Kein Entrinnen

Mit allen Mitteln forschen sie unser Privatleben aus: Werbeunternehmen, Auskunfteien und Kreditkartenunternehmen. Jetzt liefern wir ihnen unsere Daten auch noch freiwillig ins Haus – via Internet.

Sie gieren nach Daten, Voyeure auf unserer Cyberfährte. Sie wissen mehr über uns als unser bester Freund. Unsere Schuhgröße, unser Einkommen, unsere Hobbys und unsere Lesegewohnheiten. Wenn sie sich anstrengen, finden sie auch etwas über unsere sexuellen Vorlieben oder Krankheiten heraus. Sie sind ziemlich sicher, daß wir dieses Jahr nach Afrika reisen. Ihre Systeme ermitteln, daß wir bald unsere Bank wechseln werden. Dabei wissen wir das selber noch gar nicht.

Die Wächter über unsere Daten-Schatten sitzen nicht im Geheimdienst, sondern in Banken, Fluggesellschaften, Versicherungen und Versandhäusern, bei American Express oder bei Electronic Data Systems Corporation (EDS) in Texas, der bestinformierten privaten Firma der Welt. Sie erfassen unser Kaufverhalten, speichern unsere Lieblingsfarbe und durchforsten unsere Konsumdaten.

Datenschützern wird es langsam unheimlich: „Die großen Verdatungsrisiken gehen nicht mehr vom Staat aus, sondern vom Zusammenspiel von Kreditschutzorganisationen, Banken, Versicherungen, Adreßhändlern, Warenhäusern und Auskunfteien“, analysiert Thilo Weichert von der Deutschen Vereinigung für Datenschutz.

Persönliche Kundendaten – die Goldader der Zukunft

Noch stehen wir am Anfang: „Database Marketing“, gedacht als strategisches Erfassen des Kundenverhaltens zum Zwecke der Direktwerbung, elektrisiert derzeit die Werbebranche. Die weltweiten Datennetze spielen dabei eine wichtige Rolle. Streuverluste von Mailing-Aktionen zwingen zum Sparen. Durchschnittlich 97 bis 98 Prozent der Briefe landen im Müll. Da übt das Versprechen der Online-Anbieter, mit dem einzelnen Kunden schnell, direkt und unmittelbar zu kommunizieren, eine ungeheure Faszination auf die Branche aus. Es scheint, auf dem Daten-Highway werden die Schürfrechte der Zukunft vergeben: Data Mining an der Goldader Kunde.

Ob Online-Dienst oder Internet-Provider, alle türmen Berge von Kundendaten auf: „In den weltweit entstehenden Netzen können künftig Informationen für persönliche Dossiers und Nutzerprofile in einer Weise zusammengeführt werden, die bisher undenkbar war“, beklagt sich der Berliner Datenschutzbeauftragte Hansjürgen Garstka.

Verbindungsdaten, wie sie Compuserve oder AOL speichern, erregen das Mißtrauen der Datenschützer. „Die Rechner dieser Unternehmen wissen über den Kunden letztlich mehr als seine engsten Freunde, ja, mehr als er selbst“, so Bundesdatenschutzbeauftragter Joachim Jacob (s. Interview): „Das Unternehmen kann von der Nutzungszeit des Systems über die Gewandtheit bei der Suche bis zum Inhalt der abgerufenen Informationen oder sogar dem Inhalt der elektronischen Post das Verhalten des Nutzers sehr genau beobachten und festhalten.“

