

Besteht der Verdacht auf Verletzung von Datenschutzbestimmungen abseits der subjektiven Rechte, dann kann zwar Anzeige erstattet werden, es gibt jedoch keine Parteienstellung, selbst wenn das Ergebnis der Anzeige eine Schädigung des Betroffenen aufzeigt.

Stellen Sie sich eine Gesellschaft vor, in der etwa das geheime Wahlrecht ebenfalls individuell im Wahllokal durchgesetzt werden müsste. Ein Jahr später hätte man vielleicht einen Bescheid, der den Bruch des Wahlergebnisses bestätigt.

ÜBERWACHUNG IN IHRER TECHNOKRATISCHEN DIMENSION

Was mit Überwachung im engeren Sinn assoziiert wird, sind eine Reihe technischer Konzepte, auf die kurz einzugehen ist.

Die biometrische Versuchung

Schon der Teufel wusste um die Vorzüge der Biometrie bescheid. Er ließ seine Verträge bevorzugt mit dem Blut der Opfer unterschreiben.

Tatsächlich sind biometrische Merkmale wesensbestimmend für eine Gemeinschaft. Mittels Aussehen und Verhalten, aber auch durch die persönliche Unterschrift können wir Personen identifizieren und miteinander kommunizieren. Auch unsere bisherigern Personaldokumente sind voll mit biometrischen Informationen, wie Augenfarbe, Alter, Größe, Aussehen (Bild) und Unterschrift.

Offensichtlich geht es bei der Biometriedebatte um etwas anderes, als um die jahrtausendelange Tradition der Identifikation von Menschen an Hand ihrer Merkmale. Tatsächlich geht es genau um die Zerstörung dieser Tradition, um die Umformung eines sozialen Prozesses in eine großtechnische Anwendung.

Wenn heute von Biometrie gesprochen wird, dann meint man die Übersetzung natürlicher Merkmale in digitale Zeichenketten und deren Weiterverarbeitung.

Der Prozess der Erfassung benötigt aufwändige Geräte, der Prozess der Übersetzung selbst ist an komplexe, zum Teil geheime und zum Teil patentrechtlich geschützte Verfahren gebunden. Die Verantwortung für die Identifikation von Menschen wird an Maschinen (BlackBoxes) delegiert.

Die Qualität dieser Verfahren ist noch völlig unausgereift und hängt im Wesentlichen vom betriebenen Aufwand ab. Je exakter diese Verfahren arbeiten, desto teurer wird jede Kontrolle, desto länger dauert sie und auch desto störanfälliger ist sie.

Das Problem biometrischer Informationen ist die Übereindeutigkeit. D.h. ein Mensch hat nicht bloß einen eindeutigen rechten Daumenabdruck oder eine eindeutige Unterschrift, sondern beide sind bei jeder Abnahme unterschiedlich. Tatsächlich ist eine völlig idente Unterschrift der exakteste Beweis, dass sie gefälscht wurde.

False Acceptance Rate (FAR) und False Rejection Rate (FRR) sind die technokratischen Zauberwörter die dieses Problem beschreiben. FAR beschreibt die Zahl der akzeptieren Fälle, obwohl tatsächlich keine Übereinstimmung beseht, FRR beschreibt die Zahl der zurückgewiesenen Fälle, obwohl Übereinstimmung besteht.

Das deutsche Bundesamt für Sicherheit in der Informationstechnik hatte 2003 vier renommierte Gesichtserkennungssysteme getestet und kam zu FRR Werten zwischen 65 und 99%, d.h. zwischen 65 und 99 % der präsentierten Gesichter wurden nicht erkannt. Im Bereich der Fingerprints ist die Situation um einen Faktor 100 besser, aber natürlich noch immer meilenweit von sicheren Anwendungen entfernt.

Besonders dunkel ist der Bereich der Iriserkennung, hier ist nicht einmal klar, ob Eindeutigkeit besteht, da die Verfahren patentrechtlich geschützt sind und daher kaum Forschung betrieben wird.

