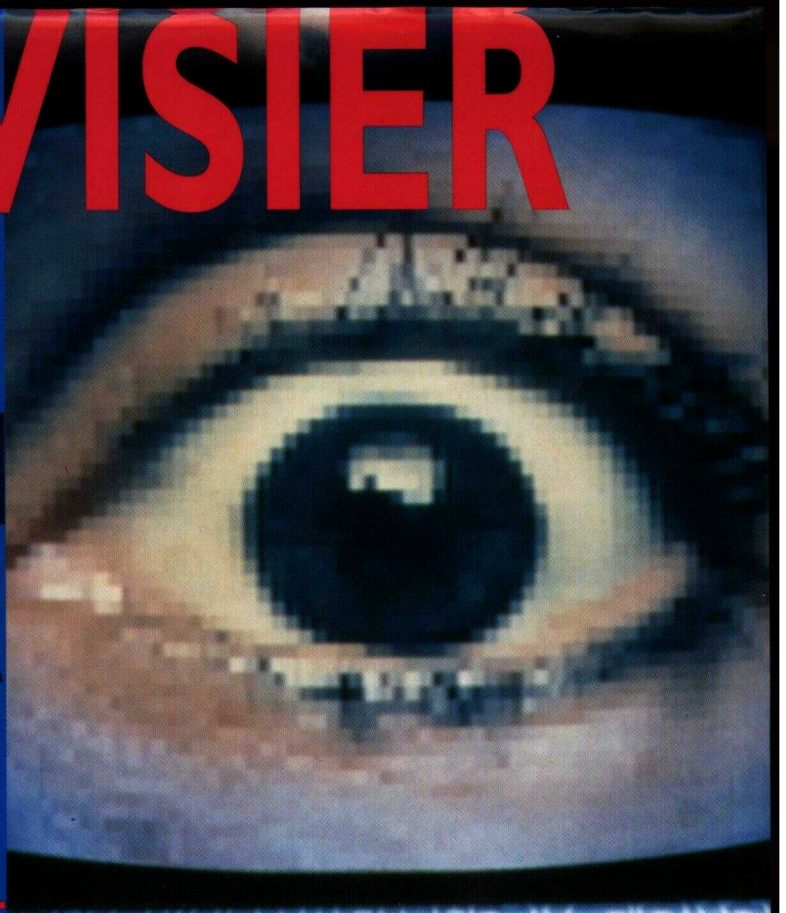
# IM VISIER DER DATEN JÄGER



GERALD REISCHL

- WIE SIE IHR HANDY VERRÄT
- WER IHRE KRANKHEITS-DATEN SAMMELT
- WIE DIE BANKEN SIE IM GRIFF HABEN

Ueberreuter

*Gerald Reischl*

# IM VISIER

## DER DATENJÄGER

*Ueberreuter*

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

**Reisch], Gerald:**
Im Visier der Datenjäger / Gerald Reisch]. - Wien : Ueberreuter, 1990
ISBN 3-8000-3695-9

AU 0462/1

Umschlagfoto: Fix - Stockmarket

Printeri in Austria
7 6 5 4 3

# *Inhalt*

Vorwort

***Total überwacht am Telefon*** ***11***

Das Handy als Peilsender - Großer Bruder hört mit - Das GSM-Abhörgerät - Von kleinen und großen Lauschangriffen - Auf Reizworte programmiert - Unschuldig abgehört - Auch Faxe sind nicht sicher - Gefährliche Anrufbeantworter - Der Lügendetektor für den Hausgebrauch - Pager-Botschaften für jedermann - Die Jagd nach Telefon-Betrügern - Schau mal, wer da spricht - Vorsicht bei Babyphones - Das manipulierbare Netz

*Voll erfaßt im Straßenverkehr* *34*

Autofahrer unter ständiger Beobachtung - Die GPS-GSM-Kombination - Tempokontrolle via Road-Pricing-Satellit - Verbrecher werden überführt - Lkw-Road-Pricing ist erst der Anfang - Flotte unter Kontrolle - Autodieben auf der Spur - Die Zentrale weiß, wo Sie sind - Verkehrs-TV

***Kartenmacher sammeln gern*** ***49***

Die Kontrollore der Plastikkarten - Karten-Fährte - Die Kundenkarte - Unknackbarer Code? - Entweder Sie klauen eine oder Sie bauen sich eine - Intelligenz auf 20 $mm^2$ - Die Gefahr der Multifunktionskarten - Lesegeräte für die Polizei - Krankheiten abrufbereit - Die Mega-Karte

**»Lauschangriffe« im Datenreich** 69

Der abhörbare Home-PC - Auf Schritt und Tritt registriert - Von Keksen, die nicht schmecken - Die Computer-Hacker sind unter uns - Firewalls, die Burgmauern eines Rechnersystems - Der Kummer mit der Kreditkartennummer - Das Problem mit dem Klammeraffen - »Wir verlieren unsere Privatsphäre« - Das Krypto-Schloß

**Banken mit Verbindungen** 85

Auf der Jagd nach Versicherungsbetrügern - Das Loch im Teppich - 10 Punkte für Beamte - Die geheimen Datenbanken der Banken - Rotes Auto: höhere Prämie -»Schwarze Listen« - Die legale Kartei der Schuldner - Kooperationen mit und ohne Grenzen - Wenn die Bank das Telefon ist - Auf Captain Kirks Spuren - Wie uns die Finanz unter Kontrolle hat

**Die Daten der Exekutive** 104

Die DNA-Datenbank - Die Gefahr liegt im Code - Deutsche DNA-Datenbank vor dem Start - Vorn Blutstropfen zum Phantombild - Menschenauslese via Genanalyse - Die Mörderseele im Computer - Ein Druck für den Fingerabdruck - Ein Computer, der Stimmen speichert - Die Handschrift als Karriere-Hemmschuh - Die Datenbank der Fahnder - Nase Nr. 7 und Augenbrauen Nr. 11 - Das größte Überwachungssystem Europas - Der »Schengener Datenklau« - Das europäische FBI

**Im Visier der Hasterfahnder** 136

Kommissar Zufall und die Rasterfahndung - Rasterfahndung »made in Germany« - Positive und negative Rasterfahndung - Kleine und große Rasterfahndung - »Völlig veraltet und inkompatibel« - Die tägliche Rasterfahndung in der Privatwirtschaft - Wie Kunden gescannt werden - Die Methoden des Data-Mining - Wenn der Computer selbständig denkt - Im Visier der Marketing-Strategen - Mit Geo-Marketing Verbrechern auf der Spur - Vom Handy-Kunden bis zum Weinliebhaber



**Kranksein ist gefährlich** 145

Die HIV-Tests des österreichischen Außenministeriums - Das fast anonyme Aids-Register - Das Register der Organspender - Digitales Krankenhaus -Chirurg in Amerika, Patient in Europa - Wie krank ist der Präsident?

**Stadt und Staat schauen genau** 159

Die Mega-Datenbank und die »schwarze Kugel« - Medikamentenstatistik - Die Gefahr der Güteklassen-Medizin - Die »Strom-Forscher« - 3000 Lücken im Münchner Magistrat - Alles unter Kontrolle - Auf Knopfdruck zum Bürger - Von Schwarzfahrern und Schwarzarbeitern - »Einberufungsbefehl« für einen Mercedes

**Gute Adressen sind teuer** 172

Die Methoden der Beschaffer - Wie unsere Kaufkraft berechnet wird - Die »schlechte Adresse« - Bausparvertrag für Neugeborene - Die Adressenverfeinerer - Wie der Vorname Ihr Alter verrät - So viel kostet Ihr Name - Robinsons Liste - Adreßhändler im Internet- Heiße Adressen auf Telefon-CDs

**Die Spione der Lüfte** 190

EU is watching you - Schmugglerjagd vom All aus - Heiße Bilder aus dem All - Geheime Luftbilder auf dem freien Markt

- Schwarzarbeiter aufgepaßt! - Deponiekontrolle mit Zeitreisen - Wenn Seen immer kleiner werden - Satellitenbilder gegen den Briefbombentäter - Satelliten über den Supermärkten

***Datenschützer contra Datenjäger*** ***206***

Wenn Geheimes öffentlich wird - Bundesbeauftragter und Datenschutzrat - Der Zugang zur Intimsphäre - Was die EU-Richtlinie bringt

*Der Autor* ***215***

Datenbank-Register Gerald Reischl

Quellen und Literatur 219

# *Vorwort*

Man weiß mehr über uns, als wir alle vermuten würden. Mit jedem Tag werden die Informationen bei Staat und Wirtschaft umfangreicher, detaillierter und intimer - »Big brother is watching us«. Doch gegen die neuen Technologien wirkt selbst George Orwells »Big Brother« wie ein winziger Zwerg.

Jeder Bürger ist in beinahe hundert Datenbanken gespeichert, vom Schulregister über die Führerscheindatei bis hin zu Krankenkasse, Autofahrerclub und diversen Versicherungen. Polizei, Ämter und Privatorganisationen sammeln akribisch alle möglichen Informationen über jeden Bürger. Staat und Wirtschaft kennen keinen Datenschutz.

Wir verwenden Mobiltelefone und sind durch diese Technologie jederzeit lokalisierbar. Unsere Telefone und Pager werden abgehört, pro Jahr lauscht bei Tausenden von Telefonaten ein Polizist mit.

Kredit- und Bankomatkarten verraten unseren Lebensstil und ermöglichen, daß über uns praktisch auf Knopfdruck ein Benutzer- bzw. Kundenprofil erstellt wird.

Kommt es tatsächlich zum Road-Pricing, dann ist der Bürger auch auf der Straße nicht mehr sicher. Allein die Kombination der Bereiche Mobilkommunikation, Plastikkarten und Verkehrsüberwachung macht aus ihm einen »gläsernen Menschen«.

Mit unbewußter Selbstverständlichkeit geben wir unsere persönlichen Daten weiter. Wir nehmen an Preisausschreiben teil, ordern Kundenkarten, und verschicken mit unseren Home-PCs via Internet Daten - und mit ihnen gleich Informationen über uns - in die ganze Welt.

Mit offenen Armen nimmt man uns in die Kundenkartei des Supermarkts, des Spotgeschäfts, des Airline-Vielfliegerprogramms auf- und lockt mit Spezialangeboten. Für 3 Prozent Rabatt geben wir unsere persönlichen Daten, Charaktereigenschaften, Gewohnheiten und Vorlieben preis.

Sogar die Satellitentechnologie wird eingesetzt, um uns zu kontrollieren: Die Felder von Bauern aus Bayern oder dem Burgenland werden überwacht, Seegrundstück-Besitzer werden aus 800 Kilometern Höhe observiert, und sogar auf Supermarkt-Parkplätze werfen die Spione aus dem All ein Auge.

Banken und Versicherungen haben uns voll im Griff. Kunden werden auf zum Teil bekannten, aber auch geheimen Listen geführt, um sie besser berechnen zu können. Kreditwerber werden nach Punkten beurteilt: Beamte sind weniger wert als Angestellte, Verheiratete mehr als Geschiedene.

Unsere Gesundheitsdaten werden praktisch ewig gespeichert, in den Spitälern haben aber nicht nur Berechtigte Zugriff auf heikle Informationen. Immer wieder versuchen Computer-Hacker, die Krankenhaussysteme zu knacken, um an die heiklen Daten zu gelangen.

Bei der Bekämpfung von Straftätern steht der österreichischen Polizei seit Ende 1997 eine DNA-Datenbank zur Verfügung. Auch in Deutschland wird eine solche demnächst eingeführt. Aber mit Hilfe der DNA-Datenbank lassen sich nicht nur Verbrecher überführen, sondern auch Krankheiten vorhersagen. Noch haben Arbeitgeber und Versicherungen keinen Zugriff auf diese Informationen ...

Es sind also nicht nur Ämter und Behörden, die gierig unsere Daten aufsaugen, auch private Organisationen und Wirtschaftskonzerne. Gegner der polizeilichen Rasterfahndung sollten sich bewußt sein, daß in der Privatwirtschaft täglich gerastert wird. Mit derselben Technologie, mit der auf Verbrecher Jagd gemacht wird, werden die Kunden durchschaut, ihre Einkaufszettel analysiert, um voraussagen zu können, was sie am kommenden Wochenende kaufen werden.

George Orwell hat sich mit seinem «1984« um fast 15 Jahre verschätzt. Erst jetzt ist das eingetreten, wovor er uns gewarnt hat: Am Ende des 2. Jahrtausends kennt man uns besser, als wir uns selbst kennen, weiß man mehr über uns, als uns lieb ist. Die Jahrtausendwende hat das Blatt für den Bürger gewendet - wir sind im Visier der Datenjäger.

# Total überwacht am Telefon

**> Warum Sie als Handy-Besitzer überall geortet werden können.**

**> Wie man heute feststellen kann, wo Sie sich vor 14 Tagen aufgehalten haben.**

**> Wieso in Zukunft jedes Ihrer Telefonate belauscht werden kann.**

**> Wieso Sie künftig vermeiden sollten, am Telefon über »Kokainaffäre« oder über eine »Mafia-Serie« zu plaudern,**

**> Warum Ihre Pager-Nachricht für jedermann lesbar ist.**

**> Warum auch Sie unter den Hunderten Staatsbürgern sein können, die jährlich unschuldig abgehört werden.**

**V Wie Sie als »Dauertelefonierer« plötzlich zu einem verdächtigen Betrüger werden.**

**> Warum Ihr Babyphone gefährlich ist.**

## Das Handy als Peilsender

Der Techniker der deutschen DeTeMobil D1 tippt die Telefonnummer des gesuchten Handykunden in den Computer und drückt die »Enter«-Taste. Nach wenigen Sekunden erscheint die gewünschte Information am Display: »local area, Wien« -der deutsche Handy-Besitzer befindet sich also in Österreich. So wie D1 feststellen kann, wo sich DI -Kunden aufhalten, ist das auch D2, E-Plus sowie den österreichischen Netzbetreibern Mobilkom, max.mobil und

künftig Connect-Austria möglich. Auf Knopfdruck können Techniker und Kriminalisten Verdächtige orten. Überall auf der Welt.

Diese technische Möglichkeit macht Schule. Mehrmals pro Monat sind die Kriminalisten in den Netzwerk-Management-Center der Mobilfunkbetreiber zu Gast und winken mit einem vom U-Richter oder Dreier-Richtersenat unterzeichneten Schreiben, wenn sie deren Büro betreten. Oft wollen sie nur Gesprächsdaten, Ausdrucke mit Telefonnummern und Uhrzeit, um festzustellen, mit wem -der Mordverdächtige X oder die Drogendealerin Y wann telefoniert hat. Immer öfter aber wollen die Kriminalisten Tatverdächtige lokalisieren und diese von der Zentrale aus verfolgen. Wenn im Abstand von wenigen Minuten immer wieder die Nummer eingetippl wird, läßt sich klar erkennen, wohin sich eine Person bewegt. Ein Weg-Zeit-Diagramm wie aus dem Bilderbuch entsteht.

Denn wer ein Mobiltelefon besitzt, hat mit dem Handy zugleich auch einen Peilsender in der Tasche. So praktisch ein Mobiltelefon ist, es macht uns leichter kontrollierbar und verfolgbar. Man kann heute feststellen, wo wir gestern oder vor 14 Tagen waren.

Das Mobiltelefon steht in ständigem Kontakt mit der nächsten Funkstation. Auch wenn nicht telefoniert wird, meldet sich das Handy im Abstand von wenigen Minuten bei der Station. Diese leitet die Daten an ein sogenanntes Mobile Switching Center (MSC) weiter, das wiederum informiert die Zentrale, das Home Location Register (HLR). Wenn sich ein deutscher oder österreichischer Handy-Besitzer im Ausland, beispielsweise in Australien, aufhält, funktioniert das ähnlich. Sobald man in Sydney aus dem Flugzeug steigt und das Handy einschaltet, tritt das Mobiltelefon mit der nächsten Funkstation in Kontakt, diese mit dem Besucher-Register und dieses informiert schließlich die Zentrale in Deutschland oder Osterreich.

Zwar funktioniert die Ortung nicht auf Meter genau, aber in den städtischen Bereichen kann die Position eines Menschen manchmal bis auf 20, 30 Meter bestimmt werden. Denn in Ballungszentren kommen sogenannte Mikrozellen zum Einsatz, Mini-Funkstationen, die in geringem Abstand hintereinander an den Hausfassaden angebracht sind.

Schwieriger ist das Lokalisieren auf dem Land, denn dort stehen die Funkstationen einige Kilometer voneinander entfernt. Offiziell läßt



sich dort der Standort eines Kunden nur auf einen Radius von wenigen Kilometern bestimmen, denn eine große Basisstation wird in drei Sektoren unterteilt, und in einem dieser Sektoren ist das Mobiltelefon angemeldet. Inoffiziell ist der Standort aber punktgenau errechenbar. Die Techniker greifen dabei auf ein System zurück, das sich Timing-Advance (TA) nennt. Bei TA wird die Distanz errechnet, die ein Funksignal von einer Funkstation zum Handy zurücklegt. Will man den genauen Standort wissen, errechnet man zuerst den TA-Wert des Handys von jener Station, bei der es angemeldet ist. Danach wird dem Handy von der Zentrale aus befohlen, auf die nächstgelegene Funkstation auszuweichen. Dort wird der Vorgang wiederholt. Dort, wo sich die beiden TA-Linien kreuzen, befindet sich der Handy-Benützer.

Nur wenn das Mobiltelefon ausgeschaltet ist, läßt es sich nicht lokalisieren. Im Zentralcornputer scheint dann die jeweils letzte Station auf, bei der sich das Handy angemeldet hatte. Aber auch diese Daten können höchst aufschlußreich sein. Wenn sich ein Mobiltelefon nämlich täglich am Abend bei einer bestimmten Basisstation zuletzt meldet, kann angenommen werden, daß der Teilnehmer in der Nähe übernachtet.

Zwar darf ein Handy-Besitzer nur über richterlichen Befehl geortet werden, Mobilfunkbetreiber machen hin und wieder aber auch Ausnahmen. Heftig dementiert wird der Fall eines Unternehmers, der seine Außendienstmitarbeiter mit Handys ausgestattet hat. Einen von ihnen versuchte er einen ganzen Tag lang zu erreichen, erhielt aber immer dieselbe Antwort: »Dieser Anschluß ist derzeit nicht erreichbar ...« Und das, obwohl sein Mitarbeiter angab, in einem Gebiet zu sein, das auf einer Landkarte als »versorgt« angegeben wurde. Der Beschwerdeanruf beim Netzbetreiber soll daraufhin Klarheit geschaffen haben. »Ihr Mitarbeiter mit der Handy-Nummer 1234567 war an diesem Tag nicht dort, sondern im 150 Kilometer entfernten XY, und dort funktioniert unser Netz noch nicht.« Trotz offizieller Dementis sind Insider aus der betroffenen Branche überzeugt, daß es sich tatsächlich so zugetragen hat. Die Begründung: »Wenn eine Firma, die viele Handys bei uns angemeldet hat, droht, alle zu kündigen und diese beim anderen Mobilfunkbetreiber anzumelden, wird man ihm wohl jede Information geben.«

Vor einigen Jahren, als die österreichische Mobilkom noch in die staatliche Post eingegliedert war, meldete sich der Besitzer eines C-Netz-Telefons nach einem feuchtfröhlichen Heurigen-Besuch bei den Funktechnikern: Er wisse nicht mehr, wo er sein Auto geparkt habe. Die Techniker sollten ihm bei der Lokalisierung des Autos mittels C-Netz-Autotelefon helfen. »Wir haben ihm ausnahmsweise geholfen«, erzählt der Techniker. »Da beim C-Netz die Funkstationen aber ziemlich weit auseinander stehen, konnten wir ihm nur sagen, in welchem Bezirk sein C-Handy angemeldet ist. Diese Information hat ihm genügt, er hat sein Auto wiedergefunden.«

## *Großer Bruder hört mit*

Prognosen für das Jahr 2000 gehen davon aus, daß es in Deutschland 15 Millionen und in Österreich 3 Millionen Handy-Benützer geben wird. Die überwiegende Anzahl wird auf das als »abhörsicher« angepriesene CSM-Netz (Global System for Mobile Communications) setzen. Doch mit der Vertraulichkeit des GSM-Netzes ist es seit 1997 vorbei - Big brother is listening to you. Gemäß den Telekommunikationsgesetzen sind die Betreiber der Mobilfunknetze nämlich gezwungen, in ihren Netzanlagen Geräte zu installieren, die das Abhören von GSM-Gesprächen möglich machen. »Jeder Betreiber [...] ist verpflichtet, den gesetzlich zur Überwachung der Telekommunikation berechtigten Stellen auf deren Anforderung einen Nelzzugang [...] vorrangig bereitzustellen«, heißt es im § 88 Abs. 4 des deutschen Telekommunikationsgesetzes, das am 1. August 1996 in Kraft getreten ist. Ein ähnlicher Wortlaut im § 89 des seit 1. August 1997 gültigen österreichischen Telekommunikationsgesetzes hat auch die österreichischen Netzbetreiber erzürnt: »Der Betreiber ist […] verpflichtet, alle Einrichtungen bereitzustellen, die zur Überwachung des Fernmeldeverkehrs nach den Bestimmungen der StPO erforderlich sind.«

Den wahren Ärger hat aber der Anhang zu diesem Paragrafen ausgelöst: die Abhörgeräte sollen dem »jeweiligen Stand der Technik« entsprechen. »Das bedeutet«, befürchtete Ende 1997 der damalige max.mobil-Chef Hansjörg Tengg, »daß Innen- und Justizministerium uns zwingen können, ständig die neuesten Geräte zu installieren. Zahlen müssen immer nur wir.« Lapidarer Kommentar aus dem Innenministerium: »Verglichen mit den Lizenzgebühren [4 Milliarden Schilling, Anm.], sind die paar Millionen peanuts.«



Auf die Netzbetreiberkommen allerdings Investitionen in der Höhe von dreistelligen Millionenbeträgen zu. Allein die drei deutschen Mobilfunkbetreiber rechnen damit, daß sie diese Überwachung bis ins Jahr 2003 insgesamt 120 Millionen Mark kostet. Die österreichischen Netze Mobilkom und max.mobil gehen von Investitionen von je 150 Millionen Schilling aus. Zahlen müssen die Netzbetreiber, »obwohl wir an sich der Meinung sind, daß derjenige zahlt, der bestellt«, wie D1-Sprecher Stefan Wichmann betont. Der Mannesmann-Konzern (D2) wollte diese gesetzliche Zwangsbeglückung nicht hinnehmen und hat am 1. Juli 1996 eine Klage beim Verwaltungsgerichtshof in Köln (22K5896/96) eingebracht. Ein Urteil stand Anfang 1998 noch aus.

In Deutschland war Mitte 1997 die »Hochrüstung« der Netze bereits abgeschlossen. Was die Abhörgeräte genau können, wollen die Netzbetreiber nicht verraten. »Sonst kann die eine Seite, nämlich die Kriminellen, reagieren und die andere, das Innenministerium, noch bessere Geräte fordern.« Was sicher funktioniert: Hineinhören in Gespräche, das Lokalisieren von Handy-Benützern und die Gesprächsaufzeichnung.

Die Wunschliste des Innenministeriums ist jedenfalls endlos. In Deutschland genauso wie in Österreich. »Die wollen alles und jedes, weil sie es nicht bezahlen müssen«, bestätigt der Leiter des juristischen Dienstes der obersten Fernmeldebehörde in Wien, Alfred Stratil. »Die Leute vom Innenministerium fordern nicht nur Abhörgeräte, sondern auch Wortscanner, die sich automatisch einschalten und ein Gespräch aufzeichnen, wenn gewisse Reizworte fallen, und, und, und.« Auch eine Datei, in der die Namen sämtlicher Inhaber einer SIM-Karte (Subscriber Identification Module = Handy-Benutzerkarte) aufgelistet sind, stand im Forderungskatalog der österreichischen Sicherheitsbeamten. Diesbezüglich hat man sich vermutlich Deutschland zum Vorbild genommen, denn dort müssen alle Teilnehmerdaten - Name, Nummer, aktivierte Features wie etwa Fax- und Datenübertragung, verschlüsselte Kopien der Sicherheitscodes der SIM-Karte sowie die von den

Teilnehmern selbst festgelegten PIN-Codes fürs Aktivieren des Handys und der Mobilbox - den Sicherheitsbehörden weitergeleitet werden.

Die österreichischen Netzbetreiber halten die von oben angeordnete Handy-Spionage auch aus einem weiteren Grund für nicht sinnvoll: »Weil es nämlich sehr einfache Möglichkeiten gibt, der Kontrolle des Staates zu entkommen.« Zum einen werden Banden und Kriminelle mit Telefonwertkarten ausländischer Netzbetreiber, wie etwa aus der Slowakei, Tschechien oder Slowenien telefonieren und öfter die SIM-Karte wechseln. Roaming-Kosten {die Kosten für Handy-Teiefonate im Ausland) spielen im internationalen Verbrechen keine Rolle. Zum anderen kann man, zumindest in Österreich, auf die angebotenen Handy-Telcfonwertkarten ausweichen. Wer im Telefonnetz unentdeckt bleiben und weiterhin anonym telefonieren möchte, muß lediglich auf diese PrePaid-Produkte umsteigen. Anders als in Deutschland sind nämlich in Österreich B-Free oder klax.max, wie die Telefonwertkarten von Mobilkom und max.mobil heißen, anonym. In Deutschland müssen sich Kunden einer Bonitätsprüfung unterziehen und sogar Adresse und Bankverbindung angeben. In Österreich kauft man Handy oder Telefonwertkarte und kann sofort telefonieren. Eine Anmeldung soll, muß aber nicht zurückgeschickt werden.

## *Das GSM-Abhörgerät*

Das Abhören im GSM-Netz ist relativ einfach, wenn ein Handy-Teilnehmer mit einem Fcstnetzanschluß telefoniert. Das Gespräch geht vom Handy zur Basisstation, von dort zum Mobile Switching Center und dann ins Festnetz. Die Abhöranlagen sind im MSC installiert und fangen jedes Gespräch auf. Komplizierter wird es, wenn es darum geht, ein Handy-zu-Handy-Gespräch zu belauschen. Die absolute Abhörsicherheit des GSM-Netzes wird von den Mobilfunkbetreibern noch immer als Wettbewerbs- und Verkaufsargument angeführt. Obwohl bereits seit 1996 Geräte angeboten werden, die ein Abhören des GSM-Netzes möglich machen, halten dies manche Techniker nach wie vor für unmöglich bzw. noch für



zu kostenaufwendig. Doch mit der absoluten Vertraulichkeit ist es auch im CSM-Netz vorbei. Im März 1996 stellte ein amerikanisches Unternehmen sein GSM-Abhörsystem vor. Die Anlage und das Funktionsprinzip stellte bereits der deutsche Abwehrexperte Manfred Fink in seinem 1996 erschienenen Buch »Lauschziel Wirtschaft« vor. Seit 1997 ist bekannt, daß die in München ansässige Firma Rohde & Schwarz seit Jahren an einem derartigen Gerät tüftelt (vgl. »Spiegel«, 25. B. 1997). Die zwei Ende 1997 bekannten Modelle trugen die Typenbezeichnungen »GA 900« und »GA 901«.