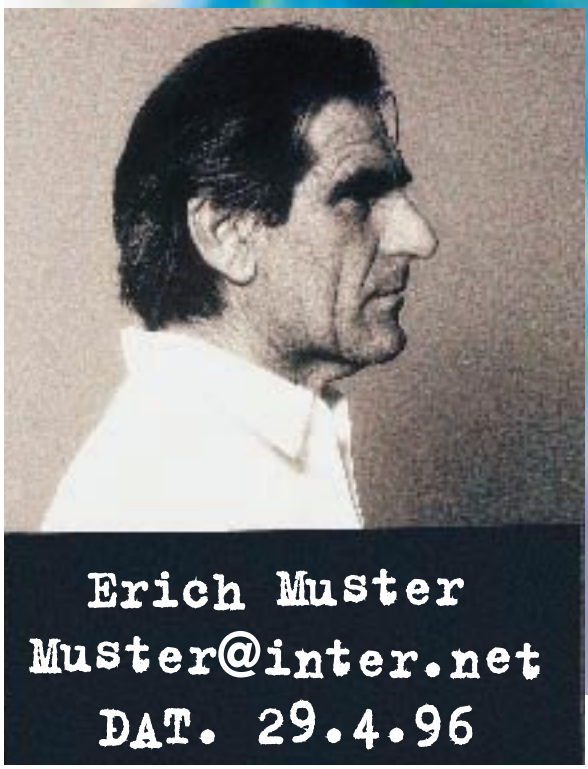
Daraus läßt sich Kapital schlagen: 1994 hatte AOL in den USA detaillierte Kundendaten, mit Angabe über Computer-Ausrüstung, anfallende Benutzungsgebühren und dergleichen öffentlich zur Miete angeboten. Auch die anderen Online-Dienste machten heimlich Geschäfte mit den Adreßdaten ihrer Teilnehmer.

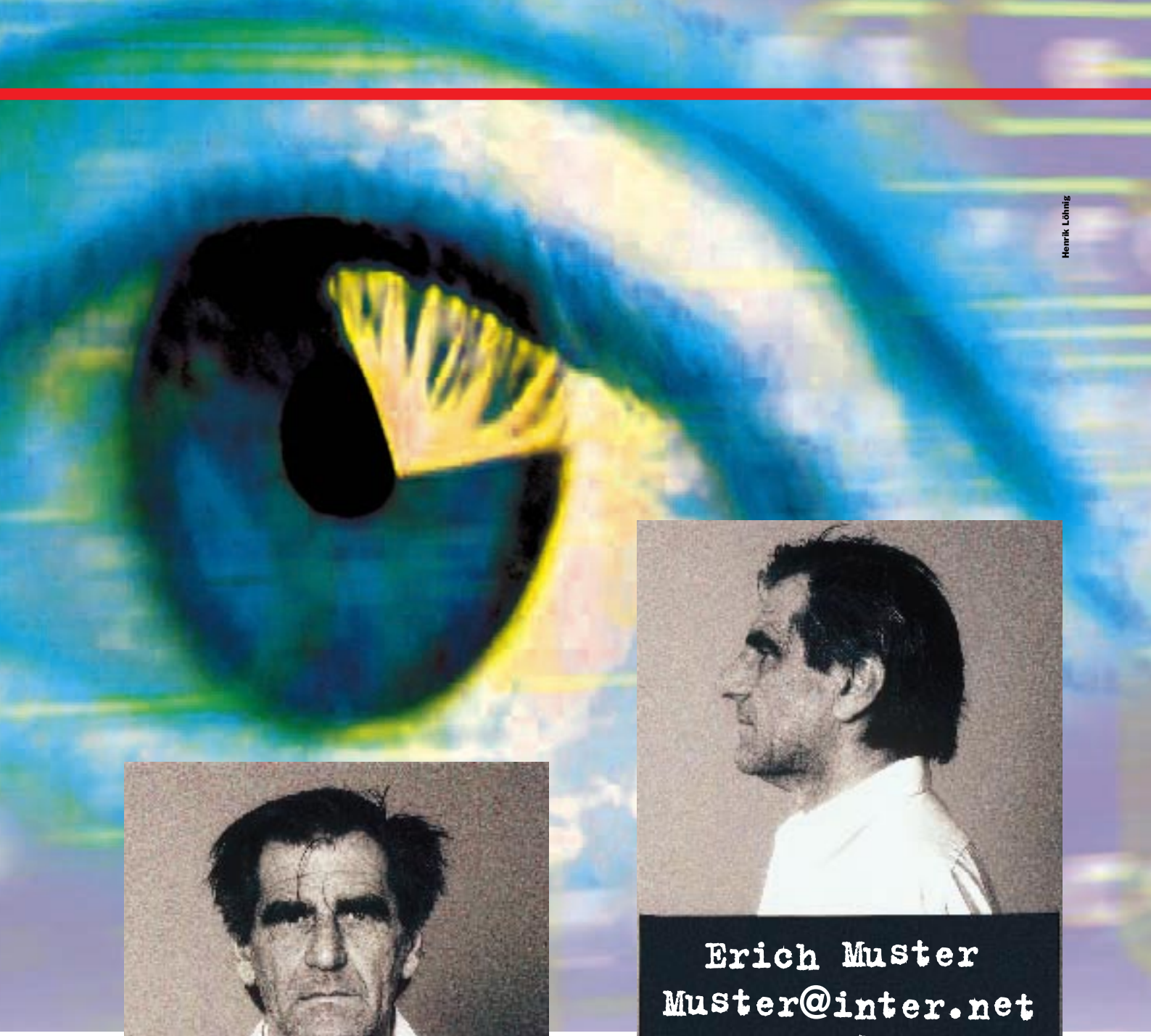
Doch die Aktion ging nach hinten los, empörte die eigene Kundschaft. Der Imageverlust hält an. Die Online-Dienste scheuen sich, solche Datenbestände allzu hemmungslos weiterzuveräußern. Dennoch gilt: Wer will, kann Kundenadressen von Compuserve bei einer deutschen Adreßagentur erhalten.