Würde man etwa am Frankfurter Flughafen mit seinen 400.000 Abfertigungen pro Tag ein Verfahren mit 99%iger FRR-Sicherheit anwenden, hätte man 4.000 unberechtigte Anhaltungen und Flugversäumnisse täglich. In Hinblick auf die Dichte der hochgradigen Geschäftskunden wäre wohl zu Mittag des ersten Tages der Versuch gestoppt.

Einhelligkeit besteht selbst bei Biometrie-Vertretern, dass eine zuverlässige Identifikation ohne Mitwirkung des Betroffenen auch in weiterer Zukunft nicht möglich ist.

Trotzdem gibt es zwei Gründe warum der Biometriehype derartig geschürt wird. Erstens ist es blanker Lobbyismus. Die Biometrieindustrie benötigt Absatzmärkte für ihre teuren Investitionen, staatliche Stellen mit ihrem millionenfachen Ausweisbedarf sind dazu geradezu ideal.

Zweitens kommen die Systeme auch den Intentionen der Sicherheitspolitiker entgegen. Ihre Mechanismen sind hochgradig undurchschaubar, sie erzeugen das Gefühl der omnipräsenten Überwachung und wirken damit als Sicherheitsplacebo. Es muss jedoch bezweifelt werden, ob eine demokratsche Gesellschaft auf das Funktionieren patentrechtlich geschützter und in den Händen von Großunternehmen liegender Systeme bauen kann.

Menschen, die sich professionell mit diesen Systemen und deren Umgehung beschäftigen, werden immer geeignete Schwachstellen finden und wir können sicher sein, die organisierte Kriminalität gehört dazu.

Soziale Kontrolle durch Videoüberwachung

Der Einsatz von Videoanlagen ist in Österreich, sieht man vom Arbeitsplatz, der Polizei und dem Veröffentlichen der Bilder ab, nicht geregelt.

Jede Privatperson darf an jedem beliebigen Ort Videoanlagen installieren, selbst Nachbargrundstücke, Wohnungen, Toilettanlagen, Umkleidekabinen oder fremde Lokale sind davon nicht grundsätzlich ausgenommen. Verboten wäre zwar die Verletzung der Privatsphäre, wann diese beginnt oder endet müsste in jedem Einzelfall bei einem Zivilgericht geklärt werden, ein teures, riskantes und zeitaufwändiges Unterfangen. Mit dem Ergebnis, dass es dazu erst 2-3 Verfahren in Österreich gab.

Trotz der enormen Beliebtheit der Videoüberwachung, Österreich hat geschätzte 160.000 Kameras wird damit nur ein winziger Teil des öffentlich zugänglichen Raumes erfasst, vielleicht 1 Promille der urbanen Flächen.

Videoüberwachung ist nach wie vor eine teure und personalaufwendige Angelegenheit. Auch die letzten Vorstöße des Innenministers sollen nicht zu einer flächendeckenden Verbrechensbekämpfung führen, dazu würde das gesamte Bruttoinlandsprodukt nicht ausreichen, sondern sollen punktuell "Kriminalitäts-Hot-Spots" überwachen.

Ein Unterfangen, das schon im Ansatz zum Scheitern verurteilt ist. Mobile Kriminalität, wie Geldtaschendiebstahl oder Drogenhandel, verlegt schlicht ihren Aktionsplatz auf die nicht überwachten Plätze und Seitengassen, objektorientierte Kriminalität, wie Einbrüche, wenden sich den nicht oder weniger geschützten Objekten zu oder professionalisieren den Angriff, sodaß die Überwachung nichts hilft.

Trotzdem gibt es einen wesentlichen Grund zur Videoüberwachung. Durch Videoüberwachung lässt sich sehr leicht sozial unerwünschtes Verhalten erkennen. Lästige Bettler, zerlumpte Sandler, herumlungernde Drogenjunkies, angeheiterte Jugendliche stören das Bild der sauberen Fußgängerzonen und Einkaufsstraßen. Hier ist die Videoüberwachung ein wirksames Mittel diese Personen zu entdecken und wegzuweisen bzw. kommen sie nach einiger Zeit nicht mehr in derartige Straßen. Die Ursachen für diese sozialen Außenseiter werden nicht beseitigt, sie werden aber abgedrängt, in die weniger wichtigen Stadtviertel, in die Seitengassen. Konsequent eingesetzte Videoüberwachung wird die Kriminalität nicht senken, sie wird sie verschieben, es werden aber auch soziale Gegensätze verschiedener Ortsteile verschärft.