Der IMSI-Catcher, wie sich die Anlage nennt, hört aber nicht ab, wie vielfach behauptet wird, sondern beschafft jene Information, die das Lauschen erst möglich macht. Um ein Handy abhören zu können, braucht man dessen IMSl (International Mobile Subscriber Identity); sie ist eine Kennummer, die beim Verbindungsaufbau mitgesendet wird. Wird mit dem Handy telefoniert, so übermittelt das Mobiltelefon seine Kennummer an den IMSI-Catcher (dieser muß sich aber in der Nähe des Handys befinden). Die IMSl wird in weiterer Folge an eine vorgetäuschte Funkstation der ermittelnden Kriminalisten weitergeleitet, die so klein ist, daß sie auch in einem Klcinlastwagen Platz hat. Diese Funkstation übermillelt dem Handy dann den Befehl: »Sende unverschlüsselt.« In der GSM-Technologie sind in Europa drei Verschlüsselungsvarianten, Algorithmen genannt, verbreitet. Ihre Code-Bezeichnungen lauten A5, A3 und A 0. AO bedeutet, daß nicht verschlüsselt wird. Und genau dieser Befehl, »sende auf A 0«, ermöglicht es den Behörden, Gespräche mitzuschneiden. Das Problem beim GSM-Lauschen ist allerdings, daß man merkt, wenn man abgehört wird. Von einem »gecatchten« Handy kann man nicht die Mobilbox anrufen, auch der Wählton ist anders.

Rohde & Schwarz zeigt sich zugeknöpft, will man mehr über den IMSI-Catcher wissen. Das Thema ist heikel, denn für die Mobilfunkbetreiber ist das Gerät, das eine Weiterentwicklung eines ganz normalen Testgeräts ist, ein Alptraum. »Im schlimmsten Fall kann das Netz einer ganzen Region zusammenbrechen«, seufzt D1-Sprechcr Stefan Wichmann. In den Labors der deutschen T-Mobil in Bonn wurde der IMSI-Catcher bereits getestet und zerlegt. Einer von vielen Prototypen, die Rohde & Schwarz in den vergangenen zwei Jahren entwickelt hat. Anfangs sollte ein Gerät etwa eine

Million Schilling kosten, mittlerweile liegt der Kaufpreis angeblich bei der Hälfte.

Verkaufsgespräche gibt es bereits seit eineinhalb Jahren. Nicht nur beim deutschen Bundesnachrichtendienst (BND) und beim Bundeskriminalamt (BKA) in Wiesbaden, auch aus dem Ausland melden sich Interessenten. Das österreichische Heeresnachrichtenamt (HNA) und die Staatspolizei haben sich von der Qualität des Geräts bereits überzeugen lassen. Anhand anschaulicher Praxistests, bei denen nicht nur die polizeieigenen Handys abgehört worden sind. Die deutschen und österreichischen GSM-Netze werden bereits abgehört. Im Frühjahr 1997 wurde im Zuge der Ermittlungen in einem »grenzüberschreitenden« Kokain-Fall ein GSM-Abhörgerät von den Behörden eingesetzt. Sowohl in Deutschland als auch in (Nieder-)Österreich wurde das GSM-Telefon eines Drogendealers überwacht. Ohne eine dafür notwendige Bewilligung der obersten Fernmeldebehörde.

Der Generaldirektor für öffentliche Sicherheit, Michael Sika, gibt aber unverblümt zu: »Das GSM-Netz stellt für uns überhaupt kein Problem mehr dar.« Unbestätigt ist auch das hartnäckige Gerücht, es seien 50 IMSI-Catcher bereits nach Rußland verkauft worden.

Gegen dieses Gerücht spricht allerdings die Tatsache, daß in bestimmten Ländern GSM-Gespräche ohnehin unverschlüsselt sind. Konkret wollen Techniker diese Länder nicht nennen, sie geben aber klar zu verstehen, daß man wohl in einigen Staaten des ehemaligen Ostblocks als Mobiltelefonierer damit rechnen muß, abgehört zu werden. Die Netzbetreiber vermuten deshalb, daß Handy-Erzeuger bald Mobiltelefone mit Warnlämpchen auf den Markt bringen - brennt das Lämpchen, sendet das Handy unverschlüsselt und ist leichter abzuhören.

## Von kleinen und großen Lauschangriffen

Die Begriffe sind verwirrend, da sie in Deutschland und Österreich eine unterschiedliche Bedeutung haben. Der »kleine Lauschangriff« in Österreich heißt, daß ein Kriminalbeamter oder eine Vertrauensperson bei einer verdeckten Aktion - wie etwa bei



Scheinkäufen von Suchtgift - ein Tonband oder ein Mikrofon am Körper trägt und das Gespräch überträgt. Bekanntes Beispiel dafür ist der Kriminalfall der russischen Geschäftsfrau Walentina Hummelbrunner. Sie hat den Erpressungsversuch des Wiener Autoverleihers Kalal für die Fahnder der EDOK (Einsatzgruppe zur Bekämpfung der Organisierten Kriminalität) übertragen und aufgezeichnet. Der deutsche »kleine Lauschangriff« hingegen erlaubt es den Kriminalisten, in öffentlichen Räumen und im Freien zu lauschen.

Der am 16. ianuar 1998 beschlossene »große Lauschangriff« in Deutschland erweitert den Einsatzbereich des Abhörens, in Zukunft werden auch Wohnungen und Privatsphäre zur Verbrechensbekämpfung überwacht, wenn ein Dreier-Richtersenat dem Antrag zustimmt. Nur bei Gefahr im Verzug dürfen auch andere Stellen wie etwa ein Polizeipräsident das Abhören anordnen. An sich wird der »große Lauschangriff« in Deutschland ohnehin schon praktiziert, in den Polizeigesetzen der Länder war das Abhören von Privatsphäre zur Gefahrenabwehr bereits erlaubt.

Im August 1997 hatten sich die Koalition und die SPD nach monatelangen Verhandlungen über das Abhören von Wohnungen geeinigt. Voraussetzung für das große Lauschen ist in Deutschland neben Änderungen in der Strafprozeßordnung und im Strafprozeßbuch ein geänderter Artikel 13 des Grundgesetzes - in Österreich mit dem Verfassungsgesetz vergleichbar -, für den eine Zweidrittelmehrheit notwendig ist. Widerstand gab es vor allem aus dem Lager der Grünen, die bei einer »Aushöhlung der Grundrechte« (»FAZ«, 1.9.1997) nicht mitmachen wollten. Auch bei der FDP meldeten sich Kritiker zu Wort, die in den geplanten Gesetzestexten noch einige »offene und noch zweifelhafte Fragen« geortet hatten.

Wie in Deutschland hat der Lauschangriff auch in Österreich heftige Diskussionen ausgelöst. Beim österreichischen »großen Lauschangriff«, der seit 1. Oktober 1997 im § 149 d der Strafprozeßordnung erlaubt ist, gehen die Ermittler mit Richtmikrofonen und versteckten Wanzen auf Verbrecherjagd. Gegner dieser Ermittlungsmethoden befürchten das Ende der Privatsphäre, da künftig auch Wohnungen belauscht werden dürfen. »Aber nur bei sehr schwerwiegenden Fällen, vor allem zur Bekämpfung der Organisierten Kriminalität«, heißt es im Justizministerium. »Denn der große Lauschangriff ist eine sehr teure Angelegenheit.«

Wird die Wohnung eines Verdächtigen oder die Zentrale einer Bande überwacht, so müssen die Kriminalisten und Kriminaltechniker mindestens dreimal «einbrechen« - wenn auch mit richterlichem Befehl. Einmal zum Auskundschaften der Wohnung: Es werden Fotos gemacht und Lageplan erstellt, anhand dessen die Plazierung der Abhörgeräte errechnet wird. Beim zweiten Besuch werden die Geräte im Wert von »mehreren Millionen« installiert, beim dritten montieren die Kriminalisten die Geräte wieder ab. »Wenn jemand glaubt, daß so etwas häufig vorkommt, hat er sich getäuscht«, verteidigt ein Justizbeamter den großen Lauschangriff. Die Organisierte Kriminalität (OK) kämpft mit den gleichen Mitteln wie die Kriminalisten, sie kennt fast alle Tricks. Wanzen, Abhör- und Videogeräte brauchen Strom. »Das hat sich auch schon bei der OK herumgesprochen. Wenn sich Banden in einer Wohnung treffen, schalten sie daher einfach alle Geräte ab, um nachzuprüfen, ob nicht doch noch irgendwo ein Stromschlucker, sprich eine Wanze, versteckt ist«, erklärt ein Kriminalist. Nachhilfe können sich sowohl die deutschen als auch die österreichischen Kriminalisten bei den Geheimdiensten holen. Denn sowohl für den BND als auch für das HNA und die Staatspolizei sind diese Methoden nicht ganz neu.

## Auf Reizworte programmiert

Obwohl es immer wieder beslritten wird, sind bei den Geheimdiensten in aller Welt Wortscanner im Einsatz. Große Erfahrung in diesem Bereich hat der Bundesnachrichtendienst, in Pullach, wie Udo Ulfkotte in seinem spannenden Buch »Verschlußsache BND« schreibt. Seit einem Jahrzehnt sind NASA-Spracherkennungscomputer in der Telefonüberwachung im Einsatz, Spracherkennungssysteme von IBM, Philips oder Siemens werden nun auch im zivilen Bereich angewendet - in Büros, bei Diktaten. Philips hat mit seinem »Genie« sogar ein Handy auf den Markt gebracht, das automatisch die Nummern aus dem eingespeicherten Telefonbuch wählt, wenn man den Namen in das Mikrofon spricht.
Diese hochkomplizierten Spracherkennungssysteme in der Form von Wortscannern überwachen den gesamten Telefonverkehr



Deutschlands. Die Technik hat sogar der deutsche Bundesbeauftragte für den Datenschutz, Joachim Jacob, in seinem Tätigkeitsbericht 1995-1996 exakt beschrieben. Dem BND ist es im Zuge der Fernmeldeaufklärung erlaubt, den gesamten Telefonverkehr von und nach Deutschland zu überwachen, und das sind etwa 8 Millionen Gespräche pro Tag. Hochkornplizierte Wortscanner überprüfen dabei die Gespräche und schalten sich automatisch ein, wenn bestimmte Reizworte fallen. Diese »Hit-Wörter« stammen aus den Bereichen Drogen- und Waffenhandel oder Terrorismus. Das Hit-Wörterbuch ist streng geheim. Beim Wort »Kalaschnikow« wird sich der Wortscanner vermutlich einschalten, doch weit heikler als dieses Wort sind für die Agenten des BND russische und chinesische Wörter, wie sie bei der russischen Mafia oder bei den chinesischen Triaden verbreitet sind.
Ähnliche Wortscanner könnte sich das österreichische Innenministerium auch für Österreich vorstellen. Ob Heeresnachrichtenamt, Heeresabwehramt (HAA) oder die Staatspolizei diese Technik nutzen, ist gut gehütetes Geheimnis. Bei den Mobilfunknetzen möchte man die Wortscanner im Kampf gegen das organisierte Verbrechen einsetzen, also auch im Kampf gegen den internationalen Drogenhandel. Ob aber in diesem Bereich Wortscanner die ideale Lösung sind, ist fraglich, geben Techniker zu bedenken. Wenn das Wort »Kokain« etwa einen Aufnahmemechanismus auslösen würde, wären in der Kokain-Al'färe des österreichischen Schispringers Andreas Goldberger wohl beinahe alle Telefonate in Österreich aufgenommen werden. Auch das Wort »Schnee« als Synonym für Kokain sei ein Problem. Was tun die Sicherheitsbeamten, die die Aufzeichnungen auswerten, in einem strengen Winter?

## Unschuldig abgehört

Belauscht zu werden kann jeden treffen, auch wenn er nichts verbrochen hat. Die Statistik beweist es. In Deutschland werden pro Jahr mehr als 6400 Telefonüberwachungen durchgeführt, ein Viertel der Überwachungen betrifft Mobiltclefone. In Österreich genehmigten die Gerichte 1996 (gemäß § 149 a ff. Strafprozeßord-

nung) insgesamt 319 Telefonüberwachungen (eine Unterscheidung zwischen Fest- und Mobilnetz wird in der österreichischen Statistik nicht gemacht). Dabei wurden nicht weniger als 644 Anschlüsse kontrolliert - 270 Telefone davon sogar länger als einen Monat. Beinahe alle 13 Stunden wird in Österreich ein Telefon angezapft. Das österreichische Magazin «News« behauptet sogar, daß die Polizei jährlich 70000 Telefongespräche abhört, und listet die interessantesten Fälle der österreichischen Kriminalgeschichte auf- vom Wiener Bau-Skandal rund um das Allgemeine Krankenhaus (AKH) über den Fall Lucona bis zum Noricum-Skandal. »Grundsätzlich ist Österreich ein Land der Lauscher und Spitzel«, schreibt »News«. »Im prozentuellen Vergleich mit den USA werden bei uns zehnmal mehr Telefonüberwachungen genehmigt als in Amerika.« {»News«, Nr. 18/97) Rekordhalter beim Abhören ist das Wiener Sicherheitsbüro, dicht gefolgt von der Truppe des niederösterreichischen Drogenfahnders und Leiters der Polizei auf dem Flughafen Wien-Schwechat, Oberst Alfred Rupf. An dritter Stelle folgt die Staatspolizei, die im Kampf gegen Rechtsradikale immer ein Ohr in der Leitung hat.

Zwar wurden in Österreich die Telefonate von 568 Verdächtigen belauscht, aber die Zahl der unschuldig Überwachten - als »unbeteiligte Dritte«, wie es in einem Bericht des Justizministeriums heißt - ist groß. 283 Personen wurden 1996 bespitzelt, ohne etwas verbrochen zu haben. Ihre Protokolle landeten sogar in den Akten und bleiben dort 30 ]ahre lang. Dokumentiert für die Nachwelt.

Die Gerichte sind sehr großzügig bei der Genehmigung von telefonischen Abhörungen. »Es wird so gut wie kein Fall abgewiesen«, bestätigt auch ein Insider. Im Fall des Frauenrnörders )ack Unterweger etwa wurden insgesamt zehn Telefonanschlüsse überwacht. Daß hier auch Unschuldige zum Handkuß kamen, nur weil sie mit dem Frauenmörder bekannt waren, ist klar. Die Telefonüberwachung kostete den Staat 2 Millionen Schilling. Die österreichische Post mußte einen eigenen Beamten abstellen, der die Kriminalisten bei ihren Erhebungen unterstützte. Üblicherweise kostet die Telefonüberwachung pro Fall im Durchschnitt 10000 bis 20000 Schilling. Neben den »legalen« Überwachungen werden Telefone aber auch von Geheimdiensten überwacht. Entdeckt werden sie meist durch Zufall. Der »Kurier« berichtete am 5. November 1997 über einen



Abhörskandal in Wien, der den Ruf der Stadt als internationale Spionagedrehscheibe bestätigte: US-Agenten hatten ein Wählamt der Post und Telekom Austria (PTA) in Wien-Währing manipuliert. Ziel war es, Nordkorea-Diplomaten abzuhören. Die US-Lauscher hatten, vermutlich mit Hilfe eines Beamten, in das Wählamt eine »technische Brücke« zwischen Relais eingebaut. Bei jedem Anruf bei einer bestimmten Telefonnummer wurde das Gespräch gleichzeitig auch an ein zweites Telefon geschaltet. Konkret wurde das Telefon des 1. Sekretärs der nordkoreanischen Botschaft abgehört. Von einer Wohnung aus, die ein als US-Diplomat getarnter Agent gemietet hatte. In der Wohnung fanden die Staatspolizisten Abhörgeräte, in regelmäßigen Abständen wurden die Tonbänder ausgewechselt und in die US-Botschaft gebracht. Der US-Diplomat mußte aufgrund seiner diplomatischen Immunität wieder freigelassen werden, wurde aber in die Vereinigten Staaten zurückbeordert. Ungeklärt blieb, wie US-Agenten in das Wählamt gelangen und die Relais manipulieren konnten. Zutritt haben offiziell nur Postangestellte, Fremdpersonen wären sofort aufgefallen - der Fall wird wohl nie lückenlos aufgeklärt werden können.

Die Telefonüberwachung ist schon lange nicht mehr so kompliziert wie früher. Vorbei sind die Zeiten, in denen die Kriminalisten in die Wählämter marschierten und sich dort mit einem Tonband- oder Diktiergerät in die Leitung hängen mußten. Heute genügt ein Anruf beim zuständigen Techniker des Netzbetreibers, der auf richterlichen Befehl eine Leitung in die Büros der Kriminalisten, Einsatzkommandos und Sondereinheiten umleitet. Läutet das Telefon des Verdächtigen, klingelt gleichzeitig das Telefon bei der Polizei, dort zeichnet ein digitales Aufnahmegerät jedes Telefonat auf.

»Ohne richterlichen Befehl geht gar nichts«, heißt es bei den Netzbetreibern, »ob Festnetz oder Mobilfunknetz.« Oder doch? Richter sind überzeugt, daß einige »anonyme Hinweise« durch »illegale Methoden« - nicht genehmigtes Abhören - zustande kommen. Wenn z. B. Kriminalist Hans Funktechniker Karl anruft und ihn bittet: »Karl, schalt schnell die Leitung rüber.« In den Führungsetagen der Netzbetreiber werden solche Methoden als »völlig undenkbar« bezeichnet. Der Ansprechpartner innerhalb des Unternehmes, der das Abhören genehmigt und den Auftrag dazu erteilt, ist nicht ident mit jenem Techniker, der die Umschaltung vornimmt.

Daß manchmal sogar ein kleiner Polizeichef und Richter seine eigene Auslegung von Telefonüberwachung hat, beweist die Tatsache, daß die Post und Telekom Austria vor kurzem mit der Anfrage eines Polizeichefs eines örtlichen Postens konfrontiert war, der einen Telefonanschluß abhören wollte. Und ein Richter verlangte sogar, vermutlich in Unkenntnis der gesetzlichen Lage, Gespräche in das Zimmer eines Gendarmeriepostens umzuleiten.

Auch in Deutschland werden zu viele Telefone abgehört. Zu diesem Schluß kommen Andreas Böttger und Prof. Christian Pfeiffer aus Hannover in ihrer Vergleichsstudie »Der Lauschangriff in den USA und in Deutschland«: »Für den deutschen Bürger ergibt sich ein etwa 13mal so hohes Risiko, Ziel einer Überwachungsmaßnahme zu werden, wie für einen amerikanischen Bürger.« Innerhalb von zehn Jahren hat sich die Zahl der Telefonüberwachungen in Deutschland vervierfacht. Waren es 1987 nur 1806 Fälle, so wurden 1996 exakt 6428 telefonische Lauschangriffe registriert. Insgesamt wurden 8 1 1 3 Anschlüsse überwacht. Zwar richtete sich der Lauschangriff nur gegen 8922 verdächtige Personen. Aufgrund der enorm großen Anzahl an überwachten Anschlüssen kann aber angenommen werden, daß die Gespräche von Tausenden unschuldigen Deutschen in die Abhörprotokolle gelangen. Tatsache ist, daß es bei den Statistiken, die die Abhörungen betreffen, zu Ungereimtheiten und »erheblichen Diskrepanzen« kommt, was selbst der parlamentarische Strafrechtsausschuß in seinem Bericht bestätigt hat. Die Justizministerien nennen andere Abhörzahlen als die Netzbetreiber. Während die »justitiellen Bedarfsträger« von 3182 Betroffenen ausgehen, gaben die Netzbetreiber 8922 betroffene Personen an, die bei 6428 Anordnungen überwacht wurden.

Viele Telefonüberwachungen beinhalten aber nicht die Gesprächsaufzeichnung, sondern eine Rufdatenerhebung - mit wem hat Verdächtiger X wann telefoniert etc. »Das Auskunftsersuchen ist oft aufwendiger als die Gesprächsüberwachung«, bestätigt ein Techniker der Deutschen Telekom. 87 Tage lang bleiben bei der Telekom die Gesprächsdaten gespeichert. Will eine Polizeidienststelle sämtliche Gespräche und Nummern aufgelistet haben, die ein Verdächtiger in diesen 87 Tagen geführt und empfangen hat, so kostet das eine gewaltige Summe - 10000 Mark pro Stunde Rechncrzeit. Billiger gibt es da schon die österreichische PTA. Eine



nachträgliche Bekanntgabe der Gesprächsdaten kostet 10000 Schilling. In Österreich sind die Gesprächsdaten allerdings drei Jahre lang in den Computersystemen der Billing-Center (Telefonbetreiber-Verrechnungscenter) zu finden.

Ein Paradebeispiel dafür, wie informativ Gesprächsdaten für die Kriminalisten sein können, war der tödliche Unfall von Prinzessin Diana in Paris. Anhand der Gesprächsaufzeichnungen von den Handys der Paparazzi konnte die Polizei nachweisen, daß die Sensationsreporter zuerst ihre Fotoagenturen und nicht, wie behauptet wurde, die Rettung verständigt hatten.

## Auch Faxe sind nicht sicher

Vertrauliche und geheime Mitteilungen sollten nicht via Fax bekanntgegeben werden, denn nicht nur Telefonate, auch Fax-Geräte können abgehört werden. Dabei wird lediglich ein zweites Fax-Gerät an den Anschluß parallel geschaltet. Das kann zum einen im Haus selbst gemacht werden, wo sich das Fax-Gerät befindet, aber auch in der Vermittlungszentrale. Jedes Fax, das beim Anschluß A einlangt, wird dann auch vom Gerät B ausgedruckt - ohne daß es der Besitzer der Fax-Nummer merkt.

Unsicher sind Fax-Mitteilungen auch noch aus einem anderen, sehr simplen Grund: Faxe langen nicht immer dort ein, wo sie ankommen sollen. Etwa weil irrtümlich die falsche Nummer gewählt wurde. So passiert es, daß Abhörprotokolle statt im Gericht bei Privatfirmen oder Mitteilungen von Staatsanwälten in Privathaushalten landen. Besonders peinlich war die Fehlleitung einer Bezirksregierung in Nordrhein-Westfalen. Die Beamten wollten Beurteilungsdaten mehrerer Polizeibeamtcn ans Innenministerium faxen. Das Fax landete aber nicht beim Innenministerium des Landes Nordrhein-Westfalen, sondern beim Landesbeauftragten für den Datenschutz. Zum Glück - nicht auszumalen, hätte diese heiklen Informationen ein Fax-Gcrät in einem Haushalt oder einer Firma zutage befördert.

Doch auch das kommt vor, wie der »Spiegel« (Nr. 30/97) berichtete: Ein Leipziger Immobilienmakler erhielt am 3. Juli 1997 sechs

Seiten detaillierte Polizei- und Meldedaten sowie eine Mitteilung aus dem BKA-Fahndungscomputer über einen indischen Staatsbürger zugefaxt. Absender war die Bahnpolizeiwache Leipzig des Bundesgrenzschutzes. Nachdem der Immobilienmakler die Polizisten über ihr fehlgeleitetes Fax informiert hatte, wurde er gebeten, die Fax-Seiten zu vernichten. Eine halbe Stunde später langte ein weiteres Fax der Leipziger Bundesgrenzschützer ein. Die Erklärung der Beamten: ein Kollege habe das Fax-Gerät falsch bedient.

## Gefährliche Anrufbeantworter

Beinahe jeder dritte Haushalt ist mit einem Anrufbeantworter ausgerüstet. Wer sich einen Anrufbeantworter kauft, sollte sich für ein Modell entscheiden, das mit einem vierstelligen PIN-Code (Personal Identification Number) gesichert ist: Bei praktisch jedem auf dem Markt angebotenen Gerät funktioniert die Fernabfrage - aus der Ferne kann das Tonband des Anrufbeantworters durch Eintippen eines Zahlencodes abgerufen werden. Diese Nachrichten können mitunter aber von Unbefugten abgehört werden. Aus zwei Gründen: Zum einen gibt es Anrufbeantworter auf dem Markt, die nur mit einem zweistelligen Code gesichert sind. Zum anderen vergessen viele, nach dem Kauf eines Anrufbeantworters den vom Werk einprogrammierten Code zu ändern. Denn die Hersteller haben oft die gleichen Modelle mit dem gleichen Code abgesichert. Wer sein Paßwort nicht ändert, kann von Besitzern des gleichen Anrufbeantworter-Modells abgehört werden, da auch jenem der Code und die Funktionalitäten bekannt sind. Das wiederum bedeutet, daß sogar Nachrichten gelöscht und die Raumüberwachung aktiviert werden können.

## Der Lügendetektor für den Hausgebrauch

Lügendetektoren gibt es nur bei Geheimdiensten und in Hollywood-Streifen. Seit 1 7. Dezember 1997 aber bietet das israelische Unternehmen Makh Shevet ein derartiges Gerät für den Hausgebrauch an. Es nennt sich »Truster«, kann an jedes gewöhnliche Haustelefon angeschlossen werden und entlarvt angeblich Schwindler und Lügner - von untreuen Ehegatten bis zu Versicherungsbetrügern.



Während herkömmliche Lügendetektoren mit Elektroden die Körperreaktionen messen, analysiert der Truster die Unwahrheit anhand der Stimme. Das Prinzip beschrieb der Projektleiter Amir Liebermann in der »Welt« (19.12.1997): »Wenn das Gehirn etwas hört, was der Mund sagt und womit es nicht einverstanden ist, dann gibt es eine Verzögerung in der Stimme. Und diese winzigen Effekte können wir messen und analysieren.« Die Anregung zum Online-Lügendetektor gaben die israelischen Sicherheitsbehörden, die durch bloßes Befragen herausfinden wollten, ob ein einreisender Palästinenser »harmlos ist oder einen Anschlag plant«, wie die »Welt« schrieb.

Seit 17. Dezember 1997 ist die israelische Truster-Variante auf dem Markt, die englische Version wurde eine Woche später präsentiert, die deutsche ist seit 15. Februar 1998 erhältlich.

Drei verschiedene Ausführungen werden angeboten, die Modelle kosten 149 Dollar, 500 und 2500 Dollar. Die Zuverlässigkeit liegt, so verspricht der Hersteller, bei 85 Prozent. Lediglich bei Psychopathen funktioniert der Truster nicht, »weil sie von dem, was sie sagen, überzeugt sind und es nicht überdenken«.

Das Interesse für den Truster ist jedenfalls groß, bestätigt Makh-Shevet-Generaldirektor Tamir Segal. Denn der Truster ist (bis auf das für den Telefonanschluß mitgelieferte Kabel) kein Gerät, sondern eine Software, die auf einer CD geliefert wird. Voraussetzung ist ein 32-MB-Laufwerk und Windows 95. Sowohl aus Deutschland wie auch aus Österreich liegen bereits Hunderte Bestellungen vor. In den ersten vier Wochen wurden bereits 150 Stück nach Deutschland und Österreich verkauft. Ob der Truster gegen bestehende Gesetze verstößt- immerhin ist er durchaus mit einem Lauschangriff zu vergleichen -, ist derzeit nicht klar. »Wenn in einem bestimmten Land den Leuten dabei mulmig wird, dann werden sie sich wohl ein spezielles Gesetz überlegen müssen«, meinte sogar Makh-Shevet-Generaldirektor Tamir Segal in der »Welt«.