Hintertürchen hält man sich auch beim deutschen Gratisanbieter Callisto Germany.net GmbH offen. Dieser Internet-Dienst ist ausschließlich auf das Sponsoring seiner Werbekunden angewiesen. Zwar hat Germany.net eine vorbildliche „Ethik-Richtlinie“ an die Mitarbeiter herausgegeben, nach der diese keine personalisierten Verhaltensmuster aus den Kundendaten generieren und weitergeben dürfen. In den rechtsgültigen Geschäftsbedingungen steht allerdings genau das Gegenteil drin. Dies seien Bestimmungen, klärt Geschäftsführerin Michaela Merz auf, die für den „casus belli“ gedacht seien.

Erfrischend offenherzig ist Europe Online: Dort heißt es in der Mitgliedsvereinbarung, daß der Geschäftspartner persönliche Daten für „Werbekampagnen“ von EOL erhält und nutzen darf.

Dabei ist das Datenschürfen auch ohne die Hilfe des Cyberspace schon





Henrik Löhnig

Kai Bornhak

kaum zu kontrollieren. Schlimm treibt es die Versicherungsbranche: Versicherungsvertreter werden von gewieften Immobilienmaklern angebaggert und lassen sich unterm Tisch hochsensible Personendaten abschwatzen. Ein Beispiel: In einem Frankfurter Hotel wurde 1994 etwa 30 Versicherungsvertretern von einem Immobilienvermittler ein „Joint Venture“ angeboten: Man möge doch wohlhabende Privatversicherte aus der Kundendatenbank heraussuchen und diese zu einer Beratung einladen. Die Immobilienmakler würden sogar kostenlos das Anschreiben der Kunden auf dem Briefpapier des Agenten übernehmen.

Die Sache hatte einen Haken: Die Vertreter sollten für das Mailing die Anschriften ihrer Versicherten, mit Angaben zu Familienstand, Einkommen, Lebensversicherung und so weiter an den Immobilienmakler weitergeben. Als Dank wurde den Vertretern vertraglich eine Provision von 4000 Mark pro verkaufte Immobilie angeboten. „Die versuchen über diese Hintertür einen qualifizierten Adressenbestand aufzubauen“, berichtet ein mißtrauisch gewordener Versicherungsfachmann, der an dieser Veranstaltung teilnahm und in der Direktion einer großen Versicherungsgesellschaft als Ausbilder tätig war, gegenüber CHIP. Für ihn ist die Datentrickserei kein Einzelfall: „Das passiert flächendeckend über die ganze Bundesrepublik.“

Leicht könne der Vertreter auch das Einkommen seiner Kunden herausfinden, zumindest bei Selbständigen, die üblicherweise eine Krankentagegeld-Versicherung abgeschlossen haben. Bei einem Vertrag von 150 bis 300 Mark pro Tag „kann ich davon ausgehen, daß die ungefähr ein Nettoeinkommen von 4500