Der Lauschangriff

Fast völlig aus der öffentlichen Diskussion verschwunden ist der "große Lauschangriff". Die bisherigen Erfahrungen waren eher ernüchternd, selbst bei der größen Operation, "Operation Spring" sind die Ergebnisse dürftig. Aus

grundrechtlicher Sicht hat der Lauschangriff wenig Bedeutung, zu teuer und personalintensiv ist der Einsatz, zu unwichtig sind die meisten Bürger, als dass es wert wäre, sie persönlich zu belauschen, mittlerweile existieren bessere Mittel der Überwachung.

Der totalitäre Zugriff auf die Kommunikation

"Date Retention" ist nunmehr das neueste Zauberwort aus der Überwachungsküche. Durch die vorbeugende Speicherung aller Kommunikationsbeziehungen, sei es Telefon oder Internet, ist es möglich herauszufinden, wer mit wem in welchem Umfang in Kontakt getreten ist.

Die EU denkt hier an eine zumindest einjährige Speicherung der Verbindungs- und Verkehrsdaten nach.

Im Gegensatz zu den vorherigen Methoden ist dieses System ausgereift, effizient und hochgradig standardisiert. Im ETSI, dem Normungsinstitut der EU arbeiten Telekom-Techniker unter Anleitung von FBI- und Mossard-Spezialisten an jenen Schnittstellen, die eine automatisierte Auswertung der Gesprächsprofile erlauben.

Damit die Telekombetreiber ruhiggestellt wurden, wurde in der neuen Überwachungverordnung eine großzügige Entgeltregelung geschaffen.

Wird dieses Gesetz umgesetzt, dann müssen wir uns von der Idee der Meinungs- und Versammlungsfreiheit endgültig verabschieden. Jede Internetcommunity stünde dann unter Dauerbeobachtung.

DER INVENTARISIERTE MENSCH

Viel bedrohlichere aktuelle Entwicklungen finden derzeit auf Gesetzgebungsebene statt.

Bisher scheiterte staatliche Überwachung an den administrativen Sonderlösungen der verschiedenen Behörden. Die Identifikation der Bürger erfolgte nach unterschiedlichen Verfahren, ausreichend für die jeweilige Behörde, jedoch ungeeignet zur nationalen oder internationalen Datenvernetzung.

Mehrere Gesetzesvorhaben beseitigen diesen "Missstand" und stellen eine reale Gefahr der demokratischen Grundlagen dar.

So wurde vorerst das Melderregister zentralisiert, der Zugang für Privatunternehmen erleichtert und die Sperre der Meldeauskunft erschwert.

Durch die Bildungsevidenz wurde ein EU-weit einmaliger Vorstoß gemacht. Detaillierte Schuldaten sollen bis ans Lebensende, jedenfalls weit über das Pensionsalter hinaus individuell gespeichert werden. Durch Verwendung der Sozialversicherungsnummer als Zugangsschlüssel können diese Daten auf Knopfdruck auch mit beliebigen anderen Beständen, etwa dem Finanzamt oder der Sozialversicherung abgeglichen werden.

Was bisher zu wenig beachtet wurde ist jedoch der direkte EIngriff in die Lebensplanung der heranwachsenden Menschen. Schule ist immer auch ein Ort der ersten Bewährung und der ersten Konflikte. Viele Schüler mit disziplinären Vergehen oder Lernschwächen werden später angesehene Bürger und umgekehrt. Mit dem Wissen, dass viele Schuldetails lebenslang gespeichert werden und niemand heute sagen kann, wer in 20, 40 oder 60 Jahren darauf zugreifen wird, welche Schlüsse gezogen werden, wird angepasstes Verhalten geradezu gefordert.