## Pager-Botschaften für jedermann

Alles, was die Schnüffler brauchen, ist ein normaler PC und ein Scanner. Mühelos kann man die Text-Nachrichten, die an andere bestimmt sind, mitlesen. »Schatz, vergiß Brot und Milch nicht«, »Wir treffen uns im Stadtcafe, Gruß Olli« oder »Lisa, war ich gut gestern nacht?« Der »Stern« (Nr. 30/97) machte auf das Problem aufmerksam, daß Telefon-Botschaften über Textpager von Fremden mitgelesen werden können. Auch von der Polizei. Vielen ist es vielleicht egal, ob auch andere wissen, daß man für den Einkauf zuständig ist, daß man ein geselliger Mensch ist und sich gerne mit Freunden trifft. Aber der deutsche Bundesdatenschützer Joachim Jacob befürchtet, daß sich eine relativ große Zahl von Computer-Experten diese Möglichkeit zielgerichtet nutzbar machen könnte - auch für kriminelle Zwecke, denn mit der Nachricht wird auch die Pager-Nummer mitgeliefert. Sein Rat: Wichtige Informationen nicht via Pager verschicken. »Das ist quasi wie eine Botschaft über die >Tagesschau<.«

Zum einen kann wochenlang eine bestimmte Pagernummer gezielt abgehört, sprich jede Nachricht mitgelesen werden, wodurch ein Bild des Besitzers entsteht - Beruf, Hobbys, Alltag. Aufgrund der Pager-Nachrichten läßt sich klar erkennen, ob der Besitzer verheiratet ist, ob er Kinder hat, wie seine Freunde heißen, wo er arbeitet etc. Zum anderen können Hacker den Pager-Inhaber sogar gezielt in die Irre führen und Falschmeldungen ins Display schicken - »Bitte um Rückruf unter 1234567«. Ruft der Inhaber retour, scheint aufgrund der digitalisierten Anschlüsse in Deutschland auch die Nummer im Telefondisplay auf. Über diese Nummer kann der Hacker dann - mit Hilfe von in Deutschland zwar verbotenen, aber trotzdem auf dem Markt erhältlichen Telefon-CDs -, den entsprechenden Namen und die Adresse finden. In Österreich sind diese CDs sogar erlaubt.

Der scheinbar aus der Mode gekommene Pager hat in den vergangenen zwei Jahren ein Revival erlebt. 1,2 Millionen Pager-ßesitzer gibt es in Deutschland, 150000 sind es etwa in Österreich. Den Boom haben vor allem die CPP-Pager (Calling Party Pays) ausgelöst, bei denen der Anrufer die Kosten übernimmt. Ein weiterer Vorteil der CPP-Pager ist die Anonymität. Der Pager ist beim Kauf sofort aktiv, eine Anmeldung nicht mehr notwendig. Der Besitzer des »Piepserls« bleibt unbekannt. Beliebt sind diese anonymen Kommunikatoren - ob sie nun Seall (T-Mobil), Quix (Deutscher Funkruf), TellMe (Miniruf GmbH) oder CallMe (Mobilkom) und Airpage heißen - vor allem bei Drogendealern.

Alexander (Name geändert) ist als Ecstasy-Dealer in den Techno-Tempeln im Osten Österreichs Stammgast. »Immer wenn der Pager piepst, wird bestellt. Jede Nachricht bedeutet Bargeld.« Angst vor der Polizei hat er keine, denn sein Pager ist anonym. »Keiner weiß, wer hinter dieser Pager-Nummer steckt. Und den Anmeldeschein, den man ausfüllen soll, habe ich nicht zurückgeschickt.«



## Die Jagd nach Telefon-Betrügern

Tag und Nacht sitzen sie vor den millionenteuren Geräten und warten darauf, daß diese Alarm schlagen. Den 30 ßetrugsbekämpfern der Fraud-Divison in der deutschen Telekom entgeht nichts. Von Düsseldorf aus kontrollieren sie praktisch den gesamten Telefonverkehr Deutschlands. In jeder Nacht rücken sie mindestens zehnmal aus, urn gemeinsam mit der Polizei Telefon-Betrüger dingfest zu machen.

Die Systeme schlagen bei »Unregelmäßigkeiten« Alarm, bei »untypischem Telefonierverhalten«. Wenn jemand pro Tag durchschnittlich zehn Telefonate führt, plötzlich aber hundert. Wenn Telefonkoslen von einem Tag auf den anderen ins Uferlose steigen oder wenn auffällig lange Gespräche von einem Telefon geführt werden. Mit Hilfe des Zeitfaktors kann auch auf mögliche Raubkopien von SIM-Karten rückgeschlossen werden. Es ist nicht möglich, mit einem Handy um 12 Uhr in Hamburg zu telefonieren und eine Stunde später in Darmstadt. Ab einer Entfernung X muß eine bestimmte Zeit Y vergehen. In allen diesen Fällen kann es leicht passieren, daß plötzlich Betrugsbekämpfer vor der Tür stehen.

Weltweit beträgt der Schaden, der den Telcfongesellschaften durch Fraud, also Betrug, entsteht, 8 Milliarden Dollar. Allein in Deutschland sind es Hunderte Millionen Mark, bei den Mobilfunkbetreibern verursachen Telefonbetrüger einen Schaden von etwa 2-3

Prozent des Telefonumsatzes, jede Gesellschaft, jeder Mobilfunk-Netzbetreiber hat deshalb ein eigenes Fraud-Team. Die allumfassende Kontrolle kommt den Kunden zugute, so wird begründet. Denn damit wird verhindert, daß Leitungen angezapft werden oder, wie vor einigen Jahren noch modern, Telefonrechnungen in die Tausende Mark bzw. Zehntausende Schilling steigen, weil durch ein Anzapfen des Anschlusses Sex-Hotlines auf den Antillen angerufen wurden. Nicht zuletzt aufgrund dieser Skandale muß sich in Deutschland jeder, der in gewisse Karibik-Staaten telefonieren möchte, von einem Operator vermitteln lassen. Aber Achtung, die »Dame vom Amt« hört mit. Im Sommer 1996 wurde ein Skandal bekannt, der das »Telekom Operator Service - Auslandsvermittlung« in Frankfurt am Main betraf. Hier wird ein handvermittelter Telefondienst angeboten. Jedes Telefonat wird aus Abrechnungsgründen auf einem eigenen »Gesprächsblatt« dokumentiert. Zur »Beobachtung des Verbindungsstatus und zur Ermittlung der Gesprächsdauer« konnte der Operator nach Lust und Laune auf eine »Mithör«-Taste drücken, um sich von der »Qualität der Verbindung zu überzeugen«, wie im Tätigkeitsbericht des Bundesdatenschützers lakonisch angemerkt ist. Wie oft der Operator ins Gespräch hineingehört hat, ist freilich unbekannt. Die Telekom begründete das amtliche Lauschen damit, daß es Staaten gebe, in denen aufgrund der dort veralteten Technik kein Signal über das Verbindungsende übermittelt werde und man deshalb »Hineinhören« müsse. Für 1998 wurde ein neues Operator-Service angekündigt.

## Schau mal, wer da spricht

Den meisten Telefonbesitzern ist es nicht bewußt, aber wer in Deutschland telefoniert, ist entlarvt. Seit 1998 sind in Deutschland alle 38,5 Millionen Telefonanschlüsse digitalisiert, in Österreich wird die Digitalisierung des 3,9 Millionen Anschlüsse umfassenden Netzes erst 1999 abgeschlossen. Digitalisierte Anschlüsse (inklusive ISDN-Kanäle) bedeuten nicht nur rauschfreie Verbindungen, sondern auch, daß bei jedem Telefonat die eigene Rufnummer



übermittelt wird und diese im Telefondisplay des Angerufenen aufscheint. Das kann sehr praktisch sein, wenn man entscheiden will, ob man etwa das Gespräch eines lästigen Geschäftspartners annimmt oder nicht. Es kann mitunter aber auch die Gefahr der totalen Kontrolle mit sich bringen. Sogar Erpressung ist möglich, wie Beispiele in Österreich zeigen.

Wer auf ein »fesselndes Vergnügen«, auf den »Erstversuch« oder auf das »Kuschelkätzchen« abfährt, kann eine böse Überraschung erleben. Wer etwa von seinem GSM-Handy eine der vielen Handy-Kontaktadressen anwählt, übermittelt nicht nur seine Telefonnummer, die im Display ablesbar ist, das Menü »Anrufregister« im angerufenen Handy speichert gleichzeitig diese Nummer. Mit der Möglichkeit der Inverssuche bei der Telefon-CD (über die Telefonnummer zum Namen) lassen sich problemlos Name und Adresse eruieren.

Zwar besteht die Möglichkeit einer Rufnummern-Unterdrückung - beim Handy ist diese über das Display programmierbar-, dies wird aber sehr wenig genutzt. In Österreich etwa stellen pro Monat im Durchschnitt lediglich 30 Kunden einen diesbezüglichen Antrag, obwohl die »immerwährende Anonymität« nur 60 Schilling kostet. Bei der Rufnummern-Unterdrückung wird verhindert, daß die Nummer übertragen wird. »Im Netz werden die Ziffern aber trotzdem durchgegeben«, erklärt der Netzsicherheitsbeauftragte der PTA, Rudolf Rapp. Andernfalls wären Fangschaltungen unmöglich.

Zwischen 300 und 400 Fangschaltungen werden pro Monat in Österreich beantragt- 100 Schilling Grundgebühr, 20 Schilling pro gefangenem Anruf und 10 Schilling Taggeld kostet das. Aber nicht alle Anträge werden genehmigt, wie Beispiele aus einigen »katholischen Bundesländern« gezeigt haben. Prostituierte und Sex-Hotline-Anbieter hatten Fangschaltungen beantragt, weil sie sich von Anrufern angeblich belästigt fühlten. Der wahre Hintergrund: Man wollte an die Daten potentieller Kunden herankommen. Die Anträge wurden allesamt abgelehnt.

Nicht ganz unproblematisch sind auch die neuen Call-Center, die bei Versandhäusern und Telefongesellschaften eingesetzt werden. Die kalifornische Aspect Telecommunications Corporation vertreibt Call-Center, die »zur Optimierung des Kundenservice« beitragen, wie die Geschäftsleitung verspricht. Nutzer dieser Technologie ist

beispielsweise die österreichische PTA. Ein Anrufer wird mittels automatischer Anruferkennung identifiziert, sprich: anhand der Telefonnummer erkennt das System, um wen es sich handelt. Innerhalb von Sekundenbruchteilen werden automatisch die gespeicherten Kundendaten auf den Bildschirm des PCs eines Kundendienstbetreuers übermittelt. Problem dabei ist aber, daß der Anrufer nicht mit dem Inhaber des Telefonanschlusses ident sein muß.

## Vorsicht bei Babyphones

Was haben die jungen Mütter in Leipzig, Berlin, Wien und Graz gemeinsam? Sie verwenden Babyphones. jene kleinen Funkgeräte, die jedes Wispern, Husten und Weinen ins Schlafzimmer der Eltern übertragen. Die technische Erfindung, die schon vielen Kleinkindern das Leben gerettet hat, ist aber auch für manch eigenartig veranlagten Lauscher von Interesse, »jeden Abend um die gleiche Zeit hör ich aus meinem Babyphone die Stimme der Nachbarin, die etwa 200 Meter von uns entfernt wohnt«, erzählt die junge Mutter aus einem kleinen Dorf in Niederösterreich und hat damit eine der negativen Seiten des Babyphones kennengelernt. Denn so wie sie die Nachbarin hört, könnte auch ihre Stimme oder das Gespräch mit ihrem Mann live in das Babyphone der Nachbarin übertragen werden. Babyphones sind, da sie ganz simple Funkgeräte sind, mit einem Scanner leicht abzuhören. Wer am Geschrei eines Kleinkindes Interesse haben soll? Lauscher sind nicht an den Geräuschen aus den Kinderzimmern interessiert, sondern vielmehr am Seufzen und Stöhnen aus den elterlichen Schlafzimmern.

## Das manipulierbare Netz

Mehrmals im Jahr lauern die Männer der Funküberwachung vor den berüchtigten Gefängnissen Österreichs in Krems-Stein oder Graz-Karlau. Wie im Film sitzen sie in weißen Lieferwägen, die im Inneren mit Peilsendern, Frequenzmessern und Funkempfängern



ausgestattet sind. Ihr Auftrag lautet: Aufspüren eines Mobiltelefons und die Identität des Besitzers feststellen.

Die österreichischen D-Handys (in Deutschland mit dem C-Netz vergleichbar) haben sich zum Lieblingsspielzeug mancher Häftlinge entwickelt, die von der Zelle aus den Drogenhandel oder sogar Ausbrüche organisieren. Offiziell dürfen Häftlinge zwar nur die Telefonzellen benützen, doch werden über dubiose Wege Mobiltelefone in Gefängnisse geschmuggelt. Die Ausforschung der Besitzer ist mit einem enormen Aufwand verbunden. Oft dauert es Tage, bis ein Handy lokalisiert und der Benutzer ausgeforscht ist. »Mit Peilgeräten und Scannern werden so lange alle Frequenzen abgesucht, bis man jene hat, die ausschließlich die des Häftlings sein kann«, erklärt der Leiter der Funküberwachung, Karl Katzenbeisser. Von der passenden Funkfrequenz ist es nicht mehr weit zur Telefonnummer, dann sind die Justizwachebeamten am Zug.

Dem österreichischen D- und deutschen C-Netz eilt der schlechte Ruf voraus, daß man sie abhören könne. Dieses Image rückt Katzenbeisser zurecht: »Diese Netze kann man nicht abhören, sondern nur belauschen. Gezieltes Abhören ist nur dann möglich, wenn die Örtlichkeit bekannt ist und eingegrenzt werden kann.« Lauscher an den Scannern - das sind in Deutschland, so schätzt Abwehrexperte Manfred Fink, etwa 1 Million, in Österreich etwa 30000 - sind auf den Zufall angewiesen. Der Besitz von Scannern ist in beiden Staaten erlaubt, der Betrieb paradoxerweise verboten.

D- und C-Netz bergen andere Gefahren in sich, weiß der Funkexperte aus eigener Erfahrung. Die relativ leicht durchschaubare analoge Technik nutzen vor allem afrikanische »Handy-Banden«. Sie mieten Hotelzimmer, in denen sie bis zu zwölf D-Handys aneinanderschalten, und vermitteln Telefongespräche. Von Rom via Wien nach Nairobi oder von Paris via Wien nach Bangkok. Von in der Gegend zufällig telefonierenden C- oder D-Handy-Benützern schnappen Scanner Nummern, PINs und Codes auf. Diese werden decodiert und dann in die manipulierten Handys eingespeichert. Telefonate Rom-Wien-Nairobi etwa werden dann entweder mittels Drahtverbindung hergestellt oder aber auch akustisch, indem beide Lautsprecher miteinander verbunden werden. Zweimal pro Monat müssen die Funküberwacher ausrücken, um »Handy-Banden« mit Peilsendern auszuforschen.

# Voll erfaßt im Straßenverkehr

> Wie Temposünder durch Road-Pricing überführt werden.

> Warum jeder gefahrene Meter dokumentiert wird.

> Wie Firmenchefs die totale Kontrolle über ihre Mitarbeiter haben.

> Wie man mit Hilfe von Road-Pricing perfekte Bewegungsprofile erstellen kann.

> Warum Road-Pricing das Ende der Privatsphäre bedeutet.

> Warum man mit Staukameras nicht nur Kolonnen filmen, sondern auch das Handy-Verbot überwachen kann.

> Warum Satelliten-Road-Pricing die Verbrechens-Aufklärungsrate verbessern würde.

> Wie mit Navigationssystemen **nicht** nur navigiert, sondern auch überwacht wird.

## Autofahrer unter ständiger Beobachtung

Sobald das Auto von der Garagenausfahrt auf die Straße fährt, beginnt das Zählwerk zu laufen: 2,7 Kilometer Landstraße, 3,1 Kilometer Bundesstraße und 57 Kilometer Autobahn legt Laborchemiker Roderich Preissler auf dem Weg zu seinem Arbeitsplatz täglich zurück. Ein Kilometer Landstraße kostet ihn 2 Cent, wie die Pfennige und Groschen nach der Euro-Einführung heißen werden. Für einen Kilometer Bundesstraße muß er 3 und für einen Kilometer Autobahn 5 Cent bezahlen. Jeder Arbeitstag kostet Roderich



Preissler also sage und schreibe 5,9 Euro Fahrtkosten, was derzeit etwa 11,50 Mark oder 80 Schilling wären. Der Betrag wird von der Chipkarte des Empfangsgerätes in seinem Wagen automatisch abgebucht. Um 6.46 Uhr fuhr Roderich Preissler aus dem Haus, um 18.32 Uhr war er wieder daheim. Für die Hinfahrt benötigt er 42 Minuten, für die Rückfahrt 1 Stunde 16 Minuten. Auf dem Nachhauseweg hatte er einen 23minütigen Zwischenstopp bei einem Einkaufszentrum eingelegt.

Das Road-Pricing-System der Zukunft weiß alles. Flächendeckend werden alle Straßen Deutschlands und Österreichs erfaßt. Via Satellit werden die Autos verfolgt und jeder gefahrene Meter nach Ort und Zeit genau dokumentiert. Die Informationen werden gespeichert - zu »Kontrollzwecken«, um bei Reklamationen Beweismittel in der Hand zu haben.

Was wie Utopie klingt, könnte sofort realisiert werden. Das haben Landvermesser bereits im Juni 1997 am Rande des 6. Österreichischen Geodätentages in Villach bestätigt. Europaweites Road-Pricing via Satellit wäre sogar um einiges kostengünstiger als die derzeit diskutierten Varianten mit fix montierten Balken bei der Fahrbahn - behauptet zumindest der oberste Landvermesser Österreichs, August Hochwartner, in einem Interview mit der Austria Presse Agentur (APA). Und die Erklärungen des österreichischen Präsidenten des Bundesamtes für Eich- und Vermessungswesen haben Gewicht.

Die derzeit diskutierten Road-Pricing-Systeme basieren auf der Kombination von im Auto installierten Geräten (sogenannte On-Bord-Units) und Sende- und Empfangsanlagen, die am Straßenrand oder über den Fahrbahnen montiert sind. Die On-Bord-Unit im Auto kann entweder ein reiner Sender und Empfänger sein, der im Inneren die Fahrtstrecke aufzeichnet und später ausgewertet wird. Er kann aber auch an eine Chipkarte gekoppelt sein. Bei dieser im voraus bezahlten »Smart-Card« werden die Kosten für die gefahrene Strecke direkt von der Karte abgebucht. Ist sie aufgebraucht, muß man eine neue kaufen.

Mit der Anonymität des Autofahrers ist es beim Road-Pricing auf jeden Fall vorbei, obwohl die Betreiber das Gegenteil behaupten. Denn zu Kontrollzwecken müssen die Daten, zumindest aber die letzte gefahrene Strecke, gespeichert sein. Mindestens 2 Milliarden Schilling würde die Realisierung der herkömmlichen Systeme in

Österreich kosten. Etwa 3 Milliarden Mark in Deutschland. In Zeiten von Sparpaketen und Arbeitslosigkeit werden sich die Verkehrsminister wohl für die kostengünstigere Variante entscheiden. Und die ist mit GPS-Satelliten zu realisieren.

## Die GPS~GSM-Kombination

Die Verknüpfung der beiden Technologien GPS (Global Positäoning System) und GSM (Global System for Mobile Communication) bringt zum einen viele Vorteile, zum anderen aber auch Gefahren mit sich. Beide Begriffe klingen zwar hochtechnisch, sind aber bereits Teil unseres Alltags geworden. Ein GSM-Handy beispielsweise haben bereits etwa 20 Prozent aller Deutschen und 30 Prozent aller Österreicher. Weltweit besitzen derzeit etwa 70 Millionen Menschen ein GSM-Mobiltelefon. Bis zum Jahr 2003 soll sich die GSM-Kundenzahl beinahe vervierfachen.

Die GPS-Technologie, die bislang nur Seglern ein Begriff war, setzt sich zunehmend auch im alltäglichen Leben durch. Nicht nur Geländewägen sind mit GPS-Empfängern ausgerüstet, auch die Navigationssysteme in neuen Automodellen der Luxusklasse arbeiten mit GPS. Ob Philips Carin 520 oder Carin 440, der Blaupunkt Travel Pilot, der Siemens AutoScout oder Delco Telepath - alle machen sich die Satellitentechnologie zunutze.

GPS wurde von der US-Armee erfunden und war ursprünglich nur für militärische Zwecke vorgesehen. 24 dieser Navigalionssatelliten kreisen dabei in einer Höhe von etwa 20200 Kilometern um die Erde. Erhält ein Empfänger - im Auto, im Schiff, es gibl aber auch eigene GPS-Empfänger für Wanderer - Daten von mindestens vier Satelliten, kann seine Position auf 50 bis 100 Meter genau festgestellt werden. Freilich geht es genauer, aber den »Regler« hat das US-Militär in der Hand: Von Amerika aus kann die Genauigkeit der GPS-Satelliten eingestellt werden. Beispiel dafür war der Absturz eines US-Kampfjets in Bosnien am 2. Juni 1995. Die F-16 war in der Nähe von Banja Luka im Westen Bosnien-Herzegowinas von bosnischen Serben abgeschossen worden. Kurz nach dem Absturz betrug die Ungenauigkeit der GPS-Daten einige Kilometer, man



sprach sogar von 15 bis 20 Kilometern. Die Amerikaner hatten am Regier gedreht, damit der Pilot Scott O'Grady nicht von den Serben geortet werden konnte. Sechs Tage nach dem Absturz wurde er gerettet, danach arbeiteten die Systeme wieder mit den gewohnten »kleinen« Abweichungen.

Diese Ungenauigkeit der GPS-Daten wird seit 1997 »bereinigt«. Das bis auf wenige Zentimeter genaue GPS nennt sich DGPS - Differential GPS. Dabei werden von einer Bodenstation, deren exakte Koordinaten bekannt sind und die zugleich ein GPS-Empfänger ist, die Ungenauigkeiten gespeichert. Diese Abweichungsdaten werden dann an Empfänger in der Umgebung gesendet, wie etwa Einsatzfahrzeuge.

Die dritte Komponenle neben GPS und GSM sind digitalisierte Straßenkarten. Größter Anbieter in Europa ist die in Hildesheim ansässige Firma Tele Atlas mit Zweigniederlassungen in Wien, Zürich, Gent und Mailand. Der Tele Atlas ist viel genauer als eine normale Landkarle, er ist digitalisiert. Jede Straße, die einen offiziellen Straßennamen trägt, ist dokumentiert. Sogar kleinste Landstraßen. Demnächst werden sogar Feld- und Waldwege in die Karte aufgenommen. Werden die Satellitendaten dann mit dieser digitalen Straßenkarte verknüpft, kann - auf wenige Zentimeter genau - festgestellt werden, auf welcher Straße sich mit GPS-Empfänger ausgestattete Pkw bewegen.

Beim Road-Pricing könnten die Fahrdaten dann zwischengespeichert und später ausgewertet oder gleich via GSM-Technologie an ein elektronisches Abbuchungssystem weitergeleitet werden.

Offiziell wurde das Thema Road-Pricing für Pkw sowohl in Deutschland als auch in Österreich ad acta gelegt. Aber gestorben ist das Projekt in beiden Ländern nicht. »Auf die Erhebung von Autobahngebühren beim Pkw wird bis auf weiteres verzichtet«, hat der deutsche Verkehrsminister Matthias Wissmann am 23. November 1995 versprochen. Die Betonung liegt auf »bis auf weiteres«. Denn die zuständigen Beamten in seinem Ministerium sind überzeugt, Anfang des kommenden Jahrtausends zuschlagen zu können. Und Wissmann selbst hat am 23. November 1995 via Aussendung mitteilen lassen, daß in Deutschland »nur vollautomatische Gebührenerhebungs- und Kontrollverfahren in Frage kommen, die in dieser anspruchsvollen Form bislang noch nirgends

im Einsatz sind«. Flächendeckendes GPS-Road-Pricing entspricht diesen Kriterien.

In Österreich hat der Autofahrerclub ÖAMTC nach einer Protestaktion das Pkw-Road-Pricing vorläufig zu Fall gebracht, aber die Straßenbenutzungsgebühr wurde bis Anfang 1998 noch immer nicht aus dem Bundesstraßen-Finanzierungsgesetz gestrichen. Das bedeutet: Road-Pricing ist in Österreich noch lange nicht gestorben. Denn: neue Regierung, neues Glück. Auch wenn Minister versprechen, daß etwas »politisch völlig vom Tisch« ist. Bei anderen politischen Konstellationen kommen gewisse Themen wieder auf die Tagesordnung.

Die Versprechungen deutscher und österreichischer Politiker sind nichts anderes als Absichtserklärungen. Denn am 22. September 1997 hat EU-Verkehrskommissar Neil Kinnock klar zu erkennen gegeben, daß er Road-Pricing forcieren wird. »Eine Verteuerung des Benzins erhöht nur die Kosten, löst jedoch nicht die Verkehrsprobleme.« Kinnock plädiert für eine möglichst EU-weite Einführung des Road-Pricing. Außerdem - und damit könnten alle Zukunftsvisionen wahr werden - fordert Kinnock, diese elektronische Maut von Fahrzeugtyp, Zeit und »Reisegegenden« abhängig zu machen. Wer beispielsweise zur Hauptverkehrszeit oder in Ballungsräumen unterwegs ist, zahlt mehr.

Kinnocks Ziele sind nur mit einem Satellitensystem zu realisieren, bestätigen Verkehrsplancr. Und genau diese Technologie macht aus jedem europäischen Kfz-Lenker einen »gläsernen Verkehrsteilnehmer«, wenn nicht grundsätzliche Datenschutzbedenken ausgeräumt werden. Denn die faszinierende Technik hat mehrere Haken. »Es ist nicht nur möglich, festzustellen, wer auf welcher Straße fährt«, warnt der Leiter der Abteilung Verkehr und Konsumentenschutz beim ÖAMTC, Dr. Karl Obermair. »Es läßt sich ein perfektes Bewegungsprofil erstellen.« Wer Informationen über einen Menschen herausfinden will, dieses Road-Pricing-System verrät sie. Jeder Meter, den ein Autofahrer zurücklegt, ist dokumentiert. Behörden, Schnüffler und viele andere, die Zugang zu den Daten haben, können feststellen, an welcher Adresse man häufig anzutreffen ist, welche Freunde man wie oft und wann besucht. Rund um die Uhr können Behörden einen Blick auf den Bürger werfen, der der staatlichen Inspektion dann nicht mehr entgeht.



## Tempokontrolle via Road-Pricing-Satellit

Die Verkehrspolizei wäre von diesem System begeistert. Vorbei die Zeit der Zivilstreifen, vorbei die Zeit, in der man bei jedem Wetter am Straßenrand mit Radarpistolen auf Verkehrssünder warten mußte. Mit Hilfe der Road-Pricing-Systeme wird nämlich nicht nur die zurückgelegte Strecke dokumentiert, man kann auch feststellen, wie schnell ein Autofahrer unterwegs war. Für die Strecke von A nach B darf er etwa - bei Einhaltung aller Verkehrsvorschriften und Geschwindigkeitsbeschränkungen - 39 Minuten benötigen. Ist er aber bereits nach 32 Minuten oder noch schneller am Ziel, so hat er das Tempo überschritten. Das Computersystem errechnet, um wieviel er zu schnell gefahren ist - 30 Minuten lang 30 Stundenkilometer über dem Limit kann teuer werden. Selbst Baustellen oder Staus können einprogrammiert werden.