So werden unsere Daten erfaßt:

Access-Provider (etwa Compuserve, AOL, T-Online): Speichern Zugangs- und Verbindungsdaten (Name, Anschrift, E-Mail-Adressen, Systemleistung zu Abrechnungszwecken). Prinzipiell ist eine umfassende nutzerbezogene Überwachung aller Zugriffe möglich. In welchem Ausmaß dies geschieht ist unbekannt. Eine eindeutige Gesetzesregelung, wie solche Daten verwendet werden dürfen, gibt es nicht, vor allem, wenn die Benutzerdaten, wie etwa bei Compuserve, in den USA gespeichert werden.
Logfiles: Registrieren die Zugriffe auf einen WWW-Server. Erfaßt werden hierbei die Rechneradresse (IP-Adresse) des Benutzers sowie alle Aktivitäten auf dem WWW-Server mit exakter Zeitangabe. Laut Datenschutzgesetz im öffentlichen Bereich in Deutschland gar nicht zulässig, trotzdem Alltagspraxis.
Cookies: Daten, die unbemerkt zwischen Browser (etwa Netscape) und WWW-Server ausgetauscht werden. Ermöglichen die Identifizierung eines Users, durch „Wiedererkennen“ des Users beim nächsten Besuch. Gedacht, um mehrfache Paßwortabfragen zu unterbinden. Hilfreich bei Anwendern, die via Online-Dienst ins Internet gehen, da diese über die (mehrfach vergebene) IP-Nummer nicht eindeutig identifiziert werden können.
Wer die Cookie-Überwachung verhindern will, muß bei Netscape die Datei COOKIE.TXT in der Browser-Software nach jeder Internet-Session löschen. Alternative: Nichtkommerzielle Browser wie NCSA Mosaic.
Überwachungsprogramme: Ermitteln das persönliche Benutzerprofil des Anwenders (beispielsweise PWS von W3.Com). Voraussetzung: Eindeutige Identifizierung durch Registrierung des Anwenders in Formblättern (Paßwort, E-Mail-Adresse, Name, Anschrift und dergleichen).
Newsgroups: Millionen öffentlicher Lebensäußerungen in den Internet-Foren (E-Mail-Adresse, Name, Interessengebiete...). Bei entsprechenden Datenkapazitäten fortlaufend archivierbar. Brisantes Datenmaterial für Auskunfteien oder Kreditschutzorganisationen. Die Search-Engine *Altavista* beispielsweise bewältigt die Volltextsuche aktueller News aus 13 000 Newsgroups.

bis 9000 Mark haben“, so der Insider. Von alldem hat der arglose Versicherungskunde natürlich keine Ahnung.

Reichen die Datenschutzgesetze kaum für die „konventionelle“ Praxis aus, versagen sie bei den neuen Informationstechnologien. Denn die Gesetze „sind in einer Zeit entstanden, als die heutigen Möglichkeiten der Informationstechnologie noch nicht abzusehen waren“, so Jacob. Der Bund formuliert deshalb gerade ein neues Multimediagesetz.

Was aber, wenn wie bei Compuserve die deutsche Kundendaten in den USA liegen? Dort gilt nicht deutsches Recht, sondern US-amerikanische Datenwildnis: „Auskunfteien und Direktmarketing-Agenturen verarbeiten selbst sensibelste personenbezogene Daten“, so Peter Schaar, stellvertretender Datenschutzbeauftragter in Hamburg, „zum Beispiel in Datenbanken über Aids-Infizierte, die bestimmte Medikamente nehmen.“

Deutsche Datenschützer verhandeln zur Zeit mit den Online-Betreibern, damit diese die höheren bundesdeutschen Datenschutzstandards anerkennen. Doch dem sekundenschnellen Transfer von Personendaten in entlegene Datenoasen stehen sie meist hilflos gegenüber.

So wurden Personenmerkmale von Millionen Bahncard-Kunden ohne deren Wissen in die USA übermittelt. Immerhin konnten Datenschützer nachträglich sicherstellen, daß die verantwortliche Citibank sich verpflichtete, die Adressen nicht an US-Firmen weiterzuverkaufen.