Damit nicht genug, eine Einkommensevidenz mit den detaillierten Einkommensdaten aller Bürger ist genaus geplant, wie eine zentrale Gesundheitsevidenz, eine Wohnungsevidenz und eine Arbeitsplatzevidenz. Sie alle werden getrennt bestehen, können, alle jedoch mit demselben Schlüssel versehen, bereit auf Knopfdruck jederzeit zusammen geführt zu werden.

Von Adorno stammt der Gedanke, frei zitiert, dass der Bürger, der einmal der Verwaltung aufgefallen ist, um seine Bürgerrechte fürchten muss. Heute wird alles getan, dass nur ja kein Bürger der Aufmerksamkeit der Bürokratie entgeht. Der Grundsatz, unbeobachtet und anonym leben zu können, solange man sich nichts zuschulden kommen läßt, wird aufgehoben.

GLÄSERNE MAUERN

Wenn wir die Entwicklung der Privatsphäre im Informationszeitalter ansehen, dann darf auch der privatwirtschaftliche Aspekt nicht vernachlässigt werden.

Die vollmundigen Ziele der 70er-Jahre, alles über den Bürger zu wissen, wurden trotz einer Vertausendfachung der Speicherkapazität und Rechnerleistung nicht erreicht.

Es ist zwar mittlerweile unglaublich billig geworden dank Internet an personenbezogene Daten heranzukommen, diese aber auch nur halbwegs aktuell Daten zu verwalten, ist heute schwieriger den je. Statt zu versuchen "alles" über die Menschen zu erfahren, werden stattdessen hoch wirksame Kategoriesierungs- und Kanalisationsstrategien entwickelt.

In zwei Branchen bestehen besondere - wenn auch unterschiedliche - Gefährdungspotentiale, im Adresshandel und bei den Wirtschaftsinformationsdiensten.

Im Bereich des Adresshandels erlaubt eine - sicherlich nicht EU-konforme - Ausnahmeregelung einen schwunghaften Datenhandel zwischen Firmen ("Inhaber von Interessenten- und Kundendaten") und Adressverlagen (Besser "Datenhändlern"). Auf Grund dieser Bestimmung können Kundendaten ohne Zustimmung der Betroffenen verkauft werden, die Adresshändler können aus den Abgleich der verschiedensten Listen, den Einkaufsgewohnheiten und dem Wohnort umfangreiche Interessens- und Kaufkraftprofile errechnen. Diese können dann dazu verwendet werden, um bestimmten Personen bestimmte Angebote zu machen oder auch nicht, ihnen bestimmte Lieferkonditionen zu gewähren oder - wie in Großbritannien schon üblich - sie zu bestimmten Supportlevels umzuleiten. Der kaufkräftige, gebildete Kunde erhält sofort Support, der arme und sozial Schwache verkommt in der Endloswarteschleife.

Ob die Kundenprofile stimmen oder nicht ist dabei unerheblich, der Konsument wird im Zugang zu den Angeboten beschränkt und kanalisiert.

Noch direkter wird das Konzept der "gläsernen Mauern" bei den Wirtschaftsauskunftsdiensten sichtbar. Immer mehr Firmen führen "schwarze Listen" bzw. "Warnlisten", in die zahlungsunwillige Kunden gelangen. Banken, Versicherungen, Telekomfirmen, Versandhändler führen derartige Listen. Es ist dabei unerheblich, ob der Kunde vorsätzlich nicht zahlt oder auf Grund einer mangelhaften Leistungserbringung Teilbeträge zurückhält. Einmal in derartige Listen eingetragen wird es schwer gelöscht zu werden, der neue Handyanschluss oder Internetanschluss, ein Bankkredit sind rasch verweigert. In zahllosen Beschwerdeverfahren musste die ARGE DATEN feststellen, dass die Herkunft dieser negativen Bonitätsdaten nicht geklärt werden konnte.

Es kommt mittlerweile schon vor, das Konsumenten entgegen ihrer Überzeugung aus Furcht vor Einträgen in diese Listen, ungenügende Leistungen bezahlen.

Es beruhigt nicht wirklich, wenn man weiß, dass die Konsumentendaten mittlerweile bei nur mehr drei Großdatenhändlern zentralisiert sind und die Wirtschaftsauskunftsdienste ebenfalls auf nur mehr sieben Anbieter konzentriert sind.