Die Möglichkeiten können weitergesponnen werden. Fährt ein Autofahrer zu schnell, registriert das Rechnersystem die Geschwindigkeitsübertretung. Diese Information wird an einen anderen Computer weitergeleitet. Dieser druckt automatisch einen Erlagschein - in Österreich auch als Anonymstrafverfügung bekannt - und sendet ihn an den Fahrzeughalter. Die Daten des Fahrzeughalters erkennt das System entweder an der Chipkarte, mit der der GPS-Empfänger betrieben wird, oder anhand des Kennzeichens, das von einer Videokamera aufgenommen wird. In Frankreich etwa ist es jetzt schon üblich, daß die Polizei am Ende von mautpflichtigen Strecken das Weg-Zeit-Diagramm von Autofahrern überprüft und jene bestraft, die um einige Minuten zu früh am Ziel waren.

## Verbrecher werden überführt

Auch die Kriminalisten könnten dieses System perfekt für die Verbrechensaufklärung nutzen. Ob bei Fahrerflucht nach Unfällen, bei Banküberfällen oder bei Morden: die Aufklärungsraten würden sich mit einem Schlag drastisch erhöhen. Aber auch die Zahl jener, die als potentielle Täter gelten und zufällig zur gleichen Zeit unterwegs waren. Unschuldige würden dadurch zu Verdächtigen. Bür-

ger, die ihr ganzes Leben kein Gesetz gebrochen haben, müßten sich rechtfertigen, warum sie da oder dort unterwegs waren. Denn Kriminalisten rufen die Daten aus dem Road-Pricing-System ab und wissen, wer zu einer bestimmten Zeit auf welcher Straße unterwegs war. Im Falle des Österreichischen Bricfbombentälers, der in der burgenländischen Stadt Oberwart mit einer Sprengfalle vier Roma getötet hat, hätte nachgewiesen werden können, welches Auto sich in der Nahe des Tatorts aufgehalten hat. Auch wenn der Täter das Empfangsgerät aus dem Auto entfernt oder zerstört hätte, würde er im Kreise der Verdächtigen sein, denn er wäre dann einer von wenigen Hunderten, deren Gerät an diesem Tag nicht funktioniert hat.

Zukunftsvision? Science-fiction? Panikmache? Beim von der Deutschen Akademie der Verkehrswirtschaft organisierten Deutschen Verkehrsgerichtstag in Goslar haben sich Verkehrsexperten, Datenschützer, Juristen und Ministerialbeamte bereits im Januar 1995 mit diesem Problem befaßt. Sie kamen in ihrem Endbericht zum Ergebnis, daß »je nach System aus den Daten Fahrtrouten rekonstruiert und Bewegungsprofile erstellt werden. Auch Fahndungszwecke könnten durch einen solch umfangreichen Informationspool sehr gut bedient werden. Straftäter, die mit einem Auto flüchten, könnten etwa mit Videoüberwachung einer verbesserten Strafverfolgung ausgesetzt werden.« Aber auch Arbeitgeber könnten diese Systeme effektiv nutzen. Sie können ihre Mitarbeiter kontrollieren, indem sie Fahrtzeiten, Ruhepausen oder Fahrtenabrechnungen überprüfen.

Von welcher Seite man das Thema Road-Pricing auch behandelt, es überwiegen nach derzeitigem Stand der Technik die Nachteile. Zwar fordern Datcnschützer, wie etwa der ehemalige Hessische Datenschutzbeauftragte und jetzige Verfassungsrichter Prof. Winfried Hassemer, daß »erhobene Daten so früh wie möglich anonymisiert werden müssen«. Aber diese Forderung läßt sich nicht leicht umsetzen. »Die Geräte können mehr, als wir brauchen, haben mehr Funktionen, als wir uns vorstellen können«, erklärt der Wiener Verkehrsplancr Ortfried Friedreich. »In irgendeinem Chip oder Zwischenspeicher bleiben Informationen erhalten, ohne daß wir es wissen.« So wie viele Besitzer von Videorecordern, Kameras und TV-Geräten die Möglichkeiten ihrer Geräte nicht kennen und deshalb nicht ausnützen, ist es bei den diversen Road-Pricing-Computern. Absolute Anonymität ist daher unmöglich.



Prof. Hassemer hat beim schon erwähnten Deutschen Verkehrsgerichtstag einen 10 Punkte umfassenden Forderungskatalog präsentiert _ für den Fall, daß Road-Pricing kommen sollte. Seine Forderungen reichen vom Verbot, personenbezogene Daten zu erheben, über eine Mißbrauchskontrolle von Videoaufzeichnungen bis zur Verwendung von Verschlüsselungstcchniken, damit Unbefugte gespeicherte Daten nicht verwerten können.

Das Hauptproblem ist aber die Kontrolle, ob bei Fchlbuchungen oder Manipulationen. Das hat auch der Feldversuch »Autobahntechnologien A 555« gezeigt. Zehn Road-Pricing-Systeme bekannter Hersteller - unter anderem jene von Siemens, Mannesmann, Alcatel und ßosch - wurden von Mai 1994 bis Mai 1995 auf der A 555 zwischen Bonn-Nord und der Abfahrt Wesseling getestet. Das beste System hatte eine Zuverlässigkeitsrate von 99,9 Prozent. Die Fehlerquote beträgt 1:10000. Bei 150000 Autos, die sich täglich über Österreichs meistbefahrene Straße - die Wiener Südost-Tangentc - wälzen, käme es täglich zu 15 Fehlbuchungen, über ein ganzes Jahr gesehen zu mehr als 5000. Von den 165000 Autofahrern, die täglich die Strecke Frankfurt-Westhofen bis Frankfurt-Niederrad zurücklegen, müßten pro Tag 30 Einspruch gegen ihre Abbuchung einlegen. Für Kontroll- und Einspruchszwecke müßten deshalb die Daten gespeichert werden.

»Was passiert eigentlich, wenn ein Firmenchef nachprüfen möchte, warum die Firmen-Smart-Card schon wieder leer ist?« fragt ÖAMTC-Verkehrsexperte Karl Obermair. Angenommen, Mitarbeiter nullen diese Chipkarte auch für Privatfahrten. »Dann muß es die Möglichkeit geben, die Daten zu hinterfragen.« Auch ein Finanzamt hat vielleicht Interesse daran zu wissen, wie viele berufliche und private Fahrten auf einer Smart-Card gespeichert sind, wenn der Firmeneigentümer sie von der Sleuer absetzen möchte.

## Lkw-Road-Pricing ist erst der Anfang

Mit dem Lkw-Road-Pricing macht man sowohl in Deutschland als auch in Österreich den Anfang. Aber das ist zugleich der Startschuß dafür, auch die Pkw in dieses System einzubauen. »Wir wollen mit

einer kleinen, überschaubaren Flotte Erfahrungen sammeln«, gibt der Leiter der Abteilung Telematik und neue Verkehrstechnologien im deutschen Verkehrsministerium, Ministerialrat Wolfgang Hahn, zu. »Beim Lkw-Road-Pricing trifft es ja nicht die Privatsphäre eines Menschen, ein Individuum, sondern ein Unternehmen, und da ist das nicht so heikel.«

Lkw-Road-Pricing, das in Deutschland um die Jahrtausendwende starten soll, betrifft 500000 deutsche und etwa 300000 ausländische Lkw. Später könnte die Kontrolle vielleicht auch auf die 40 Millionen deutschen Pkw - bis zum Jahr 2003 sollen es 43 Millionen sein - ausgedehnt werden. In Österreich ist geplant, Road-Pricing 2001 einzuführen.

Auch Pkw-Fahrer werden der staatlichen Kontrolle nicht entgehen: »Koad Pricing ist integrierter Bestandteil einer perfekten Lenkung und Verteilung des Verkehrsflusses über das Netzwerk Straße. Road-Pricing-nein-danke-Aktionen der Autofahrerclubs können folglich bestenfalls als Verzögerungstaktik ernstgenommen werden. Die Nutzung begehrter Straßenzüge zu verteuern, womöglich auch noch tageszeitabhängig, ist eine ganz dicke Säule künftiger Mobilität«, schrieb Rudolf Skarics im »Standard« vom 12. September 1997.

Der Verkehr der Zukunft kann nur mit Hilfe von Telematik bewältigt werden, elektronischer Hilfsmittel, die den Verkehrsablauf beschleunigen, lenken und verdichten können. Denn bis zum Jahr 2010 wird der Verkehr - wenn alle Prognosen stimmen - weiter stark zunehmen. Die Zahl der Autos wird um 25 Prozent steigen. Damit aber diese telematischen Systeme finanziert werden können, bedarf es einer großen Einnahmequelle. Wie sonst sollten die High-Tech-Anlagen finanziert werden? In Tokio beispielsweise werden 900 Kreuzungen überwacht, 200 TV-Kameras und 14000 Sensoren im Straßennetz liefern ständig Daten über Verkchrsfluß und durchschnittliche Geschwindigkeit in 3500 Abschnitten. 1 1 9 Großrechner verarbeiten diese Informationen und leiten sie an die Autofahrer weiter. Entweder ins Display des Autoradios, ins Mobiltelefon oder in ein Navigationsgerät, das den Weg durch den Stau zeigt. Derartig aufwendige Systeme müssen finanziert werden. Durch Road-Pricing.



## Flotte unter Kontrolle

Systeme, die ähnlich wie Satelliten-Road-Pricing funktionieren, bieten heute schon Konzerne wie Alcatel, Bosch, Kapsch oder Mannesmann Autocom an. Alcatel etwa war sehr stolz, als man 1996 einer Zukunftsvision zur Marktreife verhelfen hat: dem »Fuhrpark-Managemcnt«. Das System stellt den Standort von Fahrzeugen binnen Sekunden fest und macht dies auf einer digitalen Landkarte in der Zentrale sichtbar. Dort weiß man immer, wo sich ein Lkw, und folglich auch der Fahrer, befindet. Denn beim »Flotten-Management« wird die Posititon durch GPS ermittelt und mit Hilfe eines GSM-Netzes an die Zentrale weitergesendet.

Die Funktionsweise ist äußerst einfach. Will der Firmenchef oder der Koordinator in der Zentrale wissen, wo sich ein bestimmter Lkw zu einer bestimmten Zeit aufhält, wird die GSM-Nummer im Fahrzeug angerufen. Das mit einer GPS-Einheit gekoppelte Handy fragt die aktuellen Positionsdaten automatisch ab und sendet diese an die Zentrale, wo der Lkw als blinkendes Kästchen mit Code und Fahrername auf einer Landkarte dargestellt wird. Ohne Wissen des Fahrers kann der Chef seinen Mitarbeiter auf Schritt und Tritt verfolgen. Ihn überprüfen, ob er zu schnell oder zu langsam unterwegs ist, welche Routen er genommen hat, ob er zu lange auf dem Autobahnparkplatz steht oder schon wieder zu lange in einer Raststation sitzt.

Auch die »Passo Fleet« von Mannesmann Autocom arbeitet nach diesem Prinzip. Man kann nicht nur ein bestimmtes Fahrzeug orten, man kann die Position einer ganzen Fahrzeuggruppe in einem speziell definierten Gebiet bestimmen. Die Ortungsabfrage läßt sich in bestimmten Zeitintervallen wiederholen. Das »Flotten-Management« läßt sich auch dazu benützen, bestimmte Informationen wie etwa Lagerstand oder Lieferzeiten ins Lkw-Mobiltelefon zu übertragen. Und nicht zu vergessen: Auch bei Lkw-Diebstählen und Notfällen kann man durch »Passo-Fleet«, »Fuhrpark-Management« und ähnliche Systeme schneller agieren, da man rascher vor Ort ist. Lkw-Fahrer müssen sich aber immer bewußt sein, daß nicht nur der Lkw kontrolliert werden kann - big boss is watching you.

## Autodieben auf der Spur

Der österreichische ÖAMTC bietet ab Ende 1998 seinen Mitgliedern die sogenannte T-Box an, der deutsche Autofahrerclub ADAC wird die T-Box frühestens 1999 einführen. Die T-Box (Telematik) ist ein Gerät, das sowohl einen GPS-Empfänger als auch einen GSM-Sender enthält. Sie hat verschiedene Funktionen: Zum einen ist sie ein Crashsender. Bei einem Aufprall des Fahrzeugs werden automatisch sowohl Fahrzeugposition als auch -daten über GSM-Netz an die Einsatzzcntrale weitergeleitet. Gleichzeitig wird eine Gesprächsverbindung zwischen Unfallfahrzeug und Einsatzleiter aufgebaut. Meldet sich der Fahrer nicht, so wird ein Notarzlwagen oder ein Rettungshubschrauber zum Unglücksort geschickt. Bei einer Panne muß der Fahrer nur auf einen Knopfdrücken, Standort, Mitgliedsnummer und Autodaten werden der Zentrale übermittelt. Dort weiß man auf Meter genau, wo das Fahrzeug geparkt ist bzw. wohin der Pannenfahrer geschickt werden muß.

Auch im Kampf gegen Autodiebe wird die T-Box eingesetzt. Sender und Empfänger - ein etwa 5 Zentimeter großer Kunststoffknopf - sind im Fahrzeug versteckt. Sie senden auch dann, wenn die Batterie abgeklemmt wurde. Wird das Auto gestohlen, identifiziert sich der Besitzer mit einer PIN-Zahl bei der Zentrale, dort wird das GSM-Telefon in der T-Box angewählt und verrät die genaue Position. Der Einsatzleiter kann den Wagen auf einer elektronischen Landkarte bei einer Fluchtfahrt von Deutschland oder Österreich z. ß. von Hamburg nach Warschau oder Graz nach Bratislava verfolgen.

Andere Systeme arbeiten nach einem ähnlichen Prinzip. Der Unterschied liegt darin, daß sofort beim Diebstahl ein stummer Alarm ausgelöst wird, der in einer Zentrale einlangt. Das Auto wird dann auf einer digitalen Straßenkarte verfolgt.

Was im Kampf gegen internationale Autoschieberbanden ein hervorragendes Instrument ist, kann theoretisch aber auch kommerziell eingesetzt werden. Wie beim Road-Pricing könnten auch mit Hilfe der T-ßox Bewegungsprofile erstellt werden. Road-Pricing durch Satelliten ist noch Zukunftsmusik, weil politisch noch nicht die Voraussetzungen geschaffen worden sind - T-Boxen sind bereits Realität.



Die Exekutive kann in ihrem Kampf gegen die Organisierte Kriminalität (OK) jederzeit - Voraussetzung dafür ist freilich ein richterlicher Befehl - von den Autofahrerclubs die Herausgabe von Mitgliedsdaten fordern. Im Zuge der Rasterfahndung kann die Exekutive diese automatisierten Daten erhalten.

Den Versuch - ohne richterlichen Befehl, versteht sich - hat es bereits in der Vergangenheit mehrmals gegeben, denn die Daten von Autobesitzern sind in mehrfacher Hinsicht interessant. So gab es bei ADAC und ÖAMTC Anfragen seitens der Finanz, alle Schutzbriefbesitzer bekanntzugeben. Man wolle feststellen, wer sich durch eine Panne im Ausland Ersatzteile gekauft und diese nicht ordnungsgemäß verzollt hat. Anhand der verbrauchten Gutscheine im Schutzbrief hätte das «Zollvergehen« nachgewiesen werden können. Die Autofahrerclubs haben sich erfolgreich gegen diesen Anschlag auf den Datenschutz gewehrt.

## Die Zentrale weiß, wo Sie sind

»1997-das Online-|ahr für Autofahrer« titelte der ADAC in seinem Sonderdruck aus der »ADAC motorweit« (Nr. 4/97). Tatsächlich wurden 1997 auf dem Sektor Navigation und Verkehrsinformation jene Systeme marktreif, die uns in den kommenden Jahren das Leben auf der Straße erleichtern - oder auch erschweren können. Abgesehen von den neuen Autoradios, die mit »Traffic Message Channel TMC« ausgerüstet sind (ein Knopfdruck genügt, und die aktuellen Verkehrsinformationen erscheinen im Display des Radios). In Deutschland haben die beiden Mobilfunk-Netzbetreiber D1 und D2 mit ihren Partnern Tcgaron und Mannesmann Autocom Telematik ein System in Form von individuell abrufbaren Verkehrsinformationen realisiert.

Wer beispielsweise ein DI -Handy besitzt, wählt vor Fahrtantritt die Nummer 2211 im DI-Netz und tippt die Himmelsrichtung des Zieles mit der Tastatur ein. Die Tegaron-Zentrale erkennt sofort, wo sich der Handy-Teilnehmer befindet. In der Zentrale werden alle notwendigen Verkehrsinformationen zusammengestellt und per Sprachcomputer durchgegeben. Eine Stunde lang werden Aktuali-

sierungen übermittelt. Wer diese Fahrtroutenhilfe in Anspruch nimmt, sollte wissen, daß diese Daten auch im nachhinein abrufbar sind. In der Zentrale werden sämtliche Daten aus Kontrollgründen gespeichert - Position, Fahrtroute, übermittelte Nachrichten. Ähnlich funktioniert auch »Passo« von Mannesmann Autocom.
Seit Ende 1997 gibt es für Opel-Neuwagenkäufer »OnStar« zu kaufen. Das Gerät, das etwa 1 500 Mark kostet, beinhaltet ein Mobiltelefon mit Freisprecheinrichtung und CPS-Empfänger. Ein Knopfdruck verbindet den Fahrer mit einer - privaten - Service-Zentrale. Das CSM-Telefon übermittelt automatisch die Daten an die Zentrale, die den Fahrer online zu seinem Wunschziel leitet. Persönliche Daten in der Hand von privaten Organisationen. Immer mehr Firmen versuchen, Verkehrsinformationssysteme an den Mann zu bringen. Datenschützer sind sich dieser Problematik bewußt, im deutschen Verkehrsministerium hat man deshalb tunlichst verhindert, daß der Staat auch für die »detaillierte Tclematik«, wie es der Leiter der Telematik-Abteilung im Verkehrsministerium, Ministerialrat Wolfgang Hahn, nennt, zuständig ist: »Das ist ein sensibler Bereich zwischen Kunde und Dienstleister. Wir wollen uns hier raushalten.« Im Nachsatz: »Wer die Vorteile genießen möchte, muß die Nachteile in Kauf nehmen.« Die Vorteile sind, in einer Zeit, in der die Verkehrsnachrichten länger dauern als die Weltnachrichten, relativ staufrei von A nach B zu gelangen. Die Nachteile sind Fahrtrouten, die in privaten Rechnern lagern und auf die bei Bedarf zugegriffen werden kann.

## *Verkehrs-TV*

Sie sind auf Geschwindigkeiten programmiert. Ist das Tempo zu niedrig, schalten sie sich ein und lösen eine Stauwarnung aus. Ist es zu hoch, schalten sie sich ebenfalls ein und bannen den Schnellfahrer auf Video. Die Kameras, die die Einfahrten zu deutschen und österreichischen Großstädten überwachen, haben vieles drauf. Sie filmen nicht nur Kolonnen - obwohl sie offiziell nur zu diesem Zweck errichtet wurden -, sie werden auch bei der Verfolgung von Temposündern eingesetzt.



Das Kamerasystem funktioniert automatisch. Vor vielen »Videospots« sind zwei Induktionsschleifen in den Straßenbelag eingebaut. Diese Induktionsschleifen liefern zum einen Informationen, um welches Fahrzeug es sich handelt (der Spurabstand verrät, ob ein Pkw, Lkw oder ein Motorrad auf der Fahrbahn fährt; es kann theoretisch sogar genau der Fahrzeugtyp festgestellt werden, da der Spurabstand zwischen einem Golf, Opel Corsa oder 3er BMW verschieden ist). Die Induktionsschleifen können zum anderen aber auch die Geschwindigkeit messen und einen Aufnahmemechanismus auslösen. »Auf den Bildern lassen sich ganz klar die Kennzeichen erkennen«, erklärt der Verkehrsplaner Orlfried Friedreich. »In England sind derartige Systeme schon im Einsatz. Auch in Deutschland wird an manchen Orten schon versucht, mit Kameras Tempomessungen durchzuführen.«
Das Geschehen auf den Straßen wird von den Polizeibeamten in den Verkehrsleitzentralen verfolgt. Verkehrs-TV auf bis zu 20 Monitoren. Bei Unfällen, Staus, Geisterfahrern oder anderen »besonderen Vorkommnissen« können sie Alarm auslösen. Sie können aber auch Kollegen informieren und ihnen »heiße Tips« geben, wenn Autofahrer zu schnell unterwegs sind, oder dem Vordermann zu knapp auffahren.
Die Videokameras sind High-Tech, wie sie sich Hobby-Filmer nur erträumen können. In Straßentunnels meistens schwarz-weiß, nehmen sie bei den Tunnelportalen auch in Farbe auf. Sie sind schwenkbar und sogar mit Zoom ausgerüstet, damit die Polizei Fahrer im Bedarfsfall besser im Bild hat. Offiziell freilich nur, damit man bei Tankwagenunfällen die Gefahrengutzeichen besser lesen, bzw. bei Unfällen den Einsatz der Hilfsmannschaften effektiver koordinieren kann.
An die Staukameras auf den Autobahnen haben wir uns schon gewöhnt. Daß Polizisten damit ständig ein Auge auf uns werfen können, ist uns kaum bewußt. Mittels Videoaufzeichnungen können verschiedenste Verstöße gegen die Straßenverkehrsordnung verfolgt, dokumentiert und sogar bewiesen werden.
Abgesehen von der Geschwindigkeitsübertretung: Wer im Auto trotz Handy-Verbots telefoniert, ist überführt. Wer auf das Spursignal vergißt, eine Sperrlinie überfährt oder sich bei einem Stau auf dem Pannenstreifen vordrängt, kann bestraft werden.

Das Verkehrs-TV ist aber auch Unterhaltung. Nicht für die Autofahrer, sondern für die Überwacher. Nasenbohrende Pkw-Lenker verstoßen zwar nicht gegen Gesetze, lösen dafür aber in der Verkchrsleitzentrale Gelächter aus; küssende Paare vielleicht neidische und streitende hämische Kommentare. Wer mit seinem Auto unterwegs ist, sollte sich darüber im klaren sein, daß es auch im Wageninneren keine Privatsphäre gibt. Vorausgesetzt, es handelt sich nicht um eine Limousine mit verdunkelten Scheiben.

Die Polizei hat größtes Interesse an diesen Video-Aufzeichnungen. Die Mautstraße auf den höchsten Berg Österreichs, den Großglockner, wird von Videokameras überwacht. Die Betreiberfirma nimmt bei der Mautstation die Kennzeichen auf, um zu kontrollieren, ob eine Mautkarte nur von einem Pkw verwendet wird. Einige Male schon wollte die Gendarmerie im Zuge der Fahndung nach Autolenkern dieses Videomaterial sichten.

Neugierig war die Exekutive auch im Juni 1995. Damals stellte die ÜAMTC-Akademie ihre Studie »Der Steinzeiljäger im Straßenkreuzer« vor. Der Forschungsbericht hatte das aggressive Auffahren auf Autobahnen zum Inhalt. »Auffahrer« wurden auf Videos aufgezeichnet, aus Datenschutzgründen wurden die Kennzeichen unkenntlich gemacht. Ein Bericht dieser Studie samt Videobeispielen von Auffahrern wurde auch in der Nachrichtensendung »ZIB 2« im ORF gesendet. Bereits am Tag darauf läutete bei der ÖAMTC-Akademie das Telefon. In der Leitung war ein ranghöher Polizeibeamter, der die Herausgabe der Originalaufnahmen forderte. Sein Argument: Man möchte die Autofahrer bestrafen, benötigt dafür aber die Kennzeichen. Er erhielt die Daten übrigens nicht - aus Datenschutzgründen.

# Kartenmacher sammeln gern

> Wie wir mit Bankomat- und Eurocheque-Karten überwacht werden,

> Welche Spur wir mit Euro-Card, Kredit- und Kundenkarten hinterlassen.

> Warum Sie im Krankenstand nicht mit der Bankomatkarte Geld abheben sollten.

> Warum Kreditkarten so leicht zu fälschen sind und Betrug jeden treffen kann.

> Wie der Bankomat-Code erraten wird.

> Wie der Kantinen-Ausweis zum Kündigungsgrund werden kann.

> Welche Gefahren der Chip-Krankenschein in sich birgt

## Die Kontrollore der Plastikkarten

Der Bankomat-Großrechner steht im Hochsicherheitstrakt, die »Security-Box«, die zur Absicherung jede Geldbehebung mitspeichert, ist mit einem dicken Stahlseil im Boden verankert - eine Vorschrift des US-State-Departments, denn derartige Rechner »made in USA« dürfen nicht in jedes Land exportiert werden.

Nur mit Ausweis und Geheimcode erhält man Zutritt in die »heil'gen Hallen« der Gesellschaft für Zahlungssysteme (GZS) in Frankfurt bzw. der Europay Austria in Wien. Der Tandem-Großrechner, eine 12-Prozessor-Anlage mit dem Namen »Himalaya K.Series«, registriert alle Zahlungsvorgänge, die entweder mit Eurocheque-Karten oder MasterCards getätigt werden.

Wenn ein deutscher Tourist in St. Anton am Arlberg bei der dorti-

gen Shell-Tankstelle mit seiner EC-Card bezahlt, weiß das binnen weniger Sekunden Europay Austria und auch die GZS. Wenn ein österreichischer Urlauber bei einem Bankomat in Berlin abhebt, kann von der Zentrale aus in Wien der gesamte Abbuchungsvorgang mitverfolgt werden.

Ende 1998 werden auch die Abhebungen mit einer Eurocheque-Karte auf der ganzen Welt verfolgt werden können. Eine Kooperation zwischen Europay und MasterCard macht's möglich. Am 13. Januar 1998 verkündete der deutsche Bankenverband, daß zu den 900000 europäischen elektronischen EC-Kassen in Geschäften, Warenhäusern und Restaurants noch einmal 900000 Kassen auf anderen Kontinenten hinzukommen. Das wiederum bedeutet, daß künftig auch Nicht-Kreditkartenbesitzer weltweit ort- und verfolgbar sind.

Wer einen österreichischen EC-Karten- bzw. MasterCard-Besitzer überwachen möchte, tut sich in Österreich leicht: Alle Informationen laufen bei der Europay Austria zusammen und werden erst später an das jeweilige Bankinstitut des Kontoinhabers weitergeleitet. In Deutschland landen die Kundendaten in der jeweiligen Zentrale der Hausbank, die Informationen laufen lediglich über eine gemeinsame Schnittstelle bei der GZS, wo die Daten zwischengespeichert werden.

Jede Transaktion, die in Europa mit einer EC-Card gemacht wird, wird in der europäischen Europay-Zentrale in Brüssel gespeichert. Eine Mega-Datenbank, in der jede Transaktion, von Portugal bis Griechenland, dokumentiert ist.

Auch jede Bankomat- bzw. Kreditkartentransaktion, von einem Kontinent nach Europa oder umgekehrt, läuft über Brüssel. Von Wien aus gibt es zwei Standleitungen. Die eine Wien-Zürich-Brüssel, die andere Wien-Frankfurt-Brüssel.