Brisant wird es, wenn Online-Shops unbemerkt aus dem Kaufverhalten ihrer Kunden Schlüsse ziehen. Wird, wer im Internet-Shop Springerstiefel bestellt, als rechtsradikal eingeordnet? Werden Besteller bestimmter Kleidergrößen wegen Fettleibigkeit zum Risiko erklärt?

Wer sich ins World-Wide Web begibt, muß damit rechnen, auf Schritt und Tritt ausgespäht zu werden. „Vermutlich wissen die wenigsten Nutzer, daß die übliche Server-Software automatisch jeden Zugriff mit Rechneradresse, Datum, Aktion und Zugriffsobjekt protokolliert“, warnt Professor Herbert Kubicek von der Forschungsgruppe Telekommunikation an der Uni Bremen. Wohin der Surfer auch klickt, ob zur *taz* oder zu Coca-Cola – in sogenannten Logdateien wird sein Verhalten exakt gespeichert.

Schlimmer noch: Der eigene Rechner liefert heimlich weitere Daten an den WWW-Server des Anbieters, etwa sogenannte Cookie-Files. Ihr Zweck: Benutzer zu identifizieren, die das Web-Angebot schon einmal besucht haben – nützlich besonders bei Benutzern von Online-Diensten, die wegen mehrfach verwendeter IP-Adressen nicht so leicht von andern Surfern zu unterscheiden sind (siehe Kasten links). Interessanterweise unterstützen fast alle bekannten Web-Browser die Technologie der unheimlichen Spione: Netscape, Microsofts Internet-Explorer, Quaterdecks Mosaic und der Web-Navigator 95.

Das bedeutende Markforschungsunternehmen Nielsen will noch weiter gehen, schreibt das Fachblatt „Werben & Verkaufen“: Netzbetreiber wie Compuserve und AOL sollen ihre Kundendaten über ein „universelles Registrierungssystem“ erfassen. Jeder Kunde, so die Vision, bekäme eine Kennung verpaßt, mit der er jederzeit identifiziert und klassifiziert werden könnte.

Wertvolle Daten fallen erst recht an, wenn der User seine E-Mail-Adresse und seinen Namen auf einer Web-Seite einträgt. Bei „Hotwired“ darf man dann ein erweitertes Angebot nutzen. User Müller muß allerdings damit rechnen, daß sich dann sogenannte Realtime-Monitoring-Überwachungsprogramme an seine Fersen heften. Personal Web Site (PWS) von der Firma W3com spioniert nicht nur exakt sämtliche Aktivitäten und Interessen des Benutzers innerhalb des Informationsangebotes aus, sondern weiß auch, woher der einzelne WWW-Nutzer kommt und wohin er weitersurft.

Am Ende wird für Nutzer Müller genau die Werbung ins WWW-Angebot eingespielt, die seinen Interessen entspricht. Ist Müller also Angler, bewirbt

Der „gläserne User“ am Angelhaken der Werbung

der Anbieter ihn nicht mehr mit Allerweltsprodukten, sondern etwa mit Angelhaken. Am Angelhaken hängt auch Müller: als bis in die ureigensten Bereiche erfaßter Online-User.

Völlig irrwitzig sind die Folgen, wenn Online-Anbieter Adreßdaten auf das Internet bringen. 90 Millionen Anschriften von US-Bürgern samt Telefonnummern hat die Banyan Systems, Inc. in ihrem WWW-Switchboard-Angebot aufs Netz gehievt. Wer will, kann hier seinen persönlichen Eintrag um Hobbys und Beruf ergänzen. Die Sache hat aber einen Haken: Nur derjenige, der sich bei Switchboard mit der eigenen E-Mail-Adresse registriert, kann seinen persönlichen Ein-

trag vor unberechtigtem Zugriff schützen. Prompt kamen einige Bösewichte auf die Idee, fremde Anschriften mit diffamierenden Bemerkungen zu versehen.