In etlichen Fällen werden Inkassodienste-, Adresshandel und Wirtschaftsauskunftsdienste innerhalb desselben Konzerns auf derselben Büroadresse abgewickelt. Da kann es dann schon passieren, dass eine Auskunft zum Monatseinkommen aus einem Lifestyle-Fragebogen zur Bonitätsbeurteilung herangezogen wird.

VIELE KLEINE "GROSSE" BRÜDER

Die Verletzung der Privatsphäre beginnt nicht erst beim spektakulären Datenklau, dem Veröffentlichen intimer Details und Fotos oder der Weitergabe von Gesundheitsakten.

Die Verletzung beginnt im Kopf jedes Einzelnen. Sobald man sich Gedanken machen muss, wer in Zukunft auf bestimmte Daten zugreifen wird, wie mein erwünschtes Verhalten auszusehen hat und welche Querverbindungen hergestellt werden können, wird in meine Privatsphäre eingegriffen.

Die größte Gefahr besteht heute nicht in staatlichen Zwangsmaßnahmen, die auf Grund der enormen Datenbestände gesetzt werden, auch wenn derartige Maßnahmen nicht für alle Zukunft ausgeschlossen werden können, sondern in der Manipulation des Verhaltens der Bürger. Immer mehr verunsicherte Bürger fragen an, ob Daten, die im Zuge einer Wehrdienstbefreiung anfielen zu einem Anstellungsproblem im öffentlichen Dienst werden können. Oder ob der Antrag eines Steuerabsetzbetrags für einen Heilbehelf zum Verlust des Führerscheins führen kann.

Bisher waren wir gewohnt in verschiedenen Umgebungen verschiedene Rollen zu spielen, als Berufsmensch sind wir anders aufgetreten, als zu Hause oder unter Freunden. Der Versuch Daten aus diesen sozialen Kontexten herauszulösen, sie beliebig miteinander zu verknüpfen und zu verwerten, beraubt uns wichtiger Persönlichkeitsrechte.

Privatsphärerechte sind immer auch Minderheitenrechte. Das Konzept "allein zu sein", sich zu verweigern oder anders als die anderen zu sein, ist per definitionem ein Ausschlussverfahren.

DEN "Big Brother" haben wir nicht gefunden, aber viele kleine große Brüder, manche noch in der Krabbelstufe, manche schon spätpubertär. Jeder hat, aus seiner Sicht auch ein "Anrecht" auf Kontrolle und Überwachung. Machen wir uns auf den Weg, dass dieses "Anrecht" nicht ausufert, es ist daher notwendig in jedem Fall schon den Anfängen zu wehren, hinterfragen wir jede gesammelte persönliche Information.

Es ist Aufgabe einer Zivilgesellschaft nicht nur heute für demokratisch legitimierte Ordnung zu sorgen, sondern auch alle Maßnahmen und Lösungen zu vermeiden, die in Zukunft mißbraucht werden können. Es wäre hoch an der Zeit nicht nur die Ermittlung und Verwaltung von Daten zu planen, sondern auch deren fristgerechte Löschung. Nur Daten die nicht existieren sind vor Mißbrauch sicher. Sechzigjährige Datenbanken über das Verhalten von Heranwachsenden haben dabei - beispielsweise - nichts verloren.

Unsere größte Bedrohung sind heute nicht nur die vielen kleinen großen Brüder, sondern die Gefahr der Geschichts- und Alternativelosigkeit, jener Aspekt des

Romans 1984, der meist verdrängt wird. Bestand doch die Haupttätigkeit des Protagonisten im täglichen Neuschreiben der staatlich verbreiteten Geschichte und Bestand nicht das größte Projekt in diesem totalitären Staat in der Schaffung einer neuen, völlig reduzierten Sprache in der "Freiheit" nur mehr in der Bedeutung von "Abwesenheit von Flöhen" oder "Demokratie" als Durchsetzung der Mehrheitsrechte gegen die Minderheiten gedacht werden konnte.

Eine Gesellschaft, die das akzeptiert, ist dann auch "frei" von großen Brüdern.