Die Informationen in den Europay- und GZS-Rechnern sind »heiß«. Wird eine Kontonummer in den Computer getippt, erscheint der Kontoauszug der EC-Karte - sämtliche Abhebungen und Abbuchungen, die mit der EC-Karte in den vergangenen zwei Monaten gemacht wurden - aufgelistet nach Betrag, Zeit und Ort. Selbst die Adresse des Geschäftes oder der Tankstelle, wo mit der Bankomatkarte bezahlt wurde. Der Lokalaugenschein beweist es, denn die Aussage: »An diesen Betrag kann ich mich nicht erinnern« wird



nach zwei Tastenklicks mit einem kühlen Lächeln beantwortet: »Vergangenen Montag haben Sie im Virgin-Megastore auf der Mariahilfer Straße eingekauft«, meint die Dame hinter dem PC. Im Nachsatz: »Entsprechend dem Betrag waren das vermutlich CDs.«

Die Bezeichnung »gläserner Plastikkarten-Kunde« hören die Mitarbeiter von Europay Austria und GZS nicht gern. »Uns sind keine Kundennamen bekannt«, betont Europay-Geschäftsführer Ewald Judt. »Wir haben nur Kontonummern.« Den Namen dazu haben, so die offizielle Argumentation, nur die Banken. Nur diese könnten Nummer, Namen und Informationen zusammenführen.

Offiziell wird eine Verknüpfung freilich nie gemacht. Eine Verknüpfung, die ein Weg-Zeit-Diagramm wie aus dem Bilderbuch ergibt. Inoffiziell leider schon, wie das Beispiel einer Großbank in Österreich zeigt: Der Bankangestellte Josef Weiß (Name geändert) befand sich im November 1997 wegen einer Grippe im Krankenstand. Nach seiner Genesung wurde er zum Bankdirektor zitiert. Dieser kündigte dem Angestellten an, daß der Krankenstand in einen Urlaub umgewandelt werden müsse. Begründung: Während seines Krankenstandes habe er dreimal den Bankomaten aufgesucht, was bedeutet, daß er nicht krank gewesen sein könne. Die Erklärung, daß die Freundin mit der Karte abgehoben habe, ließ der Direktor nicht gelten.

61 Millionen Deutsche und 3,1 Millionen Österreicher haben eine EC-Karte. Wer mit seiner Bankomat-Card zahlt, hinterläßt eine Spur. »Die so gewonnenen Daten könnten in der Zentrale des Systems ohne großen Aufwand zu einem Benutzerprofil zusammengestellt werden, welches Aussagen über das Konsumverhalten des Kartenbesitzers ermöglicht«, schreiben Michael Nentwich, Walter Peissl und Paul Pisjak in ihrem Buch »Konsumentenkarten«. Was die Autoren 1993 als Möglichkeit angesehen haben, ist heute bereits Realität, man könnte es sogar als »Standard-Methode« bezeichnen. Die Bankomat-Rechnung zeigt genau, wann und wo jemand Geld abhebt, wann und wo jemand tankt, also auch in welchen Gebieten Deutschlands oder Österreichs jemand mit seinem Auto gefahren ist. Die Rechnung dokumentiert aber auch, wann und wo jemand welche Produkte eingekauft hat.

Noch detailliertere Rückschlüsse laßt die Kreditkartenabrechnung zu.

Auch Banken kontrollieren die Kreditkartenabbuchungen ihrer Kunden. Männer, die in Bordellen mit Kreditkarte bezahlen, sollten sich bewußt sein, daß diese Abrechnungen gegen sie verwendet werden können. Banken wissen genau, was sich hinter gewissen Firmenbezeichnungen und Gesellschaften mit beschränkter Haftung befindet. »Wer bei uns um einen Kredit ansucht, dessen Kontobewegungen werden auf solche Abrechnungen kontrolliert«, bestätigt ein Bankbeamter.

Was man daraus ableiten kann? Die Moral des Kunden. Ist ein Mann »Stammgast« bei Prostituierten, so könnte die Rückzahlung eines Kredits darunter leiden ... Diese Methoden haben einige Bordell-Betreiber, die daneben auch »seriöse« Betriebe wie Bars oder »normale« Nachtclubs führen, veranlagt, all ihre Betriebe bei der Kreditkartengesellschaft unter einem Namen und einer Adresse bekanntzugeben. Damit können Banken nämlich nicht mehr ableiten, ob der Kunde XY in der Bar oder im Bordell Gast war.

Von den 630000 MasterCards in Österreich wurden 120000 von den Banken ausgegeben. Das bedeutet wiederum, daß die Geldinstitute zugleich auch die Abrechnungen verwalten und daher Einblick in das Kundenprofil haben. Bei den übrigen Kreditkarten erhalten die Banken üblicherweise nur die Monatsrechnungen, auf Anfrage bei Visa & Co werden ihnen aber jederzeit Detailinformationen zur Verfügung gestellt.

## Karten-Fährte

Kriminalisten nutzen die Möglichkeit, Bürger mittels EC-Karte bzw. Kreditkarte zu orten, schon seit Jahren. Europaweit gibt es 900000 Bankomatschalter, weltweit sind es 1,8 Millionen. Und von jedem ist die Adresse bekannt. Bei MasterCard gibt es, über die ganze Erde verstreut, 14,5 Millionen Schalter, von diesen sind bereits zwei Drittel online- bei jeder Transaktion »schaut die Zentrale zu«. Wer mit seiner Visa- oder MasterCard an einer dieser Online-Kassen zahlt, kann praktisch von Deutschland oder Österreich verfolgt werden. Im selben Moment, in dem der Kreditkartenautomat etwa in einer Boutique in der 5th Avenue in New York grünes



Licht gibt, weiß man auch in der Zentrale, daß sich der deutsche Kreditkartenkunde mit der Nummer XY in der 5th Avenue in New York aufhält. Zum einen kann die laufende Transaktion gestoppt, zum anderen auch die lokale Polizei verständigt werden.

Die deutsche Gesellschaft für Zahlungssysteme (GZS) wird einige Male pro Monat von Kriminalisten besucht, die die Fährte von Kriminellen und Flüchtigen aufnehmen wollen, bestätigt eine GZS-Sprecherin. Eine genaue Anzahl möchte sie aus »verständlichen Gründen« nicht nennen.

In Österreich, so schwört man bei Europay Austria, komme dies »nur sehr, sehr selten« vor. Die Beteuerungen haben allerdings einen kleinen Haken. Denn auch in Österreich wird das Bankomat- und Kreditkarten-Verhalten gesuchter Kunden von Kriminalisten und Wirtschaftspolizisten mehrmals pro Monat kontrolliert. In Österreich läuft es aber über die Bankenschiene. Nicht die Kriminalisten fordern die Herausgabe der Daten bei Europay Austria, sondern die jeweilige Bank, bei der der Gesuchte sein Konto besitzt.

Es ist sogar machbar, sollte ein Gesuchter mit seiner Bankomat- oder Kreditkarte bezahlen, daß sofort Alarm ausgelöst wird. Als der Frankfurter Bauunternehmer Jürgen Schneider im April 1994 flüchtete, wurden seine Kreditkartenkonten überwacht. Auch die Spur des österreichischen Unternehmers Wilhelm Papst, der bei der Sanierung des Kärntner Zellstoffwerks Sankt Magdalen Hunderte Millionen Schilling unterschlagen hatte, wurde nach seiner Flucht nach Südamerika anhand einer Kreditkarten-Abrechnung aufgenommen.

## Die Kundenkarte

Sie sind praktisch, haben ein faszinierendes Format, sind meistens bunt, poppig und ... je mehr man davon in der Brieftasche hatte, desto stolzer war der Besitzer bis vor kurzem. Doch die Zahl der Plastikkarten ist unüberschaubar geworden. In Deutschland und Osterreich sind Hunderte Millionen Plastikkarten verbreitet - ob Autofahrerclub, Sportgeschäft, Supermarktkette oder Airline-Vielfliegerprogramm. Hunderte Unternehmen in Deutschland und Österreich haben ihre eigenen Plastikkarten, mit denen sie ihre

Kunden an sich zu binden versuchen. Für 3 Prozent Rabatt, Sonderpreise bei bestimmten Produkten oder eine um Wochen spätere Abbuchung des Kaufpreises vom Konto verkaufen Kunden ihre Identität, ihre Privatsphäre. Denn Kundenkarten verraten mehr über den Käufer, als vielen lieb ist.

Den meisten ist es vermutlich egal, wenn das Sportgeschäft weiß, daß man häufig Squash- oder Tennisgegenstände kauft und deshalb Werbematerial über Ballsportarten zugeschickt bekommt. Den meisten dürfte es auch gleichgültig sein, daß sie die Fotohandelskette anschreibt, wenn für die jüngst gekaufte Kamera ein neues Objektiv auf den Markt gebracht wurde. Den meisten ist vermutlich aber nicht bewußt, daß der Einkauf Rückschlüsse auf ihre Privatsphäre zuläßt. Mit den Daten lassen sich nicht nur Kundenprofile erstellen (wie im Kapitel »Rasterfahndung« beschrieben wird), sondern auch exakte auf den namentlich bekannten Kunden zugeschnittene Einkaufszettel.

Wer eine Supermarkt-Kundenkarte besitzt, der läßt sich mit Leichtigkeit charakterisieren, bewerten und sogar katalogisieren. Marketing-Strategen entwickeln Bilder von Kunden, die mit der Realität gar nichts zu tun haben müssen. Kunde Maier kauft zwei Kisten Bier pro Woche - also dürfte er Alkoholiker sein. Er greift ständig zu Schweinefleisch, fettem Käse und selten zu Obst oder Gemüse - also ernährt er sich ungesund und hat vermutlich erhöhte Cholesterinwerte. Zudem dürfte Herr Maier an Schweißfüßen und Schuppen leiden sowie dritte Zähne haben - in regelmäßigen Abständen kauft er Fußpudcr, Anti-Schuppen-Shampoo und Haftcreme. Frau Maier dürfte für die Süßigkeiten verantwortlich sein, die bei jedem Einkauf im Wagen landen, außerdem ist die Wahrscheinlichkeit hoch, daß sie bald ein Kind erwartet, da sie seit vier Monaten keine Damenbinden mehr kauft.

Herrn Hubers Einkaufszettel hingegen verrät, daß er Single sein dürfte, ein sportlich und auch sexuell aktiver Kunde. Er ernährt sich bewußt, ißt Fisch, Gemüse und Obst und kauft in relativ kurzen Zeitabständen Großpackungen Kondome.

Herr Bauer wiederum ist einer der typischen »Sonderangebots«-Kunden, die ihr Geld zweimal ansehen, bevor sie es ausgeben. Er greift nur zur Aktionsware. Nur einmal im Jahr, vermutlich vor seinem Geburtstag, kauft er sich Champagner und Kaviar.



Exakt diese Informationen lassen sich anhand der Kundenkarten ableiten. 1998 beginnt die Merkur-Warenhandels-AG eine Kooperation mit der Wiener Wirtschaftsuniversität. Ziel ist eine solche Warenkorbanalyse, bei der das Verhalten von namentlich bekannten Kunden erhoben wird.

Was vielen Bürgern außerdem nicht bewußt ist, ist die Tatsache, daß im Zuge der polizeilichen Rasterfahndung auch solche Daten verknüpft werden können. Denn mit einem Beschluß eines Dreier-Richter-Kollegiums darf die Polizei auch auf private Daten zugreifen. Plötzlich weiß auch Polizist Schmidt, daß Herr Maier Schweißfüße hat und Frau Maier ein Baby erwartet. Offizielle Stellen erhalten plötzlich Einblick in intime Details, die man freiwillig nie verraten würde.

Das Einkaufsverhalten bzw. dieses Kundenprofil wäre aber auch für Firmenchefs von Interesse, wenn es darum geht, neue Mitarbeiter einzustellen. Mit Informationen über das Gesundheitsbewußtsein und spezielle Ernährungsgewohnheiten lassen sich Vorhersagen treffen, ob beim Mitarbeiter XY in späteren Jahren gesundheitliche Probleme auftreten und der Firma durch Krankenstände künftig Kosten erwachsen könnten.

## Unknackbarer Code?

Die einen - die Computer-Hacker - schwören, ihn »knacken« zu können, die anderen - Vertreter deutscher und österreichischer Banken - halten ihn für »unknackbar«. In regelmäßigen Abständen wird der Sicherheitscode der Bankomat-Karten als unsicher beurteilt. Bereits im Oktober 1995 wurde in der ARD-Sendung »Ratgeber Technik« auf die Problematik von Kartenfälschungen und unsicheren Bankomat-Codes hingewiesen. Zwei Jahre später, im November 1997, präsentierte ein Vertreter des Chaos-Computer-Clubs (CCC) im Rahmen der ZDF-Sendung »Wiso« ein mathematisches Annäherungsprogramm, das die Wahrscheinlichkeit eines vierstelligen Bankomat-Codes berechnet.

Die PIN (Personal Identification Number), wieder Bankomat-Code auch genannt wird, wird aus der Kontonummer, der Bankleitzahl,

der Kartenfolgenummer etc. errechnet. Die Chaos-Computer-Club-Hacker hatten versucht, über die Bankleitzahl bzw. die Kontonummer des Karteninhabers auf unterschiedliche Häufigkeit einiger Zahlenkombinationen zu schließen. Der Hacker hatte zuerst mit einem Kartenlesegerät Daten wie Kontonummer etc. aus dem Magnetstreifen der Karte gelesen und dann mit einem Computerprogramm die Zahl der möglichen 9999 Codes auf 150 reduziert. Einen Beweis ist der Hacker allerdings schuldig geblieben: ob unter diesen 150 Zahlenkombinationen tatsächlich die richtige dabei war...

»Den Code zu knacken ist unmöglich«, meinen Banken-Vertreter. Allen Versprechen zum Trotz läßt sich der Bankomat-Code aber trotzdem knacken. Zu diesem Urteil kam zumindest das Oberlandesgericht Hamm am 17. März 1997 (Az 31 U 72/96). Zum einen könnten kriminelle Organisationen über den Schlüssel zur Ermittlung der Geheimzahl verfügen, zum anderen könne die Geheimzahl »erraten« werden. Ein routinierter Täter, ausgestattet mit Laptop und Kartenlesegerät, könnte den Code in etwa 150 Versuchen knacken, da sich in Deutschland eine PIN meist aus den Ziffern 1 bis 5 zusammensetzt. Das automatische Einziehen der Karte nach drei Fehlversuchen kann mit einem frei im Handel erhältlichen Kartenlesegerät-100 Mark bzw. 700 Schilling-gestoppt werden.

Obwohl die Banken immer felsenfest behaupten, der Code sei unknackbar, gibt es in Deutschland ab 1999 neue PIN. »So werden die zu verwendenden Schlüssel von 56 auf 112 Stellen erhöht«, erklärte der stellvertretende Hauptgeschäftsführer des Bundesverbandes deutscher Banken, Wolfgang Arnold in der »Wirtschaftswoche« (Nr. 38/97). »Das bedeutet, daß sich die Anzahl der möglichen Schlüsselkombinationen potenziert. Sie erhöht sich auf 72 Billiarden mal 72 Billiarden.« - »Aber das«, so kontert der Darmstädtcr Gerichtssachverständige Prof. Manfred Pausch, »hat mit einer Verbesserung nichts zu tun. Es wird die Verschlüsselungstechnik geändert, der PIN-Code ist weiterhin leicht zu knacken.«

Manfred Westphal, Finanzexperte der Arbeitsgemeinschaft der Verbraucherverbände, ist in der »Wirtschaftswoche« ähnlicher Meinung. »Diese Maßnahme allein wird jedoch keine entscheidenden Verbesserungen für den Bankkunden bringen«, meinte Westphal. »Eventuell ist sogar schon der Pool-Schlüssel - der Generalschlüssel



aller Banken - geknackt worden, mit dem jede PIN entschlüsselt werden kann.« Als Skandal bezeichnet Westphal das Verhalten der Sparkassen, daß ein von Gerichten und Bundesbehörden als unsicher entlarvtes System dennoch auf dem Markt bleibt.

Denn die Zahl der EC-Karten-Mißbräuche nimmt zu. 1997 gab es in Deutschland beinahe 30000 Betrugsfälle, geschätzte Schadenssumme: mehr als 1 50 Millionen Mark. In diesen Betrugsfällen sind falsche Bankomaten ebenso enthalten wie das Ausspähen der' Nummer und anschließender Diebstahl. Es kommt aber auch vor, daß die Karte gestohlen wird und der Dieb - obwohl er die PIN nicht kennen kann - Tausende Mark abhebt.

Prof. Manfred Pausch ortet sowohl bei den Aufstellern als auch bei den Herstellern der Geldausgabe-Automaten Mängel. So war es bei einigen Geräten möglich, Geldscheine in ein verstecktes Fach umzuleiten. In gewissen Zeitabständen konnte der Täter dieses Fach »entleeren«. Noch täterfreundlicher sind jene Geldautomaten, deren Tastatur ein »Touchscreen« ist, bei dem der Kunde die Tastensymbole auf dem Bildschirm drücken muß. »Jeder Laie kann sich vorstellen, daß bei einer vorher gereinigten Bildschirmoberfläche eine PIN-Eingabe aufgrund der Hautfettspuren deutlich zu erkennen ist«, erklärt Prof. Pausch. Die Rangfolge der Zahlen kann sogar anhand des sogenannten »Verfettungsgefälles« erkannt werden-bei der ersten Ziffer ist der Fingerabdruck fetter, bei der letzten am »trockensten«.

Aber es kann nicht sein, was nicht sein darf. Dieses Motto gilt auch für österreichische Banken. Eine von diesen machte einem Wiener Lehrling sieben Jahre lang das Leben schwer. Während der junge Mann in der Arbeit war, wurden von seinem Konto zweimal 5000 Schilling abgehoben. Als er mit seiner Karte abheben wollte, wurde seine Karte eingezogen. Obwohl der Lehrling beweisen konnte, daß er in der Arbeit war und seine Karte immer bei sich hatte, wollte die Bank den Schaden nicht ersetzen. Beide Möglichkeiten-ein Duplikat der Karte bzw. ein Erraten der PIN - hielten die Bankmanager für unmöglich. Eine duplizierte Karte werde nach dem zweiten Versuch eingezogen. »Das Erraten der PIN ist bei uns in Österreich nicht möglich«, ist Europay-Austria-Geschäftsführer Ewald ]udt überzeugt, »da bei uns die Ziffern 0 bis 9 gleich häufig vorkommen.« In Österreich wird eine PIN erstellt, indem sechs

Personen aus unterschiedlichen Institutionen bis zu 256 Stellen lange Zahlenschlüssel eingeben, die den Code ergeben.
Eine Erklärung ist aber noch für jenen Fall ausständig, den der Leiter der Rechtsabteilung beim Verein für Konsumenteninformation, Peter Kolba, im November 1997 präsentierte. Eine Frau hatte sich zu einer Bankomatkarte überreden lassen. Da sie diese aber nur als Scheckkarte verwenden wollte, ließ sie den Code im Banksafe. 1997 wurde ihre EC-Karte gestohlen und danach auch Geld behoben. Der Code lag aber immer noch im sicheren Safe ...

## Entweder Sie klauen eine oder Sie bauen sich eine

Der Flug mit einer asiatischen Airline nach Kuala Lumpur hatte für den Chef eines internationalen Unternehmens ein Nachspiel. Vier Wochen nach seinem Urlaub in Malaysien war er plötzlich mit einer Rechnung der Eurocard (jetzt MasterCard) konfrontiert, die unmöglich seine sein konnte. Der Anruf bei der Eurocard-Zentrale brachte rasch Aufklärung, denn er war nicht der einzige Anrufer. jeder Passagier, der auf der asiatischen Fluglinie Duty-Free eingekauft und mit der Kreditkarte bezahlt hatte, war Betrügern aufgesessen. Sie hatten die Daten aus dem Duty-Free-Computer kopiert, Kartenduplikate hergestellt und damit eingekauft.
Kreditkarten sind relativ einfach zu fälschen. Das hat die ARD bereits im Oktober 1995 in ihrer Sendung »Ratgeber Technik« gezeigt. Man nimmt ein Stück Pappe, in der Größe einer Kreditkarten, schneidet ein Stück Magnetband aus einer Videokassette aus und klebt es auf den Karton. Die Daten einer echten Karte werden mit einem Magnetstreifen-Lesegerät herausgelesen, auf einem PC zwischengespeichert und auf die falsche Karte übertragen. Im Handel sind auch Blanko-Magnetstreifenkarten - für den Preis einer Briefmarke - erhältlich.
Wer schon einmal mit einer überhöhten Kreditkartenabrechung konfrontiert war, der wurde vermutlich Opfer dieser Methoden. Denn die Daten einer gültigen Kreditkarte können auf eine bereits abgelaufene überspielt werden. Auf diese Weise können Betrüger auf Kosten anderer einkaufen.



Gratis-Kreditkartennummern werden aber auch über das Internet vertrieben. Es gibt eigene Computerprogramme, die gültige, aber nicht vergebene Nummern erzeugen.
Die Kreditkartenkriminalität nimmt von Jahr zu Jahr zu. Mit exorbitanten Zuwachsraten. Die Wahrscheinlichkeit, Opfer von Betrügern zu werden, steigt. Mit österreichischen Visa-Karten kam es 1997 zu etwa 7000 mißbräuchlichen Transaktionen. Drei Viertel der Betrugsfälle passierten im Ausland, wobei die unsichersten Kreditkartenländer die USA gefolgt von Spanien, Frankreich und Ungarn sind. In Österreich selbst ereigneten sich aber immerhin auch beinahe 2000 Mißbräuche.
Die Unternehmen - ob MasterCard, Visa oder Diners Club - sind sich der Problematik bewußt, die ihre Magnetstreifenkarten mit sich bringen. Eine Systemumstellung ist für die Kreditkartenunternehmen aber mit enormen Investitionen verbunden, da nicht nur alle Magnetstreifenkarten durch die dreimal so teueren Chipkarten ersetzt, sondern auch alle Online-Kassen bei den Händlern umgerüstet werden müßten.
Visa hat bereits im Herbst 1997 den Anfang gemacht. Der deutsche Banknoten- und Kartenerzeuger Giesecke & Devrient hat die ersten Visa-Karten mit Mikroprozessor-Chips für die Hongkonger Overseas Trust Bank geliefert. Bis weltweit alle Karten mit Chips ausgerüstet werden, wird es aber noch Jahre dauern. »Vermutlich sind die Verluste noch nicht hoch genug«, meint ein Insider. »Die Sicherheit der Kreditkarten verbessern die Unternehmen erst dann, wenn die Umrüstungskosten geringer sind als die Verluste.«
Ein weiteres Problem ist auch noch, daß alle Kreditkartenunternehmen und die Bankomatbetreiber an einem Strang ziehen und sich auf ein einheitliches System festlegen müßten, das von allen genutzt werden kann. Ein kleiner Vorteil der Kreditkarten, verglichen mit den Bankomatkarten, ist die Haftungsgrenze: Während Kunden von EC-Karten bei der Bank um ihr Recht kämpfen und beweisen müssen, daß sie mit ihrer Karte sorgsam umgegangen sind, ist man bei Kredilkartenunternehmern »nur« für 150 Mark bzw. 1 000 Schilling haftbar. Aber auch hier gibt es eine Ausnahme, die PIN: Bei einem mißbräuchlichen Bargeldbezug haftet der Kreditkarteninhaber bei MasterCard bis zu 2000 Mark bzw. 15000 Schilling.

## Intelligenz auf 20 $mm^2$

Das goldene Blättchen mißt nur etwa einen Quadratzentimeter und ist hauchdünn. Aber dahinter verbergen sich 20 Quadratmillimeter High-Tech - entweder ein Speicherchip, der bis zu 1 000 Zeichen speichert, oder ein Mikroprozessor, der die 8,5 mal 5,5 Zentimeter große Plastikkarle in einen Mini-Computer verwandelt, der so leistungsstark und intelligent ist wie frühere Schreibtisch-PCs.

Bei den Chipkarten sind zwei Varianten üblich: Zum einen sogenannte Memory-Chips mit einer ganz normalen Speicherfunktion. Diese werden z. B. bei deutschen Telefonwertkarten eingesetzt und haben eine Speicherkapazität von maximal 1 KB. Zum anderen gibt es Mikroprozessor-Chips, die bei Eurocheque-Karten, SIM-Karten im GSM-Netz oder bei der »elektronischen Geldbörse« verwendet werden. Die neueste Entwicklung, ein 16-KB-Chip, wird vom deutschen Banknoten- und Kartenhersteller Giesecke & Devrient seit 1997 in die Plastikkarten eingebaut. 16 KB bedeuten, daß auf dem Chip 16000 Zeichen gespeichert werden können, das sind zwischen sechs und zehn beschriebene Buchseiten. Bei Giesecke & Devrient kommen vor allem Siemens-Chips zum Zug, aber auch die großen Konkurrenten wie Motorola, Philips oder Hitachi sind am High-Tcch-Markt mit ihren Produkten vertreten.

Bei der Speicherkapazität werden ständig neue Rekorde aufgestellt, denn auch 32-KB-Chips sind kein Problem mehr. Experten rechnen, daß in einigen Jahren Prozessorchips auf dem Markt sein werden, die ein Speichervolumen von 10000 Schreibmaschinenseiten haben und zehn Millionen Computerbefehle pro Sekunde ausführen können.

## Die Gefahr der Multifunktionskarten

Doch in dieser enormen Speicherkapazität liegt die Problematik der Zukunft. Große Speicher bedeuten, daß darauf viele Daten gespeichert werden können. »Es gibt viele Menschen, die sich bereits darüber beschweren, zu viele Karten in der Brieftasche zu haben«, meint G & D-Senior Manager Klaus Dargahi. Ausweg aus



dieser Plastikkarten-Misere: Große Speicherchips könnten einige Karten ersetzen, indem ein Chip mehrere Funktionen übernimmt.

Da es keinen Sinn ergibt, Speicherkapazität ungenutzt zu lassen, werden die Karten der Zukunft sogenannte Multifunktionskarten. Auf einem Speicher sind dann verschiedene Anwendungen unterschiedlicher Unternehmen oder Behörden vertreten. Beispiele haben Austria Card und Giesecke & Devrient bereits angeboten. Letztere Für Malaysia. Dort sind zwei Multifunktionskarten geplant. Auf einer werden Personalausweis, Gesundheitskarte und Führerschein kombiniert, die zweite wird eine Debit-Karte (eine direkt an das Konto gebundene Karte, die es wie z. B. eine Eurocheque-Karte sofort belastet) mit elektronischer Geldbörse sein.

In Österreich beispielsweise hat die Mcrkur-Warenhandels-AG für ihr Kundenprogramm »Friends of Merkur« Speicherplatz auf dem Chip der EC-Karte gebucht. Das wiederum bedeutet, daß auf dem Chip, mit dem die Österreicher an den Bankomaten Geld abheben können, auch der Zugang zum Einkaufszettel gespeichert ist.

jeder Chip kann bis zu acht verschiedene Funktionen haben, sprich: acht verschiedene Unternehmen könnten auf einer Karte vertreten sein. Damit aber nicht die Firma A auf die Daten von Unternehmen B zugreifen kann, gibt es im Inneren des goldenen Blättchens eine Sperrfunktion. »Auch wenn die Techniker versprechen, daß man nicht auf die Daten zugreifen kann, muß man entgegenhalten, daß das eine softwaremäßige Sperre ist, die ein gewiefter EDV-Experte mit Leichtigkeit aufheben kann«, sagt Soziologe Walter Peissl. »Wirklich sicher sind Informationen nur dann, wenn sie sich aufgetrennten Karten befinden.«

Den sprichwörtlichen Vogel hätte der österreichische Hauptverband der Sozialversicherungsträger abgeschossen, wenn dieses Vorhaben an die Öffentlichkeit gelangt wäre. Im Zuge der Diskussion um Einführung einer Sozialversicherungskarte für die Österreicher gab es Gespräche zwischen Hauptverband und Europay Austria. Die Idee: Man könnte Speicherplatz auf den Chips der Eurocheque-Karten buchen. Der Hintergrund: Der Hauptverband der Sozialversicherungsträger hätte sich damit eine dreistellige Millionensumme ersparen können. Denn die Miete auf einem bestehenden Chip ist mit einer Gebühr von 1,50 Schilling pro Jahr und Karte verglichen mit den Kosten einer eigenen Karte gering.