Daraufhin erlebte Banyan einen wahren Ansturm. Verängstigte User gaben aus Furcht vor Diffamierungen eiligst ihre E-Mail-Adresse ab, um so den eigenen Adreßbereich vor dem Schabernack der Spitzbuben zu sperren. Fazit: Ein unsicherer Zugangsmechanismus reicht aus, um die Bürger zum Offenbarungseid zu zwingen, das „informationelle Selbstbestimmungsrecht“ auszuhebeln.

Auch Kinder geraten in die Datenfalle der Werbung

Die Experten für Database Marketing machen selbst vor Kindern nicht halt. So etwa Heinz Dallmer, Chef der Unternehmensgruppe Bertelsmann Direkt, dem es darum geht, „die Kinder, die den Elternhaushalt verlassen und einen eigenen Haushalt gründen, als Kunden zu rekrutieren“. Mit raffiniertesten Tricks werden deshalb schon jetzt Informationen über die Kleinsten ausspioniert. Als Datenfalle dienen individualisierte „Print-on-Demand-Kinderbücher“.

Das geht so: Die Eltern haben einen Fragebogen ausgefüllt. Mit Alter des Kindes, Lieblingsessen, liebster Automarke, Telefonnummer, Namen von Onkeln und Tanten und dergleichen mehr. Und alle diese Daten werden in die Geschichte eingebaut. Die Kinder, die ein solches Buch geschenkt bekommen, lesen es – so zeigen Umfragen – im Durchschnitt zwölfmal.

Inzwischen sind 14 Titel solcher Identity-Produkte im Umlauf. „Daß die hier abgefragten Daten, versehen mit dem Einverständnis der Kunden für die weitere Nutzung, schon aufgrund ihres Detaillierungsgrades von großem Wert sind, versteht sich von selbst“, so Dallmer.

Fragt sich, wie lange es noch dauert, bis solche Fragebogen auch durch das Internet geistern. Die Schreckensvision der 70er Jahre, der „gläserne Bürger“, entsteigt still und leise den Datengrüften der Privatwirtschaft.

Und das Data Mining wird durch die Netzkommunikation immer einfacher: Schon das simple Verknüpfen öffentlich zugänglicher Internet-Informationen offenbart brisantes Datenmaterial:

Computerjournalisten machen sich zur Zeit einen Spaß daraus, mit Hilfe der Search-Engine *Altavista* herauszufinden, was denn der Kollege von der Konkurrenz im Internet so alles recher-

INTERVIEW

„Die informationelle Selbstbestimmung wird abgeschafft“

Bundesdatenschutzbeauftragter Joachim Jacob über Datenspuren, Datenoasen und Stoppschilder gegen die Datenwilderei.

CHIP: Was stört Sie, wenn Menschen in Online-Bibliotheken stöbern oder Flugreisen via Internet buchen?

Jacob: Prinzipiell begrüße ich die Möglichkeiten, die die neuen Informationsstechnologien bieten. Doch sollte man auch die Risiken sehen. Jeder Nutzer hinterläßt im Netz Datenspuren. Dabei entstehen detaillierte Erkenntnisse über die Interessen des Betroffenen. Wenn ich in eine virtuelle Bibliothek gehe, ist es möglich festzuhalten, wie lange ich eine Seite lese. Daraus lassen sich unter Umständen Schlüsse über die Fähigkeiten des Nutzers ziehen. Das intensive Untersuchen einer Preistabelle im Internet enthüllt, wie sehr ich auf mein Geld achte, bevor ich eine Kaufentscheidung treffe. Aus solchen Daten lassen sich ziemlich genaue Kundenprofile zeichnen. Online-Dienste können solche Daten für sich selbst nutzen oder an dritte Stellen verkaufen.

Frank Darchinger (2)

„Wirtschaftsinteressen, die den Kunden bis in die kleinsten Verästelungen ausspähen, sind kurzsichtig“

CHIP: Warum sollen solche Kundenprofile gefährlich sein?

Jacob: Die Dinge lassen sich ja noch viel weiter führen: Sie interessieren sich im virtuellen Kaufhaus für irgendwelche Fallschirmspringerstiefel. Daraus wird vielleicht der Schluß gezogen, daß Sie für rechtsradikales Gedankengut aufgeschlossen sind. Oder Ihre Frau bestellt auf Ihren Namen Damenunterwäsche. Möglicherweise schließt das Versandhaus daraus, daß Sie „spezifischen Neigungen“ nachgehen. Ich bin überhaupt kein Feind der Technik, aber ich sehe die Gefahr, daß das Recht auf informationelle Selbstbestimmung, das das Bundesverfassungsgericht 1983 im Volkszählungsurteil festgeschrieben hat, faktisch abgeschafft wird.