Hätten 8 Millionen Österreicher eine solche Karte, wären bei einem Durchschnittspreis von etwa 30 Schilling pro Karte 240 Millionen Schilling angefallen.

Das Problem bei dieser Kooperation wäre gewesen, daß Daten einer Behörde bzw. einer öffentlichen Einrichtung mit den Daten einer Bank auf einem Chip gespeichert worden wären. Durch ein Aufheben der Sperre - auch wenn alle beteuern, daß dies ungesetzmäßig ist - hätten diese Daten vermischt werden können.

Multifunktionelle Karten haben nur dann einen Sinn, wenn die daraufgespeicherten Daten relativ »unproblematisch« sind. Wenn es zu Kombinationen privater Unternehmen, wie etwa einem Sporthandel, einer Supermarktkette oder einem Modenhaus kommt. Problematisch werden multifunktionelle Karten dann, wenn Daten von Behörden mit Daten von privaten Gesellschaften kombiniert werden. Dieser Variante steht derzeit noch eine materielle Hürde im Weg. EC- und Kreditkarten sind aus billigem PVC, Personalausweiskarten aus hochwertigem Polykarbonat. PVC-Karten halten drei, Polykarbonatkarten zehn fahre.

Aber auch gegen eine Karte, auf der verschiedene Behörden vertreten sind, sollten sich die Bürger wehren, da eine theoretisch Zugriff auf die Daten der anderen hätte. Durch die schon besagte Speicherkapazität eines Chips wäre es möglich, daß sich auf einer Identitätskarte Gesundheitsdaten und Führerschein finden.

## *Lesegeräte für die Polizei*

Bei der Verkehrskontrolle wird der Führerschein durch ein Lesegerät geschoben, das im Funkwagen montiert ist. Sofort erscheinen die Informationen auf dem kleinen Display: Name, Adresse, Kennzeichen, wie viele Punkte der Fahrzeuglenker bereits verloren hat, freilich sind auch vergangene Verkehrsdelikte detailliert aufgelistet. Online können die Polizeibeamten notwendige Informationen vom Zentralcomputer im Innenministerium abrufen, Online kann der Autofahrer auch seine Strafe bezahlen - mit Kredit- oder EC-Karte. Eine Zukunftsvision? Die Online-Bezahlung ist bereits seit 1997 möglich, den Chip-Führerschein haben die Datenschützer und



Kritiker innerhalb der politischen Parteien noch verhindern können. Aber auf dem neuen, scheckkartengroßen EU-Führerschein, der in Deutschland bis 2010 völlig den alten Papier-Führerschein ersetzen soll, ist derzeit zwar kein Chip angebracht, der Platz dafür ist aber vorgesehen.

Die Österreicher vertrauen nach wie vor dem Papier und haben auf der Frontseite ihres rosa Scheines lediglich einige EU-Sterne angebracht. Es ist aber nur noch eine Frage der Zeit, bis auch Österreich auf das Scheckkartenformat setzt, mit dem dann in ganz Europa ein einheitlicher Standard geschaffen wird. Der Chip-Führerschein wird aber auch noch aus einem anderen Grund irgendwann Anfang des kommenden Jahrtausends realisiert, sind Experten überzeugt: Innerhalb der EU besteht die Tendenz, alle Systeme zu vereinheitlichen - eine Währung, einheitliche Förderungen, einheitliche Steuern und auch gleiche Strafen für gleiche Vergehen. Ein deutscher Schnellfahrer, der in Italien von einem Carabinieri wegen einer Geschwindigkeitsübertretung aufgehalten wird, kann nur dann gerecht bestraft werden, wenn der Carabinieri weiß, ob er es mit einem notorischen Tempobolzer zu tun hat. Wie sonst als mit einem Chip-Führerschein, auf dem alle bisherigen Vergehen gespeichert sind, kann dies möglich sein?

Da aber Chipkarten relativ teuer sind, wird durch Kombinationen versucht, diese Kosten relativ niedrig zu halten. Geht man davon aus, daß eine Chipkarte etwa 5 Mark kostet, wären dies bei zehn Millionen Autofahrern 50 Millionen Mark. Eine gewaltige Summe, die nur dann finanzierbar ist, wenn sich auch andere Behörden an dem Chip beteiligen. Plötzlich ist auf dem Führerschein auch die Gesundheitskarte. Zwar ist es Polizisten durch technische Sperren nicht möglich, auch die Gesundheitsdaten zu lesen, aber durch eine Fehlfunktion oder Manipulation könnten diese für ihn abrufbar werden.

## *Krankheiten abrufbereit*

Nur Name, Adresse und Sozialversicherungsnummer oder auch gewisse medizinische Daten wie Blutgruppe, Blutdruck und Allergien? Die Diskussion, die der Einführung eines Chipkarten-Kran-

kenscheins in Deutschland vorausging, war heftig. Daten Schützer, Ärzte und Kartenhersteller lieferten sich vor der Einführung der Gesundheitskarte im Jahr 1993 einen Schlagabtausch, welche Informationen nun wirklich auf der Chip-Gesundheitskarte gespeichert werden sollen.

In Deutschland hat man die Krankenversichertenkarte (KVK) 1993 eingeführt. Auf dieser Chipkarte sind aber nur die Rumpfdaten des Versicherten gespeichert. An eine Erweiterung der Information auf dem Chip wird bereits gedacht. Es ist geplant, auf jeder Karte einen sogenannten Patienten-Datensatz (Patient Data Set) zu speichern. Neben Namen und Adresse sollen auch Angaben über Erkrankungen, Allergien und Medikamente gespeichert sein, die notwendig sind, um eventuelle Komplikationen in einem Notfall zu vermeiden. Auf den neuen Mikroprozessor-Chips können sogar Röntgenbilder gespeichert werden. Wichtigster Punkt ist dabei aber, daß diese Informationen nicht automatisch gespeichert werden, sondern nur dann, wenn der Patient einwilligt. Ein Bürger muß zudem selbst entscheiden können, welche seiner Gesundheitsdaten auf der Karte dokumentiert sind.

Die Entscheidungsfreiheit des Betroffenen ist eine der wesentlichsten Forderungen der Datenschützer. Ministerialrat Werner Schmidt aus dem Büro des Bundesdatenschützers Jacob: »Jeder muß selbst bestimmen können, ob seine Gesundheitsdaten überhaupt auf seiner Chipkarte gespeichert werden. Es darf keinen gesetzlichen und sozialen Zwang geben.« Auch muß ein Patient selbst entscheiden können, ob und wann er welche Informationen auf seiner Karte welchem Arzt vorzeigt. »Auch viele Ärzte sind gegen eine zu enge Verbindung von Krankenversicherungskarte mit Gesundheitsdaten«, betont Schmidt.

In Österreich wollte man die Sozialversicherungskarte (SVK) bereits Anfang 1998 realisieren, wie erwartet kam es, so wie seinerzeit in Deutschland, zu einer Verspätung. Die Ärzte haben sich nicht mit Sozialversicherung und Ministerium einigen können, welche Daten nun tatsächlich auf der Karte gespeichert werden. Jeder sozialversicherte Österreicher, und das sind 99 Prozent der Bevölkerung, erhält eine Chipkarte. Jeder Arzt, jedes Krankenhaus, jede Apotheke wird mit einem Terminal ausgerüstet, auf dem die Daten auf der Karte gelesen werden können. Weil versprochen wird, daß



nur »verwaltungstechnische Daten« auf der SVK gespeichert sind, wird die geplante Ausweitung der Information auf den Karten von den Verantwortlichen in der Diskussion tunlichst vermieden. Denn dem internationalen Trend entsprechend, können die Gesundheitskarten Schritt für Schritt mehr. »Nicht nur die Administration kann Kosten sparen, auch der Nutzen für den Patienten ist enorm«, sagt der Vorstandsbeauftragte des Zentralinstituts der kassenärztlichen Versorgung Deutschlands, Otfried Schaefer. »Dringend benötigte Patientendaten können ohne weitere Untersuchungen direkt von der Chipkarte übernommen werden.« Schaefer denkt dabei an Daten wie etwa Allergien, chronische Krankheiten, Risikofaktoren, ob der Patient Bluter ist, Impfungen, wann er die letzte Fernreise unternommen hat etc. Schaefer: »Es macht auch einen Sinn, wenn ein Arzt weiß, wo er bestimmte Daten finden kann.« In Deutschland läuft mit einigen tausend Patienten ein Testversuch in der Region Koblenz, Anfang 2000 soll die erweiterte Versichertenkarte, sofern der Gesetzgeber zustimmt, in ganz Deutschland erprobt werden. Auch auf der österreichischen SVK sollen in Zukunft neben Name, Adresse und Versicherungsnummer weitere Daten gespeichert werden, wie ein Insider bestätigt. »Besonders in Notfällen schützen diese Informationen den Träger der Chipkarte vor einer möglichen Fehlbehandlung.«

Problematisch könnte ein Chip-Krankenschein vor allem im Unternehmen werden, wenn darauf auch heikle Gesundheits- bzw. Krankendaten gespeichert sind. Ein Betriebsarzl hat in seiner Funktion als Arzt die Berechtigung, auf der Karte Nachschau zu halten. Die Frage, die sich daraus ergibt, ist, wem der Betriebsarzt mehr verbunden ist, dem Arbeitgeber oder dem Arbeitnehmer. Auch bei Neubewerbungen könnte ein Vorzeigen des Chip-Krankenscheins ein Aufnahmekriterium werden. Zwar ist man offiziell nicht dazu verpflichtet, seine Karte vorzuzeigen. Weigert man sich aber, so kann dies Anlaß sein, die Aufnahme abzulehen, da der Bewerber vielleicht eine Krankheit zu verbergen hat.

Jene Resolution, die am 17. April 1996 im Europäischen Parlament beschlossen wurde, wird künftig Krankheitsdaten eines Deutschen und Österreichers in der gesamten Europäischen Union zugänglich machen. Ob von einem Ärzte-Terminal in Lissabon, einer Apotheke in Toulouse oder einem Krankenhaus in Neapel - überall sind

die Daten eines Europäers abrufbar - mit dem europäischen Gesundheitspaß.

In einer ersten Phase ist geplant, den Ausweis vor allem an Personen mit chronischen Erkrankungen bzw. mit schweren Krankheiten, die ständige Behandlung erfordern, auszufolgen. »Von jedem Ärzte-, Spitals- und Apotheker-Terminal können dann die Daten abgelesen werden«, erklärt Doz. Ernst Piller, Chef der Chipkarten-, Zahlungsmittel- und Sicherheitsdruck-Entwicklungs- und BeratungsgesmbH (CZS). Was bei Notfällen einen Vorteil bringt, kann aber auch mißbräuchlich verwendet werden. Zwar gelten dann innerhalb der EU dieselben Datenschutzgesetze, aber es gibt Länder, die mit Datenschutz weniger Erfahrung haben, Daten also nicht so sorgfältig behandeln wie Deutschland oder Österreich. »Das ist einer der Gründe, warum an internationalen, wirksamen Zugriffsregelungen gearbeitet wird«, betont Datenschützer Schmidt.

Die Vorstufe für dieses »EU-Ärzte-beobachten-uns-Programm« ist das ErnergencyCARDLINK-Projekt, das bereits in neun ELJ-Staaten getestet wird. Die EmergencyCARDLINK ist eine Notfallskarte, die einen vereinheitlichten Datensatz enthält, der in jedem der neun Staaten gelesen und ausgewertet werden kann. Auf dieser Karte sind Blutgruppe, Allergien, chronische Krankheiten, verschriebene Medikamente, zugewiesener Arzt etc. gespeichert. Mehr als 100000 Karten wurden auf freiwilliger Basis bereits ausgeteilt. Aber je mehr Freiwillige es für dieses Projekt gibt, desto größer wird der Druck, daß die Karte verpflichtend wird.

Innerhalb der EU sind aber auch einige andere Projekte im Laufen. Eines davon nennt sich Diabcard und beinhaltet, wie der Name schon sagt, Daten von Diabetikern.

## Die Mega-Karte

Mit unbewußter Selbstverständlichkeit ziehen Millionen von Angestellten ihre Zutrittsberechtigung aus der Tasche, wenn sie jeden Morgen das Firmengelände oder Bürogebäude betreten. Doch die Karten öffnen schon lange nicht nur Türen, Tore und Drehkreuze,



sie sind gleichzeitig auch Stechuhr, Kanlinenausweis und Computerberechtigung. Eine Karte, die die Angestellten auf Schritt und Tritt überwacht, die genau dokumentiert, wann sie ins Büro kommen, wie lange sie den Computer bedienen, wie lange sie in der Kantine sitzen etc.

Kartenkombinationen machen Schule, obwohl es nicht nur eingefleischten Gewerkschaftern die Haare aufstellen sollte, sondern all jenen, die sich gegen eine allumfassende Kontrolle in einem Unternehmen wehren. Eine Zutrittskontrolle in die Firma, in das Rechenzentrum oder in Hochsicherheitsbereiche wird immer häufiger auch mit anderen Berechtigungen kombiniert. Vor allem die Kombination Zutrittskontrolle und Kantinenausweis wird immer häufiger eingesetzt, so etwa im Salzburger Landcekrankenhaus.

Die praktische Karte hat damit einen ziemlich großen Nachteil: Der Firmenchef kann nämlich nicht nur feststellen, wie lange sich der Mitarbeiter in der Kantine aufgehalten hat, sondern (anhand der Abrechnung und des Speise- bzw. Getränke-Codes) auch, was er konsumiert hat. Ein Bier in der Mittagspause könnte zu einem Kündigungsgrund werden, da eine Arbeit im »alkoholisierten Zustand« möglicherweise nicht zur vollen Zufriedenheit ausgeführt werden kann. Mitarbeiter müssen sich plötzlich rechtfertigen, warum sie länger als erlaubt auf Mittagspause waren.

Der Bonner Datenschützer Werner Schmidt hat die »absehbaren Anwendungen von Chipkarten«, die beinahe beliebig miteinander kombiniert werden können, aufgelistet. Neben Karten im Geld- und Kreditverkehr, Gesundheitskarten und Ausweisen werden demnächst auch die »Schlüsscl-Ersatz«-Varianten - Autoschlüssel mit Versichcrungsnachweis und Schutzbrief, Haus- und Wohnungsschlüssel, Hotelzimmerschlüssel - realisiert. Schmidt kommt zum Schluß: »Viele der Anwendungen benötigen nur wenig Platz im Speicher. Damit wäre es durchaus realisierbar, alle oder doch fast alle Funktionen in nur einer Karte, einer Megakarte, unterzubringen.«

Der Trend, die Mitarbeiter mit Plastikkarten auszurüsten, steigt. Im Wiener Allgemeinen Krankenhaus wird beispielsweise überlegt, für die PCs eine Zutrittsberechtigung in Form einer Chipkarte zu schaffen. Damit das Spitalspersonal aber nicht sorglos mit den Chipkarten umgeht - sprich, die Karte stecken läßt und dadurch jedem

Zutritt in den PC ermöglicht -, ist beabsichtigt, die PC-Karte mit einem Kantinenausweis zu kombinieren. »Niemand läßt 500 Schilling herumliegen«, meinen jene, die für diese Kombination sind. »Eine PC-Kantinenkarte ist Garantie dafür, daß man sie immer eingesteckt hat.«

Giesecke & Devrient und Austria Card sind bereits mit mehreren Anfragen von Großkonzernen und mittleren Unternehmen konfrontiert, die »multifunktionale Betriebsausweise« einführen möchten. Erfahrungen hat G & D bereits seit 1996. Die Bank of America startete im Frühjahr 1996 mit ihrem »Clock-Tower-Projekt«. Ziel dieses Projekts war ein »multifunktionaler Betriebsausweis mit flexibel programmierbaren Personenprofilen«. Beim Wort »Personenprofil« müßten in Europa die Alarmglocken schrillen. Der Betriebsausweis der Bank of America ist zum einen für die Gebäude-, Parkplatz- und Sicherheitsraum-Zutrittssteuerung da, zum anderen wurde er schrittweise mit Inhouse-Anwendungen nachgeladen - Zeiterfassung, PC-Zugangskontrolle und elektronische Geldbörse. Die Chip-Technologie erlaubt, daß eine Firmenkarte beliebig erweiterbar ist - big boss is watching you.

Mit Hilfe von Karten kann eigentlich ein zweiteiliges Personenprofil erstellt werden. Zum einen ein Nutzungsprofil - wie die Karte verwendet wird. Zum anderen aber auch ein Bewegungsprofil - wann und wo die Karte verwendet wurde.

Siemens hat einen multifunktionalen Betriebsausweis in einer Siemens-Niederlassung in den USA testen lassen. Seit 1996 wird bei »Summit Mission 2000«, wie das Siemens-Projekt genannt wird, die Firmen-Zutrittskarte »schrittweise mit Inhouse-Anwendungen nachgeladen«. Die »üblichen Vorteile« wie G & D dieses Referenzprojekt beschreibt, sind »eine schnelle, effiziente und sichere, überwachungsunabhängige Zugangskontrolle nach dedizierten Personenprofilen«.

# »Lauschangriffe« im Datenreich

**> Wie man vom Nebenbüro aus Ihren PC abhören kann.**

**> Wie man aus einer Steckdose Text absaugen kann.**

**> Warum Sie im Internet nie mit Kreditkarte bezahlen sollten.**

**> Wie Microsoft via Internet feststellen kann, ob Ihre Programme Raubkopien sind.**

**> Wie FBI oder CIA in Ihrem Computer herumschnüffeln können.**

**> Wie Kollegen an Ihr Paßwort kommen.**

**> Warum Sie nicht jedem E-Mail trauen sollten.**

**> Warum ein E-Mail Ihren Computer verseuchen kann.**

## Der abhörbare Home-PC

Die Sekretärin sitzt im Büro und tippt den Text eines Diktats in den Computer. Drei Zimmer weiter packt ein Techniker einen UHF-VHF-Empfänger aus, steckt ihn an die Steckdose und klemmt die Antennenkabel mit zwei Klemmen an den Nulleiter der Steckdose. Vorsichtig beginnt er an einem Regler zu drehen. So lange, bis auf einem an das Empfangsgerät gekoppelten Bildschirm der Text von jenem Computer erscheint, den die Sekretärin drei Zimmer weiter zum gleichen Zeitpunkt eingibt. Der Text kann nicht nur gelesen, sondern auch gespeichert werden. »Das kann doch ein jeder Bastler.« Dipl.-Ing. Horst Ahlbrecht, zuständig für Abstrahltechnik im deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) in Bonn, kann sich über erstaunte Gesichter nur wundern.

»Daß man sich auf diese Art und Weise Informationen besorgen kann, haben wir doch schon vor zehn Jahren demonstriert.« Aber selbst der Techniker muß zugeben, daß diese »bloßstellende Abstrahlung«, wie sie von den Experten genannt wird, eine wenig bekannte Gefahr ist und vor allem in der Betriebs- und Firmenspionage sehr effektiv sein kann.

Warum sich ein Home- oder Firmen-PC abhören läßt, ist leicht erklärt. Jedes Gerät strahlt elektromagnetische Wellen ab. In dieser Strahlung ist Information versteckt, die von einer Antenne aufgesogen und wieder zusammengesetzt werden kann. Sich an den Nulleiter einer Steckdose klemmen zu können, der wie eine Antenne funktioniert, ist der Idealfall. »Es funktioniert aber auch mit Richtantennen«, bestätigt Ahlbrecht. Sogar aus einer Entfernung von 30 bis 40 Metern können die Informationen aufgesogen werden, etwa von einer Straße aus in ein Büro im zweiten Stock. Die Idealdistanz aber sind zehn Meter. »Früher ging es leichter als jetzt, da die Computer stärker gestrahlt haben«, erklärt Ahlbrecht. In den vergangenen Jahren mußten die Hersteller die Abstrahlung aus Gründen der Gesundheitsgefährdung reduzieren. Auch die Monitore haben eine höhere Auflösung, wodurch man bei den Empfängern höhere Bandbreiten benötigt, um die Information darstellen zu können.

Die »bloßstellende Abstrahlung« ist heute in jedem Bürogebäude möglich, da Ringleitungen diese Art von Lauschangriffen ziemlich vereinfachen. Mit ein wenig technischem Verständnis kann man ein Büro unter oder über dem eigenen anzapfen. Voraussetzung dafür ist neben dem Know-how vor allem der UHF-VHF-Empfänger. Der allerdings kostet etwa 10000 Mark. Doch Ahlbrecht warnt all jene, die derartige Methoden mit einem »mir kann das nicht passieren« abtun. Denn nicht nur Computer können angezapft werden, auch die akustische Abstrahlung von Druckern enthält Informationen: Textbausteine, die sich über Schall und Ultraschall ausbreiten und rekonstruiert werden können. Das Bundesamt für Sicherheit in der Informationstechnik - mit allen deutschen Behörden, darunter auch dem Bundesnachrichtendienst, verflochten - ist in jüngster Vergangenheit schon mehrmals mit derartigen Fällen konfrontiert gewesen. Ahlbrecht: »Warum wohl haben große Konzerne wie BMW, VW oder Siemens ihre Entwicklungsabteilungen mitten im



Firmengelände errichtet und nicht am Rand?« Räumliche Distanz ist eine der Möglichkeiten, wie sich normale PC-User schützen können. Auf dem Markt gibt es abstrahlgeschützte Geräte zu kaufen. Hersteller von PC-Bildschirmen werben mit dem Begriff »abstrahlarm« nach MPR II, TCO, SSI, wie die Richtlinien heißen. Damit sind aber nur die möglichen gesundheitsschädlichen Auswirkungen der Gerätestrahlung gemeint. Die gängigste Methode gegen die bloßstellende Abstrahlung heißt Quellentstörung. Dabei wird in den Computer ein Chip eingebaut, der Störsignale sendet, wodurch die empfangene Information für Spione unbrauchbar wird.

Ahlbrecht warnt aber auch vor dem Überkoppeln. Ein PC, der mit einem Großrechner verbunden ist, kann seine Informationen auf diverse andere Leitungen übertragen. Physikalisch ist das relativ einfach erklärt: Bei der Übertragung eines Signals ist ein Kabel mit einem elektromagnetischen Feld umgeben, das auf anderen Kabeln in unmittelbarer Umgebung Spannungen und Ströme erzeugt. Diese können dann entsprechend abgezapft werden. Bei den Leitungen sollte deshalb beachtet werden, daß einerseits nur Kabeltypen verwendet werden, die ein geringes elektromagnetisches Feld freisetzen (etwa Koaxialkabel). Andererseits sollte beim Verlegen der Leitungen ein ausreichender Abstand zu anderen Kabeln beachet werden.

## Auf Schritt und Tritt registriert

Etwa 50 Millionen Internet-Benützer gibt es weltweit, bis ins Jahr 2000 soll sich die Zahl beinahe verzehnfachen. Den meisten, die im Internet surfen, ist es nicht bewußt: Bei jedem Besuch im WorldWideWeb (WWW) hinterläßt der Besucher seine Spuren, das Verhalten wird penibel genau registriert und dokumentiert. Jeder Internet-User erhält, nachdem er sich eingewählt hat, die sogenannte IP-Adresse (Internet-Protokoll-Adresse, die persönliche Internet-Kennummer), und mit dieser ist er im gesamten WWW identifizierbar. Jeder Internet-User kann die Probe aufs Exempel machen. Das in Washington ansässige Center of Democracy and

Technology (CDT) oder die Anonymizer Inc. in La Mesa/Kalifornien liefern den Beweis. Wer die Internet-Adresse http://www.cdt.org oder http://www.anonymizer.com anwählt, wird beim CDT mit »Hi, hier ist das, was wir über Dich wissen« begrüßt. Bei der Anonymizer Inc. braucht man sich gar nicht vorstellen: »Wir wissen, wer du bist.« Binnen weniger Sekunden wird aufgelistet, was - ohne großen Aufwand - über den Internet-Surfer herausgefunden wurde. Hier kann der erstaunte Computeranwender nicht nur lesen, aus welchem Land er kommt, welches Betriebssystem er einsetzt und welchen Browser er verwendet. Sondern auch die Auflösung des Bildschirms wird genau bekanntgegeben und - sicherlich die heikelste Information - welche Seite der Internet-Surfer zuletzt besucht hat.

»Diese Möglichkeit könnten sich viele Unternehmen zunutze machen«, meint der Computerexperte im BSI, Dirk Hager. Hager ist einer von jenen Experten, die im Referat »Technische Risiko-Analyse und Abwehr« das Daten- und Internet-Reich auf Unsicherheiten kontrollieren und Probleme aufzeigen. Wer sich auf der Opel-Homepage über den neuen Astra informiert und später die VW-Homepage besucht, ist durchschaut. VW kann feststellen, daß man sich vorher für den Astra interessiert hat. Da das Konkurrenzprodukt zum.Astra ein Golf ist, könnte VW dem Kunden Golf-Prospekte zuschicken. »Theoretisch ist das freilich möglich, ob es schon gemacht wird, ist schwer zu beweisen«, meint Hager. Sein praktischer Rat: »Dazwischen andere, unverfängliche Internet-Seiten öffnen.«

Internet-Surfer, die einen Microsoft-Internet-Explorer verwenden, sind für den Microsoft-Konzern ein sprichwörtliches offenes Buch. Der US-Multimedia-Gigant hat in seinen Internet-Explorern die technischen Voraussetzungen geschaffen, daß sich Microsoft ohne Wissen des Benutzers in den Home-PC einschleichen und kontrollieren kann, ob die verwendete Software wirklich gekauft wurde oder eine Kopie ist. Voraussetzung für diese Schnüffelei ist aber, daß sich der redliche Besitzer hat registrieren lassen. Ist keine Registrierung vorhanden, kann Microsoft nicht feststellen, welches der Programme das Original und welches die Kopie ist. Nachforschungen, um das zu klären, sind Microsoft derzeit noch zu aufwendig.

Interesse an der Identität des Surfers haben auch die Geheimdienste in der ganzen Welt - ob Mi6 (http://www.cc.umist.ac.uk/sk/



index.html), CIA (http://www.odci.gov/cia) oder die National Security Agency NSA (http://www.nsa.gov). Jeder Surfer wird registriert und via Computer ausspioniert. Wer sich auf der FBI-Homepage (http://www.fbi.gov) die Bilder der zehn meistgesuchten Verbrecher der USA, die »Ten most wanted«, anschaut, wird in der Zwischenzeit online observiert.

## Von Keksen, die nicht schmecken

Die Anwender-PCs werden von Keksen ausspioniert. Damit sind aber nicht süße Plätzchen gemeint, sondern Dateien mit dem beinahe lieblichen Namen »Cookies«. Hinter diesen Keksen stecken gefährliche Trojanische Pferde, die nicht nur die persönlichen Daten eines PC-Benutzers speichern, sondern unter bestimmten Voraussetzungen sogar den gesamten Inhalt einer Festplatte verschicken können.

Cookies dringen in die Harddisk eines Benutzers ein und registrieren das Online-Verhalten - welche Seite man sich wie lange anschaut, was man in eine Seite geschrieben hat etc. Sie sind durchaus sinnvoll und erleichtern den Zugang zu bestimmten Informationen. Wer beispielsweise gebührenpflichtige Online-Zeitungen wie etwa die »New York Times« anwählt, muß seine Identität und sein Paßwort bekanntgeben. Zumindest beim erstenmal, denn gleichzeitig mit den Zutrittsformalitäten wird unbemerkt ein Cookie installiert. Beim zweitenmal erkennt die »New York Timcs«-Homepage sofort, urn wen es sich handelt, und verlangt weder Identität noch Paßwort. Auch beim Einkaufen im Internet machen Cookies durchaus Sinn. Sie merken sich den Einkaufszettel. Sollte nämlich das Computersystem aus irgendeinem Grund abstürzen, bleiben die ausgewählten Artikel gespeichert.

Das Hauptproblem der Cookies besteht aber darin, daß immer mehr Anbieter im Netz ihre Cookies auf den Anwender-PCs installieren wollen, obwohl sie nichts zu verkaufen haben. Der Grund: sie wollen die Gewohnheiten der Benutzer festhalten - wer wie oft eine Webseite besucht, welches Warenangebot häufig angeschaut wird oder etwa welche Werbeseiten am häufigsten betrachtet

werden. In diesen Schnüffler-Cookies liegt die Gefahr. Sie versuchen mehr über uns herauszufinden, als uns lieb ist.

Man ist ihnen aber nicht schutzlos ausgeliefert. »Browser wie Netscape-Navigator oder Internet-Explorer melden dem Benutzer, sobald jemand ein Cookie installieren möchte«, erklärt BSI-Experte Hager. Voraussetzung dafür ist, daß man die Option aktiviert hat. Es gibt aber auch einen Nachteil. Da es im WWW nur so wimmelt von diesen Keksen, wird das Surfen zu einer langwierigen Angelegenheit. Es gibt aber auch Anti-Cookie-Programme auf dem Markt, mit denen man gewisse Cookies akzeptieren kann und andere automatisch gelöscht werden. Mit dem Datei-Suchmechanismus lassen sich im PC auch Cookie-Dateien finden - Suchbegriff Cookie. Unter http://www.luckman.com erhält man ein freies »anonymes Cookie« - ein Programm, das ein Keks kampfunfähig macht. Und über die schon erwähnte Webseite http://www.anonymizer.com kann man völlig anonym durchs Internet surfen, ohne irgendeine Spur zu hinterlassen und ohne unbewußt in ein Keks beißen zu müssen. Die Anonym-Surf-Ausflüge sind kostenlos und verursachen nur eine verlängerte Online-Zeit um 40 Sekunden. Für Abonnenten (15 Dollar im Vierteljahr) entsteht keine Zeitverzögerung.

Mit den Informationen, die die Cookies liefern, wird der PC-Benützer für die Anbieter derzeit noch nicht transparent, die Benutzerprofile sind ohne persönliche Daten für persönliche Marketing-Strategien noch nutzlos. Problematisch wird es erst dann, wenn der PC-Benützer Name und Adresse bekanntgibt. Beim Online-Shopping ist dies meist unabwendbar. Die Anbieter versuchen aber mit diversen Tricks, an die Daten der Benutzer zu kommen. Für einige Web-Seiten muß man, bevor man auf bestimmte Inhalte zugreifen kann, einen Fragebogen ausfüllen. Tips für jene, die unbedingt an die Information nach der Fragebogen-Seite herankommen möchten: nicht die Wahrheit schreiben, Pseudonym angeben.

Bei der Datenbeschaffung sind manche Anbieter nicht zimperlich und benutzen Kinder als Informanten. Die New Yorker Children Advertising Review Unit (CARU) hat kürzlich festgestellt, daß in Seiten, die sich speziell an Kinder richten, oft von den Kindern verlangt wird, ihre Familie näher vorzustellen und so z. B. den Beruf des Vaters, der Mutter und Hobbys der Familie bekanntzugeben. Auch bei der Geldbeschaffung sind manche Anbieter nicht heikel:



Die Telefonrechnung trieb jenen Kunden, die im Februar 1997 die Pornoseite www.sexygirls.com besucht hatten, die Schweißperlen auf die Stirn: einige tausend Mark machte sie aus. Wer im Internet surft und sich diverse Webseiten - es müssen nicht unbedingt Seiten von Sexanbietern sein - aufruft, sollte beim Herunterladen von Spezialprogramrnen vorsichtig sein.

Bei www.sexygirls.com wurde der Betrachter nach einigen Bildern aufgefordert, ein Programm herunterzuladen, um auch die »schärferen« Bilder betrachten zu können. Das Programm war in Wahrheit ein Trojanisches Pferd, das den Internet-Aufbau völlig veränderte. Ohne daß der Surfer es merkte, kappte das Programm die bestehende Verbindung, schaltete das Modem ab und wählte eine Nummer in Moldawien an. Ab diesem Zeitpunkt mußte der Surfer die regulären und folglich höheren Telefongebühren nach Moldawien bezahlen. Der Skandal, der in Kanada aufflog, kostete einzelne Kunden Tausende Dollar, berichtete der »Toronto Star«. Wie viele Deutsche und Österreicher diesem Schwindel aufgesessen sind, ist unbekannt, denn die Bereitschaft, sein eigenes Internet-Verhalten publik zu machen, ist relativ gering. Wenige Wochen nach Auffliegen des Skandals wurde das Service auf Anordnung des US-Handelsministeriums geschlossen.

## Die Computer-Hacker sind unter uns

Ihr Auftrag lautet: »Knackt unser System.« Unzählige Computerexperten in Deutschland und Österreich haben sich auf die »Sicherheitsüberprüfungen von Firmennetzwerken« spezialisiert. Die Branche, die mit dem einfachen Wort »hacken« kurz und prägnant charakterisiert wird, boomt. In einer Zeit, in der 16jährige das Pentagon knacken können, sind Banken, Versicherungen, Energieversorgungsunternehmen, Krankenhäuser etc. daran interessiert, daß niemand in ihre Rechner eindringt und sich illegal Informationen verschafft.

Eine Statistik darüber, wie viele Hacker-Angriffe pro Jahr auf deutsche und österreichische Unternehmen durchgeführt werden, gibt es nicht. »Solche Vorfälle werden unter der Decke gehalten«, ist

auch Andy Müller-Maguhn vom Chaos-Computer-Club überzeugt. »Keine Bank, kein Konzern wird zugeben, wenn es einen Angriff gegeben hat«, bestätigt ein Bankeninsider. »Was glauben Sie, was passieren würde, wenn es heißt, in der Bank XY haben Hacker einen Millionenschaden verursacht. Kunden würden fluchtartig Konten schließen und ihr Erspartes abheben. Der Schaden wäre noch größer als der, der durch den Hacker verursacht wurde.«

Computer-Hacking hat eine lange Tradition. Ursprünglich wurden als Hacker jene Studenten bezeichnet, die in den Anfängen des Computerzeitalters an den Universitäten noch nach Mitternacht vor den Terminals saßen und ihre Programme in die Tastatur »hackten«. Ihre Meinung war, daß der Computer der Schlüssel für die geistige Freiheit der Menschen sei, da er Wissen für jedermann zugänglich macht. Daß die Rechner der größten Unternehmen zu knacken sind, zeigen die Security-Checks der »Berufs-Hacker«. »Bei zehn Aufträgen knacken wir zehnmal die Systeme«, schildert der Geschäftsführer des Wiener Software-Dienstleisters X-Soft, Ing. Michael Gutlederer. Er ist einer der wenigen, die offiziell in Banken einbrechen durften. »Manche Unternehmen sind überzeugt, daß ihr System keine Schwachstellen hat, und dann zeigen wir ihnen, wie leicht es wirklich ist einzudringen. Einmal«, so .Gutlederer, »haben wir innerhalb von 15 Minuten 50 Löcher gefunden. Dem Firmeneigentümer ist ziemlich heiß geworden.«

Computer-Experten sind überzeugt, daß es keine absolute Sicherheit geben kann. Das Rechnersystem des Pentagon gehört zu den sichersten auf der Welt. Dennoch schaffen es immer wieder Schüler und Studenten, die Systeme zu knacken. Der 16jährige Brite Richard Pryce ist 1995 mit einem normalen 486 SX 25 mit einer 170-MB-Festplatte und einem 9600-Baud-Modern - also einem normalen Horne-PC - in das Pentagon eingebrochen. Der schüchterne Junge, der sich »Datastream Cowboy« nannte, hackte sich in die »Computer streng bewachter militärischer Forschungseinrichtungen, spazierte ungehindert über Festplatten und stahl Programme, die nicht für die Öffentlichkeit bestimmt waren«, beschrieb der »Spiegel« (Nr. 19/97) den »Angriff auf das Pentagon«. Aufgrund dieses Einbruchs wurde 1996 eine Studie veröffentlicht, die den US-Senat erschreckte. Die Verfasser der Studie kamen zum Schluß, daß es allein im Jahr 1995 mehr als 250000 Hackerangriffe



auf die 100000 Netzwerke des Pentagon gab, und - die Schreckensmeldung schlechthin: 65 Prozent der Hackerangriffe waren erfolgreich.

Wenn das Pentagon zu knacken ist, kann eine deutsche Bank oder ein österreichisches Versicherungsunternehmen erst recht geknackt werden. Auf der einen Seite können sich kriminelle Hacker, ganz gleich, wer der Auftraggeber ist, finanzielle Informationen beschaffen und sogar umleiten. Auf der anderen Seite wären etwa Versicherungsdaten für Arbeitgeber sehr hilfreich in der Personalpolitik. Beim Hacken geht es aber nicht nur um das Eindringen in Systeme großer Unternehmen, sondern auch um betriebsinterne Spionage. Wenn Kollegen die Dateien anderer Kollegen kopieren und fremde Ideen als die ihren verkaufen. Die Paßwörter in den Firmen stellen auch für Laien kein Hindernis dar. Die meisten Paßwörter sind zu knacken. Im Internet werden sogenannte Paßwort-Cracker angeboten. Kostenlos. In diesen Programmen sind 50000 und mehr gängige Paßwörter gespeichert. »Jeder halbwegs gebildete HTL-Schülcr kann diese Programme gegen ein gesuchtes Codewort gegenlaufen lassen«, erklärt der Geschäftsführer des österreichischen Instituts für Datenschutz und Informationssicherheit (INDIS), Ing. Dieter Göschler. »Theoretisch könnte man sogar eine Wörterbuch-CD durchlaufen lassen.« Warum diese Paßwort-Cracker mit sehr hoher Wahrscheinlichkeit den Code knacken, ist einfach erklärt: Die meisten Menschen verwenden logische Codewörter - Namen, gängige Buchstaben oder Zahlen.

## *Firewalls, die Burgmauern eines Rechnersystems*

Ob das Pentagon in Washington, der Bundesnachrichtendienst in Pullach oder die Blutdatenbank des Roten Kreuzes in Wien - die Großrechner und Computersysteme all dieser Institutionen sind mit sogenannten Firewalls abgesichert. Eine Firewall kann mit einer Burgmauer verglichen werden: Sie ist ein zwei- oder mehrstufiges Sicherheitsprogramm, eine Art Filter, der jede Information, die ins zu schützende Netz gelangen möchte, daraufhin überprüft, ob sie ins System darf.

Die »Feuermauer« verhindert mit einer Reihe von Paßwörtern zum einen, daß Hacker in einen Großrechner gelangen und Daten kopieren bzw. verändern. Zum anderen lassen die dem Netz vorgelagerten Filter nur bestimmte Nachrichten durch. Eine Firewall kann z. B. so konfiguriert werden, daß keine Internet-Adressen von Sex- oder Pornoanbietern ins System gelangen können.

Eine Firewall muß aber auch ständig verbessert werden, da die Hacker ziemlich erfinderisch sind. Sobald ein Hacker dieses Schutzprogramm überwunden hat, kann er im System nach Belieben agieren und immensen Schaden anrichten.

Große Konzerne und Unternehmen lassen ihre Systeme deshalb meist von Profis checken, ob sie sicher sind. Auf diese Security-Checks haben sich zum einen eigene Firmen spezialisiert, zum anderen hat der Chaos-Computer-Club (CCC) diese Aufgabe übernommen. Vor allem in Deutschland ist der CCC zu einer Institution geworden, die von vielen privaten, aber auch staatlichen Stellen als Gutachter kontaktiert wird. Wenn der CCC ein positives Zeugnis ausstellt, können Unternehmen oder Behörden beruhigt sein, denn dann gelten ihre Rechnersysteme als sicher. Kritisiert der CCC aber den Sicherheitsstandard, so bedeutet dies, daß Hacker das System knacken können.

Der CCC ist eine Plattform der wohl besten Computer-Experten Europas, die Zweigstellen in ganz Deutschland und Partner auf dem ganzen Kontinent hat. Da die Computerfans ständig miteinander kommunizieren und neueste Entwicklungen - betreffs das Hacken eines Telefons, eines Stromzählers etc. - diskutieren, sind sie immer auf dem neuesten Stand und wissen von möglichen Gefahren Bescheid, bevor sie für Unternehmen zum Problem werden können. Dennoch gibt es unzählige Firmen, die sich der Gefahr nicht bewußt sind, daß Hacker ihre Systeme lahmlegen oder Daten stehlen können.

## Der Kummer mit der Kreditkartennummer

Wer mit seiner Kreditkartennummer bereits einmal im Internet eingekauft hat, darf sich nicht wundern, wenn er auf seiner Abrechnung plötzlich mit Ausgaben konfrontiert ist, die er gar nicht getätigt hat. Wenn Kreditkartennummer und Ablaufdatum auf der Datenautobahn auf Reisen geschickt werden, kommen sie nicht immer nur dort an, wo ihr eigentliches Ziel ist. Zum einen kann eine undichte Stelle beim Anbieter für eine Verbreitung der Daten sorgen, zum anderen kann irgendwo im Netz ein Lauscher sitzen, der nur darauf wartet, auf eine Kreditkartennummer zu stoßen. Mit eigenen »Sniffle«-Programrnen können versierte Techniker Kauftransaktionen »herausschnüffeln« und Kreditkartennummern abspeichern.



Anbieter und Käufer für diese 16stelligen Zahlenkombinationen finden sich immer. Auch hier wird man im Internet fündig. Zum einen gibt es unter http://www.hackershomepage.com kostenpflichtige Tips ab 5 Dollar, wie man Telefone anzapft, kostenlos eine Stunde im Zimmer eines Hotels verbringt - »genug Zeit für Sex« - oder aber auch, wie man mit gestohlenen Kreditkartennummern ein lukratives Geschäft machen kann.

Das WWW ist auch Umschlagplatz für Kriminelle, die die Nummern von Visa, MasterCard, Diners Club und den diversen anderen Plastikkarten-Unternehmen zum Kauf anbieten -auch die von deutschen und österreichischen Kredikartcnbesitzern. Der im Herbst 1995 in Los Angeles verhaftete Cornputer-Hacker Kevin D. Mitnick hatte nicht nur den Computer des US-Verteidigungsministeriums geknackt, sondern auch aus Datenbanken insgesamt 20000 Kreditkartennummern gestohlen. Zwei Jahre lang hatte das FBI nach ihm gefahndet. Mitnick hat eine große Fan-Gemeinde im Internet, seine Arbeit hat Nachahmer gefunden. Am 12. Dezember 1997 hatten Computer-Hacker die Homepage des weltweiten Internet-Suchprogramms Yahoo! für 15 Minuten okkupiert und gedroht, daß ein Virus aktiv wird, sollte Mitnick nicht freigelassen werden. Der Geist von Mitnick lebt in seinen Fans weiter.

»Es gibt Listen von Kreditkartennummern, die sich die Hacker gegenseitig zuschicken«, bestätigt Dieter Göschler vom Institut für Datenschutz und Informationssicherheit. Wer im Internet einkauft, sollte nur dann mit Kreditkarte bezahlen, wenn die Transaktion verschlüsselt abläuft, was sowohl im Netscape-Navigator als auch im Microsoft Internet-Explorer möglich ist. Die verwendeten Verschlüsselungsalgorithmen sind unter Fachleuten anerkannt. Als

Zeichen der Verschlüsselung scheint im Netscape-Navigator an der linken unteren Bildschirmseite ein Schlüssel-Symbol auf, im Internet-Explorer rechts unten ein Schloß-Symbol. Ist er durchbrochen, wird nicht verschlüsselt, und die Kreditkartennummer kann von Hackern im Netz gespeichert werden. Göschlers Rat: »Unverschlüsselt sollte man im Internet nur das von sich bekanntgeben, was man auch auf eine Postkarte schreiben würde.«

## Das Problem mit dem Klammeraffen

Die E-Mail, die der Bonner BSI-Experte Dirk Hager am 1 . Oktober 1997 zugeschickt bekam, hatte es in sich: Absender war die Organisation SANS Institute (Systems Administration, Networking and Security). Diese veranstaltet in den USA Kongresse und Tagungen zum Thema Netzsicherheit. Die E-Mail bestand aber aus pornografischen Bildern - ein Hacker hatte die gesamte E-Mail verfälscht. Eine der vielen Möglichkeiten, wie E-Mails »verunstaltet« werden können. Sie enthalten oft nicht nur Bilder oder unerwünschte Textbausteine, sondern auch Computerviren.

Die meisten Internet-Benutzer bevorzugen E-Mails gegenüber herkömmlichen Kommunikationsmethoden wie Brief, Fax oder Telefon: Im Normalfall dauert die Übertragung von längeren Briefen nur wenige Sekunden, auf eine Nachricht erhält man in kürzester Zeit eine Antwort. Die günstigen Online-Tarife betragen einen Bruchteil der Telefon- oder Post-Spesen. E-Mail ist umweltfreundlicher, Texte können sofort weiterverarbeitet werden, und auch schwer erreichbare Menschen kann man jederzeit kontaktieren.

»E-Mails sind allerdings schon lange nicht mehr vertraulich«, bestätigt Hager. Eine E-Mail ist wie eine Postkarte, jeder kann mitlesen, und jeder kann den Inhalt der Nachricht ändern. Unter »jeder« versteht Hager »versierte Computerfreaks«, aber derer gibt es in der heutigen Zeit genug. Wer einen Job sucht und die Zusage per E-Mail erhält, sollte daraufhin nie andere Bewerbungen zurückziehen. »Es könnte eine Fälschung sein«, warnt Hager. »Der Absender einer E-Mail kann mit Leichtigkeit vorgetäuscht werden.« Hager demonstriert es, öffnet diverse Dateien in seinem Computer, tippt



Buchstaben und @ in die Tastatur - fertig ist eine vom Büro des Bundeskanzlers verfaßte E-Mail. Problemlos kann man sich als Helmut Kohl oder Viktor Klima ausgeben und E-Mails mit seriös klingendem Inhalt verschicken.

Wie man Menschen mit E-Mails terrorisieren kann, hat eine Gruppe von Studenten an der Technischen Universität in Wien gezeigt. Die sogenannte »Tiger's Claw« startete im Zuge der Studentenproteste gegen das Sparpaket im Frühjahr 1996 eine E-Mail-Bombing-Aktion. Pro Tag wurden 30 Millionen E-Mails an die Rechner der Regierung und der Parteien geschickt und so die Systeme fast lahmgelegt. Aufsehen erregte eine Mailbombe im Frühjahr 1997 an der Universität Münster. Ein Unternehmen schickte der Uni mehr als 25000 E-Mails, woraufhin das System zusammenbrach. Das Unternehmen wollte aber nicht die Hochschule angreifen, sondern hatte versucht, allen Studenten eine Werbemitteilung zu schicken. E-Mail-Bombing schadet dem Benutzer aber auch finanziell, da schon die Übermittlung der E-Mails eine Menge Zeit und deshalb Telefongebühren kostet.

Durch die E-Mails ist auch das Computerviren-Problem größer geworden. Mit E-Mails werden Cornputerviren im Schneeball-System über die ganze Welt verstreut. Innerhalb weniger Sekunden wird ein neues Virus von einem Kontinent auf den anderen geschickt. Weltweit sind derzeit etwa 16000 Computer-Viren bekannt, alle zehn Minuten, so schätzen Experten, kommt ein neues hinzu. Ein via E-Mail verschicktes Virus bleibt aber so lange harmlos, bis man die E-Mail liest. Sobald man sie öffnet, wird das Virus aktiv und setzt sich unter anderem auf alle im Computer befindlichen E-Mail-Adressen. Beim nächsten Sendevorgang wird das Virus weiterverschickt.

Das österreichische Institut für Datenschutz und Informationssicherheit (INDIS) bietet seit Ende 1997 eine neue Service-Dienstleistung an: verdächtige E-Mails auf Viren zu untersuchen. Selbst wer eine Nachricht von Geschäftspartnern oder Freunden bekommt, kann nicht immer davon ausgehen, daß kein Virus enthalten ist. Bei unbekannten Absendern sollte man noch vorsichtiger sein. Verdächtige E-Mails können an die Service-E-Mail-Adresse von INDIS geschickt werden: viruslab@indis.at. Innerhalb von einigen Minuten wird sie nach dem jeweils neuesten Virenprogramm auf

alle bekannten Viren durchsucht und »gesund« retourgeschickt. Kosten: etwa 120 Schilling/Monat.

## »Wir verlieren unsere Privatsphäre«

Durch die immer stärkere Verbreitung von Internet - im Jahr 2000 werden weltweit etwa 500 Millionen PC-Benutzer das Internet nutzen - gewinnen die Sicherheitsaspekte eine große Bedeutung. In den kommenden lahren wird die Verschlüsselung, also das Chiffrieren von Nachrichten, eine Notwendigkeit. Schlagworte der Zukunft sind Kryptografie (Lehre von der Verschlüsselung) und digitale Unterschrift. Der berühmte US-Kryptologe Phil Zimmermann, der das Verschlüsselungsprogramm Pretty Good Privacy (PGP) erfunden hat, hat in einem Interview im »Spiegel« (Nr. 36/96) auf die Notwendigkeit von Verschlüsselungsprogrammen aufmerksam gemacht: »Je weiter das Informationszeitalter voranschreitet, desto mehr verlieren wir unsere Privatsphäre. Regierungen können heute mit automatischen Systemen den Telefonverkehr fast lückenlos überwachen und nach Schlüsselwörtern oder den Stimmen einzelner Personen durchforsten. Sie können den Datenverkehr im Internet überwachen. Dieses System widerspricht den historischen Grundlagen der Demokratie. Nur durch Verschlüsselungstechnik können wir einen Teil der verlorenen Privatsphäre zurückgewinnen.«

Im Kampf um diese Privatsphäre eröffnen sich mitunter unvorhergesehene Probleme, denn der Staat möchte die volle Kontrolle über seine Bürger. Im Zuge der Diskussion des 1996 in Deutschland beschlossenen Signatur-Gesetzes hat Innenminister Manfred Kanther im April desselben Jahres enge Grenzen für diese Technik gefordert. Kanther befürchtete, daß durch die Kryptografie die Überwachung von Gangstern keinen Nutzen mehr hat. Kanther war für ein typisches »ja, aber«. Er wollte Kontrollmechanismen schaffen, wie es sie bei der Tele- und Mobilkommunikation gibt. Sprich: in bestimmten Verdachtsfällen hätte der Staat die Codes knacken dürfen. Wirtschaftsminister Günter Rexrodt sprach sich gegen eine »Nutzungsbeschränkung« aus, und Justizminister Edzard Schmidt-Jortzig meinte: »Die Bürger müssen die Möglichkeit haben, selbst für den Schutz ihrer Daten zu sorgen« (»Die Zeit«, 9. 5. 1997). Abschreckendes Beispiel ist Frankreich. Dort müssen Codes von der Regierung genehmigt werden. Es ist nicht anzunehmen, daß dort die staatlichen Behörden Verschlüsselungen erlauben, die sie selbst nicht knacken können. Viele Staaten setzen der Kryptografie einen Riegel vor. Der Handy-Hersteller Ericsson wollte vor einigen Jahren die Kommunikation seiner weltweiten Filialen verschlüsseln. Es blieb bei der Absicht, da die Kryptografie von einigen Staaten verboten wurde.



»Aber Kryptografie ist die Zukunft«, meint der Grazer Universilätsprofessor Reinhard Posch. Posch, der zu den führenden Kryptografie-Experten Europas gehört, ist überzeugt, daß bei guter Kryptografie auch die amerikanische National Security Agency (NSA) machtlos ist. Und die Experten der NSA zählen zu den Code-Brechern schlechthin.

## Das Krypto-Schloß

»Verschlüsselung wird unentbehrlich für den Schutz der Privatsphäre, sonst werden die immer leistungsfähigeren Kommunikationstechniken auf Dauer die Freiheit zerstören«, zitierte am 9. Mai 1997 »Die Zeit« den Mathematiker Whitfield Diffie. Diffie hat 1975 die »public key cryptography« erfunden. Damals eine Sensation in der Computer-Fachwelt. Ein Algorithmus und ein Schlüssel codi,eren und decodieren eine Information. Der Algorithmus ist eine komplizierte Formel, der Schlüssel eine sehr lange Zahl - diese Codes waren bis vor wenigen Jahren sehr schwer knackbar. Jetzt aber schaffen dies Großrechner oft innerhalb weniger Sekunden.

Die Schlüssel werden in der Computereinheit Bit gemessen. Je mehr Bit, desto schwerer zu knacken. 40-Bit-Schlüssel galten bis vor wenigen Jahren noch als unknackbar. »Jetzt ist ein 40-Bit-Schlüssel innerhalb von zwei Tausendstel Sekunden zu knacken«, erklärt Universitätsprofessor Posch. Künftig werden die Schlüssel auf bis zu 90 Bit verlängert werden müssen.

Wird auf diese Art und Weise eine Information von A nach B geschickt, müssen sowohl Sender als auch Empfänger im Besitz des

Schlüssels sein, der die Nachricht codiert und decodiert. Auf Distanz ist es schwierig und zudem auch unsicher, Schlüssel bekanntzugeben. Mathematiker haben deshalb ein Krypto-Schloß erfunden. Ein Codierungssystem, das mit einem Schlüssel geschlossen und mit dem anderen geöffnet werden kann. Jemand, der im Besitz dieser Kryptografie-Technik ist, hat einen geheimen und einen öffentlichen Schlüssel. »Schickt man nun jemanden einen elektronischen Brief, so codiert man diesen mit dessen öffentlichem Schlüssel«, erklärt Posch. »Die Nachricht kann nur mit dem geheimen Schlüssel entziffert werden.«

Das »Krypto-Schloß« wird das Verschlüsselungsinstrument der Zukunft. In Deutschland werden diese Verschlüsselungstechniken bei der »digitalen Signatur« bzw. in Österreich bei der »digitalen Unterschrift« eingesetzt.