CHIP: Solche Daten sollen also gar nicht zustande kommen?

Jacob: Das sollte der Grundsatz sein. Der beste Datenschutz ist gegeben, wenn Daten erst gar nicht entstehen. Solange ich zum Beispiel keine konkrete Kaufabsicht äußere, muß das virtuelle Shopping wie in der Wirklichkeit ablaufen: Niemand überwacht in einem Kaufhaus, an welchen Regalen ich wohl entlangschlendere. Ist allerdings eine Erhebung von Daten zur Vertragsabwicklung erforderlich, dann ist sicherzustellen, daß die Daten nur zu diesem Zweck verwendet werden. Möchte darüber hinaus ein Unternehmen diese Daten zu anderen Zwecken, beispielsweise für Werbung oder Marketing, nutzen, dann ist es doch wohl richtig, wenn der Betroffene um sein Einverständnis gebeten wird.

CHIP: Wissen Sie, welche Daten bei Online-Diensten gesammelt werden?

Jacob: Bei den Datenschützern besteht hier leider eine gewisse Unsicherheit, insbesondere wenn es um multinationale Konzerne geht, die im Zeitalter globaler Netze ihre Nutzerdaten ja oft auch im Ausland verarbeiten.

„Die einflußreichen Staaten müssen sich weltweit auf Mindeststandards einigen“

CHIP: Reichen die Datenschutzgesetze noch aus?

Jacob: Nein, nicht mehr. Sie sind in einer Zeit entstanden, als die heutigen Möglichkeiten der Informationstechnologie noch nicht abzusehen waren.

CHIP: Offensichtlich sind für Sie jetzt nicht mehr Geheimdienste und der Staat, sondern Versandhäuser und Online-Dienste das Böse?

Jacob: Die Informationstechnologie hat tatsächlich eine Akzentverschiebung bewirkt. Fortgeschrittenes Database Marketing ermöglicht es, jedes Mitglied der Gesellschaft hüllen- und grenzenlos digital zu erfassen. Der nichtstaatliche Bereich hat dadurch eine ganz andere Qualität für den Datenschutz des einzelnen bekommen. Darüber hinaus darf man nicht vergessen, daß solche Daten auch beschlagnahmt und für staatliche Zwecke genutzt werden können.

CHIP: Stehen Sie mit Ihren Vorstellungen nicht allein auf weiter Flur?

Jacob: Bei vielen Unternehmen reift die Erkenntnis, daß der Schutz von Privatheit ein entscheidendes Argument dafür ist, daß sich der Bürger überhaupt auf die Datenautobahn wagt. Wirtschaftsinteressen, die den Kunden bis in kleinste Verästelungen ausspähen, sind kurzsichtig. Niemand wird die Datennetze wirtschaftlich nutzen, wenn er ständig einen Kloß im Bauch hat, weil er nicht weiß, was hinter seinem Rücken mit seinen Daten gemacht wird. Die Informationstechnologien werden nur dann ein wirtschaftlicher Erfolg sein, wenn sie von einer großen Bevölkerungszahl für viele Dienste, etwa Teleshopping, Telebanking oder Teleworking, in Anspruch genommen werden.

CHIP: Sie meinen also, der Datenschutz ist ein zusätzliches Verkaufsargument für die Informationsindustrie?

Jacob: Richtig. Datenschutz schafft Akzeptanz. Übrigens hat das auch die Industrie verstanden: Auf dem Treffen der G7-Staaten 1995 drängten nicht nur die Regierungssprecher, sondern auch Wirtschaftskreise auf einen Schutz der Privatsphäre des einzelnen. Die haben erkannt, daß die Akzeptanz der neuen Technologien einen Schutz der Privatheit erfordert. Ich bin ganz optimistisch, die Wirtschaft als Bündnispartner zu gewinnen.

CHIP: Unternehmen können in Sekundenschnelle ihre Daten um den Globus transferieren. Die besten Datenschutzgesetze enden aber an den Grenzen Deutschlands. Wie wollen Sie denn gegen Datenmißbrauch im Ausland vorgehen?

Jacob: Hier türmen sich riesengroße Probleme auf. Es nützt tatsächlich nichts, wenn wir strenge nationale Regelungen haben und diese an den Grenzen Deutschlands haltmachen. Aber darf man resignieren, weil man vermutet, die Probleme seien riesig? Nein! Wenn weltweit die einflußreichen, großen Staaten sich auf bestimmte Mindeststandards einigen, dann wird es einfacher sein, Druck auf Drittstaaten auszuüben, die diese Regeln nicht anerkennen. Ob man sich dabei auf das deutsche Datenschutzniveau einigen kann, bezweifle ich allerdings.

CHIP: Sie werden wohl kaum alle Staaten mit einer internationalen Datenverkehrsordnung beeindrucken...

Jacob: Einverstanden, doch wenn wir eine weltweite Absprache hinkriegen, könnte man auf der Datenautobahn Stoppschilder aufbauen. Die signalisieren dem Nutzer dann: Achtung, hier beginnt die Datenwildnis. Wenn du diese Grenze überschreitest, verläßt du den rechtsstaatlichen Sektor.

Das Interview führte CHIP-Redakteur Peter Diesler

chiert. Altavista bietet sämtliche aktuellen Nachrichten von über 13 000 Newsgroups im Internet zur Volltextsuche an.

An sich wäre dies unbedenklich, denn Diskussionsforen sind ja öffentlich. Doch wenn eine ehemals aufwendige Suche sich in Sekundenschnelle durchführen läßt, entsteht eine andere Qualität: Nur durch Zufall hätte man Herrn Müller in einem weit abgelegen alt.sex-Forum dabei ertappen können, wie er sich nach Pornobildern erkundigt. Nun reicht es, seinen Namen und gegebenenfalls die E-Mail-Adresse einzugeben. Schon listet Altavista säuberlich die gesamte News-Korrespondenz von Herrn Müller auf.

Fachleute wie der Internet-Spezialist Kurt Jaeger vom Forum Informatiker für Frieden und Gesellschaftliche Verantwortung (FIfF) verweisen noch auf ein ganz anderes Datenschutzproblem: „Stellen Sie sich vor, Sie besitzen die Lebensäußerungen von Millionen Internet-Usern und korrelieren diese Daten beispielsweise mit dem Datenbestand eines Kreditkartenunternehmens.“

Tatsächlich ist es technisch kein Problem, über Jahre sämtliche Nachrichten aus den Newsgroup-Foren in einer Datenbank zu speichern. Einen Test haben 1994 die Journalisten Sabine Woln und Reiner May vorgenommen. Probeweise sammelten sie zwei Monate lang in 53 Newsgroups 30 000 Adressen, aufgeschlüsselt nach Interessengebieten. Im freien Verkauf hätten sie seinerzeit 50 000 Mark für die Liste bekommen können.

Brisantes Rohmaterial ergäben solcherart archivierte Newsgroup-Nachrichten auch für Auskunfteien. Vielleicht nur eine Zukunftsvision, aber: Arbeitgeber könnten sich erkundigen, ob Mitarbeiter des öfteren in Newsgruppen für Drogensüchtige Rat gesucht haben. Vermieter könnten so die Lebensgewohnheiten (Hundebesitzer?) ihrer zukünftigen Mieter erkunden.

Fazit von Kurt Jaeger: „Auch öffentliche Äußerungen sind, wenn sie durch elektronische Mechanismen korreliert werden, eine Gefahr.“ *Peter Diesler*

Internet-Adressen:

Datenschutzinformationen: *http://www.rewi.hu-berlin.de/Datenschutz/* oder *http://www.uni.paderborn.de/arbeitsgruppen/fiff/*

Infos zum Thema Cookies *http://home.netscape.com/newsref/std/cookie_spec.html*

Search-Engine Altavista: *http:// www.altavista.digital.com/*