Das Verfahren der digitalen Unterschrift sieht vor, daß der Bürger bei Organisationen wie etwa bei Banken, Telekommunikationsunternehmen, Post oder Sozialversicherungen eine digitale Unterschrift beantragt. Dort erhalt er einen geheimen und einen Öffentlichen Schlüssel. Der öffentliche wird in einem öffentlichen Register gespeichert, der »geheime Schlüssel« steht nur dem Bürger zur Verfügung. Mit diesem kann dann eine elektronische Unterschrift unter ein im Computer geschriebenes Dokument gesetzt werden. Behörden, Organisationen und Firmen können die Richtigkeit des Dokumentes und die Identität des Senders mit dem öffentlichen Schlüssel überprüfen. Posch: »Diese Unterschrift ist dann bei Behörden genauso gültig wie bei einer Bank oder im Reisebüro. Künftig wird man beim Online-Shopping im Internet mit der digitalen Unterschrift Einkäufe bestätigen. Auch eine Bestellung in einem Baumarkt kann mit der digitalen Signatur unterzeichnet werden.«

Eine digitale Unterschrift wird für zwei Jahre zwischen 20 und 30 Mark, 120 und 200 Schulung kosten. Firmen und Unternehmer müssen etwa 200 Mark für eine zwei Jahre gültige digitale Unterschrift bezahlen. Die Zweijahresfrist hat einen simplen Grund: Die Verschlüsselungstechnik könnte in dieser Zeit überholt sein. Die derzeit übliche, aber auch knackbare Schlüssellänge beträgt 512 Bit. Schlüssel, die länger sind als 1000 Bit, sind derzeit noch nicht knackbar - nicht einmal von der amerikanischen NSA, schon gar nicht vom deutschen BND oder dem österreichischen HNA.

# Banken mit Verbindungen

**> Wie uns die Banken im Griff haben.**

**> Warum für die Banken ein Beamter mehr wert ist ais ein Arbeiter, aber weniger als ein Angestellter.**

**> Wer auf der »schwarzen Liste« der Banken steht.**

**> Warum Autofahrer mit schwarzen und roten Autos bei Versicherungen bald höhere Tarife zahlen müssen.**

**> Wie Versicherungen künftig Haushaltsversicherungs-Betrüger ausfindig machen.**

**> Wie man den Bürger anhand der Kontobewegungen charakterisiert.**

**> Wie gefährlich Online- und Telefonbanking ist.**

**> Wie gut die Kooperation der internationalen Zöllner funktioniert.**

## Auf der Jagd nach Versicherungsbetrügern

Der 15. August 1997 war ein schwarzer Tag für die Familie P. in Tirol: Zuerst hatte Alois P. mit Ewald P. eine Kollision, am Nachmittag fuhren Josef P. und Roman P. zusammen. In beiden Fällen waren die Autos stark beschädigt, aber zum Glück kam die Kfz-Haftpflichtversicherung des jeweils anderen für die Schäden auf. Zumindest waren die P.s davon überzeugt. Was die Tiroler nicht wußten, war, daß in einem Zentralcomputer in Wien alle Kfz-Versicherungsfälle gespeichert, verglichen und Ungereimtheiten oder »Zufälle« aufgelistet werden. Unfälle, an denen Autos von Namensgleichen beteiligt sind, sind solche »Zufälle«, auf die die

Betrugsreferenten der Versicherungsanstalten - auch »rote Referenten« genannt - online zugreifen können.

Auch bei Simon A. war ein solcher Datenabgleich erfolgreich. Er hatte am 29. Juli 1997 einen Unfall verursacht. Zwei Wochen später fuhr ihm in seiner Heimatgemeinde zufällig ein Traktor in seinen Wagen. Ob der Wagen zu diesem Zeitpunkt schon repariert war, ist fraglich, sogar eher unwahrscheinlich, wenn man bedenkt, daß Traktoren, Lastwagen und Motorräder nicht ins Malus kommen. Auch wenn diese Auffälligkeit alleine noch lange kein Beweis für einen Betrug ist, können Betrugsreferenten den Fall kontrollieren.

So wie die Kollision von Franz V. und Friedrich L., die sich am 8. August 1997 zugetragen hatte: Beide hatten Glück, niemand wurde verletzt, nur Sachschaden. So wie eineinhalb )ahre zuvor. Damals, am 8. Dezember 1995, waren auch beide mit ihren Fahrzeugen zusammengestoßen.

Seit 1988 steht den österreichischen Versicherungen im Versicherungsverband das Zentrale Informations-System (ZIS) zur Verfügung. Im ZIS werden alle Kfz-Haftpflicht- und Kaskoschäden gespeichert. Neun Millionen Kfz-Versicherungsfälle sind in der Datenbank ständig gespeichert und werden laufend miteinander abgeglichen.

Durch das rapide Ansteigen des Versicherungsbetruges wurde das ZIS notwendig. Schätzungen gehen davon aus, daß den Versicherungen durch Betrug pro Jahr in Österreich 5 bis 7 Milliarden Schilling Schaden entstehen.

Jeder Unfall oder Kfz-Diebstahl ist genau dokumentiert- Name des Verursachers, des Geschädigten, Kennzeichen, Fahrgestellnummer sowie Zeugen. Professionelle Versicherungsbetrüger treten nämlich gegenseitig als Zeugen auf. Auffällig sind auch die Kfz-Diebstähle bei Leasing-Autos. »Meistens werden sie kurz vor Ablauf des Leasingvertrages gestohlen«, bestätigt ein Insider. »Vermutlich haben die Autos dann zu viele Kilometer auf dem Tachometer.«

Die Suche nach Betrügern ist ein interessantes Spiel, denn das ZIS kann nach verschiedenen Kriterien abgefragt werden. Jedes Auto, das in den vergangenen drei Monaten zwei und innerhalb eines Jahres fünf Unfälle hatte, scheint auf dem Bildschirm auf. Jeder Autofahrer, der innerhalb eines Monats zuerst Verursacher und dann Geschädigter war, wird aufgelistet. Ebenso Namenspaare,



sämtliche Totalschäden, für die Ablöse kassiert wurde, sowie Kfz-Diebstähle.

Für die Versicherungsbranche ist das ZIS ein Erfolg. Bereits 1995 konnten die fünf größten Versicherungen mit Hilfe von ZIS insgesamt 900 Versicherungsbetrügereien aufklären und sich 58 Millionen Schilling ersparen. 1997 wurden beinahe 1 500 Fälle aufgedeckt und dadurch beinahe 100 Millionen erspart.

Was bei den Österreichern ZIS, heißt bei den Deutschen UNIWAGNIS. Der Gesamtverband der deutschen Versicherungswirtschaft (GDV) in Hamburg hat seit 1993 mit UNIWACNIS ein Verfahren, in dem dubiose Schadensfälle gemeldet werden.

Anders als in Österreich haben die deutschen Versicherungen bei UNIWAGNIS aber keinen Online-Zugriff. Schäden werden mittels Formular, Magnetband oder in Listenform gemeldet. Im Gesamtverband werden diese Informationen in das System eingespielt und an die Versicherungen weitergeleitet. Die etwa 600 deutschen Versicherungen müssen dabei nach einem Kriterienkatalog und nach einem Punktesystem vorgehen. Sind 60 Punkte erreicht, muß der Schaden gemeldet werden. UNIWAGNIS gleicht nicht nur bereits passierte Schadensfälle ab, sondern auch jeden Antrag auf eine Kfz-, Transport-, Lebens- oder Hausratsversicherung mit den gespeicherten Daten.

Jeder Totalschaden mit einem Miet-Lkw muß gemeldet werden, Kollisionen, bei denen einander Verursacher und Geschädigter kennen, Unfälle zu ungewöhnlicher Zeit an einem ungewöhnlichen Ort. »Wenn z, B. eine Großmutter in der Nacht von Samstag auf Sonntag auf einer einsamen Landstraße mit ihrem Daimler einen Unfall verursacht, dann sollte der Fall automatisch gemeldet werden«, sagt Olaf Harms vom GDV.

Von den 9 Millionen Kfz-Schadensfällen in Deutschland gelangen aber nur jene 1,5-2 Millionen in die Datenbank, die verdächtig sind. »Es fallen Betrügereien durch den Kost«, ist auch Harms überzeugt. Aber die gewaltige Menge von Schadensfällen pro Jahr würde sonst die Speicherkapazität des Computers sprengen, da die Daten fünf Jahre gespeichert werden müssen. Im CDV rechnet man damit, daß auch diese Datenmengen in einigen Jahren gespeichert und durch noch bessere Analyseprogramme abgeglichen werden können. Im Kfz-Bereich gehen Praktiker von 5-20 Prozent Mani-

pulation aus. »Diesen Prozentsatz könnte man erheblich senken«, erklärt Harms. Den deutschen Versicherungen entsteht durch Betrug ein Schaden von mehreren Milliarden Mark.

## Das Loch im Teppich und das kaputte Handy

»Ich brenn dir ein Loch in den Teppich, dafür setzt du dich auf meine Brillen.« In Österreich wird dem Kavaliersdelikt Haushaltsversicherungsbetrug seit Anfang 1998 der Kampf angesagt. Unbeachtet von der Bevölkerung wurde das ZIS auf den Haushaltsbereich ausgeweitet. Im deutschen UNIWAGNIS wurde dieser Schritt bereits 1997 getan. In Österreich beträgt der Schaden, der durch Haushaltsfälle entsteht, geschätzte 500 Millionen Schilling, in Deutschland ist es eine Summe von 5-10 Milliarden Mark. »Besonders oft werden Brillen, Herdplatten und Verglasungen kaputt«, erzählt ein Insider. »Auch Handys fallen ziemlich oft von einem Tisch oder einem Schrank herunter. Vor allem dann, wenn neue auf den Markt kommen.« Künftig werden Fälle, bei denen der Geschädigte in einem bestimmten Zeitrahmen auch Verursacher ist, ausgeworfen und von den »roten Referenten« kontrolliert. Auch ein Doppelinkasso wird schwieriger, denn im Sach-ZIS, wie das System bezeichnet wird, werden auch Typen- und Seriennummern eingetragen.

## 10 Punkte für Beamte

Wer ist mehr wert? Ein Beamter oder ein Arbeiter? Ein Jugoslawe oder ein Türke? Ein Familienvater oder ein Geschiedener? Deutsche und österreichische Banken wissen die Antwort - Credit-Scoring nennt sich die Punktevergabe, bei der Kreditantragsteller typisiert und katalogisiert werden. Wer einen Kredit beantragt, wird, ohne es zu wissen, mit Punkten bewertet. Für Nationalität gibt es Punkte, für Alter (28 ist besser als 18}, Beruf (Anwalt ist besser als Angestellter), Wohnort (Villengegend ist besser als Arbeiterviertel), Verdienst und verschiedene andere Eigenschaften.



»Wer ist der bessere Kunde?« fragt der Direktor des Kreditschutzverbandes (KSV), Johannes Nejedlik, und zitiert ein Beispiel. »Ein Gastarbeiter, der 35000 Schilling verdient und zwei Kinder hat, oder ein Gastarbeiter mit 17000 Schilling Gehalt und drei Kindern?« Für die Banken natürlich letzterer. Bei einem Arbeitsplatzverlust findet er mit seinem Gehalt leichter wieder einen Job. Beamte stehen bei den Banken höher im Kurs als Arbeiter, da durch die Pragmatisierung ein Jobverlust beinahe ausgeschlossen werden kann. Übertroffen werden sie allerdings von den Angestellten, da bei diesen das Lohnniveau meist höher ist.

Auch verheiratete Kreditantragsteller werden von den Banken besser beurteilt als geschiedene: Weil eine Scheidung oft mit unvorhersehbaren finanziellen Folgen verbunden ist.

Auch Menschen, die oft einen Job wechseln, bekommen weniger Punkte: Ein oftmaliger Jobwcchsel steht für Unsicherheit und Inkonsequenz.

Auch Männer oder Frauen, die an einer Krankheit leiden oder offensichtlich schwerer krank sind, erhalten einen Punkteabzug: Wer soll den Kredit bei Arbeitslosigkeit zurückzahlen?

»Im Prinzip geht es darum, gute und schlechte Kunden voneinander zu trennen«, erklärt ein Bankenvertreter einer Privatkreditabteilung. »Credit-Scoring baut darauf auf, daß schlechte und gute Kunden gewisse Eigenschaften haben, die sich bei anderen Kunden wiederholen.« Einfach ausgedrückt: gute Kunden haben Eigenschaften A bis |, schlechte Eigenschaften K bis Z. »Die Scoring-Systeme wurden aber nicht geschaffen, um Kunden zu durchleuchten, sondern um sie vor unnötigen und unvorhersehbaren Folgen zu schützen«, meint KSV-Direktor Nejedlik. Durch diese Punktehewertung könnten Kunden davor bewahrt werden, daß sie einen Kredit in einigen Jahren nicht mehr zurückzahlen können.

Credit-Scoring funktioniert ähnlich wie etwa der Fragebogen, den jene ausfüllen müssen, die nach Australien auswandern möchten: Wer Englisch spricht, erhält Punkte, wer einen Beruf ausübt, der in Australien benötigt wird, bekommt Punkte, wer dort lebende Verwandte hat, bekommt ebenfalls Punkte. Wird eine bestimmte Punktezahl erreicht, wird der Einwanderung zugestimmt.

Ein ähnliches Punkteschema ist bei den Banken üblich: 100 Punkte können maximal erreicht werden. Bis 90 ist man in der grünen

Zone - der Kredit wird anstandslos genehmigt, ebenso wie in der gelben Zone. Bei der roten Zone kann der Filialleiter oder Bankdirektor aufgrund eines »persönlichen Eindrucks« selbst entscheiden, ob der Kredit genehmigt wird oder nicht. Wer in der »Sperrzone« landet, hat keine Chance auf einen Kredit.

In der Vergangenheit haben sich die Banken ihre Scoring-Systeme selbst zurechtgebastelt. Erste Versuche, Kunden zu typisieren, gab es bereits in den 70er Jahren. Mitte der 80er wurden die ersten Punktesysteme bankintern realisiert. Seit einigen Jahren bieten eigene internationale Anbieter ihr Know-how an (die meisten kommen aus den USA). In Österreich hat die Bank Austria gemeinsam mit dem Kreditschutzverband 1996 die Firma Score-Consult GmbH gegründet, die Credit-Scoring-Systeme vertreibt. Scoring hat sich zum Trend entwickelt, da immer mehr Unternehmen ihre Kunden zu schematisieren und besser zu beurteilen versuchen.

Scoring ist in den Vereinigten Staaten eine gängige Methode, die nicht nur von Banken, Versicherungen und Kreditkartenunternehmen genutzt wird. In den USA sind im Versandhandel, aber auch in normalen Geschäften Kaufwahrscheinlichkeits-Scorings in Verwendung, die berechnen sollen, ob Interessierte zu Kunden werden könnten.

Eines jener Bankinstitute, die in Deutschland schon seit Jahren erfolgreich mit Scoring-Systemen arbeiten, ist die CitiBank. Dort gibt es mehr als zehn verschiedene Scorings für jede Kundengruppe. Man ist der Meinung, daß es nicht nur auf den Kunden selbst, sondern auf die Art des Kredits ankommt. Bei der CitiBank gibt es eigene Scorings für Inländer-, Gastarbeiter- oder Wohnungskredite. Übrigens werden auch Ausländer unterschiedlich beurteilt. Türkische Staatsbürger, so bestätigen Bankenvertreter, zeichnen sich durch eine gute Zahlungsmoral aus und bekommen deshalb eine höhere Punkteanzahl.

Immer stärker verbreitet ist auch das sogenannte Behaviour-Scoring, das Bewerten des Kundenverhaltens. Bei dieser Variante werden bestimmte Merkmale des Kunden bewertet - wann er seine Erlagscheine zahlt, pünktlich oder verspätet. Welche Bankprodukte er besitzt, Bausparvertrag oder Anleihen. Ob er risikofreudig ist und auf Aktien oder andere Wertpapiere setzt, etc.



## Die geheimen Datenbanken der Banken

Der Kontoauszug ist sehr informativ. Es sind nicht bloß die Ziffern, die Aufschlug über einen Kunden geben, sondern es sind die Wörter, die vor den Geldbeträgen stehen. Für die Banken sind die Kunden ein offenes Buch. Anhand der Kontobewegungen läßt sich ein Kunde relativ genau charakterisieren.

Die Bankomat-Behebungen verraten, wann er wo eingekauft hat. Daueraufträge für die Telekom, für das Mobilfunkunternehmen und für das Elektrizitätswerk lassen erahnen, ob Herr X viel telefoniert, ob er viel Strom verbraucht, folglich oft zu Hause ist oder eher selten. Das Gehalt ist bekannt, auch die Beträge, die er regelmäßig auf sein Sparbuch bzw. auf sein Kreditkonto abbuchen läßt. In der Bank weiß man, daß er geschieden ist, da er Alimente an seine Frau überweist. Der Höhe nach dürfte er Alimente für zwei Kinder zahlen. Herr X fährt einen teuren Leasingwagen, steht öfter im Parkverbot, weil er ständig Erlagscheine einzahlen muß. Seine Hobbys sind Tennis - jeden Monat läßt er seinen Mitgliedsbeitrag auf das Konto eines Tennisvereins überweisen. Er ist Bezieher einer Lexika-Ausgabe, »Premiere«-Seher und öfter im Ausland. Dort hebt er mit seiner EC-Karte Geld ab.

Die Banken haben schon längst erkannt, daß die Informationen, die sie über ihre Kunden haben, geschickt für Marketingzwecke genützt werden können. Da es aber praktisch unmöglich ist, daß sich ein Bankbeamter alle Kundendaten merkt, steht ihm im Bankcomputer die inoffizielle Kundendatei zur Verfügung, in der alle »Sekundärmerkmale« der Kunden aufgelistet sind - Hobbys, Sparformen etc. Offiziell werden diese Informationen nur gesammelt, um ein besseres Sevice anbieten zu können und auf die »individuellen Kundenwünsche« besser eingehen zu können.

Wer den Mitgliedsbeitrag für seinen Fitness-Club von seinem Konto überweisen läßt, darf sich nicht wundern, wenn ihm plötzlich sein Bankenbetreuer eine Unfallversicherung anbietet. Wessen Leasingvertrag ausläuft, der könnte bald mit einem neuen Angebot von seiner Hausbank konfrontiert sein. Kein Zufall sind auch Fragen, oh man einen Bausparvertrag abschließen möchte.

Von diesen Methoden sind Datenschützer nicht begeistert, denn »Tatsachen des Giroverkehrs sind Gegenstand des Bankgeheimnis-

ses«, hat der österreichische Oberste Gerichtshof (OGH) bereits am 25. Februar 1992 entschieden (4 Ob 114/91). »Der Anspruch des Kunden auf Wahrung des Bankgeheimnisses wird verletzt, wenn geheimzuhaltende Tatsachen innerhalb ein und derselben Bank an Personen weitergegeben werden, die zwar nach außen selbst geheimhaltungspflichtig, mit der Sache des Kunden aber in keiner Weise befaßt werden.« Basis dieses Urteils ist eine Klage gegen eine österreichische Bausparkasse.

Jede der fünf österreichischen Bausparkassen arbeitet mit bestimmten Kreditunternehmen zusammen. Da jedes Institut Verträge ihres Partners forciert, wurden die Bankangestellten von der Leitung der Bank aufgefordert, »Fremdbausparer« festzustellen und diese zu einem Vertrag mit der hausinternen Bausparkasse zu überzeugen. Was die Bank den Angestellten empfahl, sollte nicht nur Daten-Schützer erschüttern. Schwarz auf weiß war in der bankinternen Broschüre zu lesen: »Fremdbausparer: sie müssen rasch identifiziert werden. Wenn sie ihre Bauspareinlagen über Dauerauftrag oder Einziehungsauftrag leisten, werden sie EDV-mäßig registriert. Die beiden Sektor-Rechenzcntren stellen allen X-Banken EDV-Listen über diese Zielgruppen zur Verfügung. Andere Fremdbausparer müssen entweder bei Zahlschein-Einzahlungen erkannt oder im persönlichen Beratungsgespräch festgestellt werden. Wichtig ist jetzt das Ablaufdatum des Fremdsparvertrages vorzumerken und den Kunden bereits ein Jahr davor anzusprechen.« Für den OGH lag sowohl eine Verletzung eines Bankgeheimnisses wie auch eine Verletzung des Datenschutzgesetzes vor.

Trotz dieses Urteils sind aber Insider überzeugt, daß derartige Methoden noch immer gang und gäbe sind: »Nur ist halt niemand mehr so blöd und gibt da etwas Schriftliches heraus. Heute werden solche Aufträge nur noch mündlich erteilt.«

## *Rotes Auto: höhere Prämie*

Noch mehr Informationen als den Banken stehen den Versicherungen zur Verfügung. Sie kennen meist nicht nur die finanziellen Verhältnisse ihrer Kunden - beim ersten Verkaufsgespräch geben



die Interessenten oft freiwillig an, was sie verdienen, damit die Prämie besser berechnet werden kann. Versicherungen haben auch heikle Daten wie Gesundheitszustand, Operationen etc. gespeichert.

Alles offiziell, versteht sich. Wer eine Lebensversicherung abschließt, kommt nicht darum herum, eine ärztliche Untersuchung dem Vertrag beizulegen. Wer sich weigert - oft ist dies gar nicht möglich -, zahlt eben höhere Prämien. Diese ärztlichen Attests sind mitunter sehr detailliert. Detaillierter als notwendig. Da Versicherungen Risiken ausschließen möchten, werden die Kunden durchleuchtet.

Beim Abschluß eines Versicherungsvertrages sind sich wohl viele nicht bewußt, was sie von sich selbst verraten. Abgesehen von den persönlichen Daten, werden auch Informationen über das Umfeld gesammelt- Frau, Kinder etc.

Interessant sind auch die diversen Rabatte, die Versicherungen bei Abschluß einer Kfz-Versicherung gewähren. Mehr als 100 verschiedene Rabattmöglichkeiten stehen Kunden zur Auswahl, jede einzelne verrät Details über den Kunden.

Es gibt Rabatte für Prokuristen, Geschäftsführer, Polizisten, Bahnbedienstete oder auch Soldaten. Es werden Lady-Rabatte angeboten, Vergünstigungen, wenn auch andere Familienmitglieder eine Versicherung haben oder eine bestimmte Anzahl von Kfz versichert haben. Es gibt aber auch Versicherungsinstitute wie etwa die Basler, Donau oder Volksfürsorge Jupiter Versicherung (VJV), bei denen »Männer am Steuer« bei einem Unfall mehr Schadenersatz leisten müssen als Frauen.

Wer günstige Prämien zahlen möchte, sollte in Zukunft auf PS-starke Modelle verzichten. Fahrer mit leistungsstarken Fahrzeugen müssen bei einigen Instituten, wie etwa der Interunfall oder der VJV bis zu 30 Prozent höherer Prämien zahlen. Auch die Farbe des Wagens wird künftig entscheidend sein. Schon jetzt gibt es Versicherungen, die überlegen, daß Lenker von roten und schwarzen Pkw um 10 Prozent höhere Prämien zahlen müssen. Basis dieser Verteuerung ist eine 1997 präsentierte Studie, wonach Lenker von schwarzen und roten Fahrzeugen die aggressiveren Autofahrer und deshalb »unfallanfälliger« sind.

## »Schwarze Listen«

Sie sind »unerwünscht« an den Kassenschaltern, erhalten keinen Kredit- bei keiner Bank in ganz Österreich -, und meist wird ihnen auch ein Konto verweigert. Die Existenz der UKV, wie sie genannt wird - »Unerwünschte Kontoverbindung« - wurde jähre-, jahrzehntelang heftig dementiert, Schalterbeamte hüllten sich in kryptisches Schweigen, und auch der Finanzminister schaute bewußt weg, obwohl das Finanzministerium verpflichtet wäre, das Bankgeheimnis zu kontrollieren. Die meisten Österreicher wissen bis heute nicht, daß es eine solche »schwarze Liste« gibt.

»Auf dieser Liste zu stehen kann die Existenz eines Menschen ruinieren«, bestätigt der ehemalige Konsumentenschützer im Bundeskanzleramt, Hans-Peter Lehofer. Denn mitunter kommen auch Unschuldige auf diese Liste. Das Hauptproblem, das von Daten- und Konsumentenschützern kritisiert wird: Man wird nicht informiert, wenn man auf die UKV gesetzt wird. Wer aber auf der UKV steht, dem wird meist auch ein Gehaltskonto verweigert. Das wiederum kann Probleme am Arbeitsplatz bzw. bei der Jobsuche mit sich bringen. Forderungen österreichischer Konsumentenschützer, Betroffenen wenigstens ein Haben-Konto zu ermöglichen, werden von vielen Banken abgelehnt. Inoffizielle Begründung: mit reinen Haben-Konten ist für Banken nichts zu verdienen.

Franz O. steht auf dieser UKV. Der Salzburger hatte 1977 durch ein Hochwasser sein Haus verloren. Entschädigung erhielt er nicht, also häuften sich Schulden an. Nach Problemen mit einem Geschäftspartner wurde er von einem Raiffeisen-Bank-Direktor auf die UKV gesetzt. Verständigt wurde er von diesem Schritt nicht, erst als auch Kreditanträge bei anderen Banken abgelehnt wurden, wurde ihm bewußt, daß er auf einer »schwarzen Liste« stehen mußte.

Bei einer parlamentarischen Anfrage am 15. Mai 1996 (Nr. 329/J), beantwortete der damalige Finanzminister Viktor Klima die Vereinbarkeit der UKV mit dem Datenschutzgesetz folgendermaßen: »Insoweit die an der Liste teilnehmenden Kreditinstitute von ihren Kunden die entsprechenden Zustimmungen gemäß § 38 Abs 2 Z 5 Bankwesengesetz einholen bzw. eingeholt haben, ist das Führen einer solchen Liste mit dem Bankgeheimnis rechtlich vereinbar.«

Franz O. gab in einer Sachverhaltsdarstellung an, nicht verständigt worden zu sein. In einer parlamentarischen Anfrage der Grünen vom 27. November 1996 (1490/j) machte der Grün-Abgeordnete Rudi Anschober weitere zwei Fälle von Betroffenen namhaft, die nicht über den schwarzen Punkt informiert worden waren.

In ganz Österreich stehen 200000 auf der UKV. »Das ist gerade jene Anzahl, die laut internationalen Studien problematisch wird«, erklärt man beim KSV »Mit 8 bis 12 Prozent der Kreditkunden bekommen die Banken Probleme.«

»Die UKV wird auch als Druckmittel verwendet«, erklärt Konsumentenschützer Lehofer und schildert einen Vorfall, bei dem sich ein Geschäftsmann beim Bankdirektor über den seiner Meinung nach zu hohen Kreditzinssatz beschwerte. »Die Drohung des Direktors: >Ich setze Sie auf die Liste< hat den Geschäftsmann rasch wieder verstummen lassen.«

Die Existenz der UKV wurde in den vergangenen Jahren auch aus einem anderen, ganz simplen Grund bestritten: sie widerspricht dem Rechtsgrundsatz der Unschuldsvermutung, da ein Bankdirektor, ein Filialleiter über Recht und Unrecht entscheidet und einen Kunden etwa als Kreditkartenbetrüger auf die Liste setzen läßt, ohne daß es dafür ein richterliches Urteil gibt. Lehofer: »Die UKV basiert auf Vermutungen, auf unbewiesenen Behauptungen.« Nur jene Bank, die den Kunden auf die Liste gesetzt hat, kann diesen auch wieder herauslöschen.

Die UKV gibt es in Österreich bereits seit 1. Dezember 1965. Der Verband Österreichischer Banken und Bankiers fädelte diese Vereinbarung ein, die damals zwischen Creditanstalt-Bankverein (CA), der Länderbank, dem Österreichischen Credit-Institut fÖCI), der Bank für Arbeit und Wirtschaft (BAWAG), der Girozentrale und Bank der österreichischen Sparkassen AG, der Ersten, der Zentralsparkasse, der Genossenschaftlichen Zentralbank und der Zentralkasse der Volksbanken geschlossen wurde. »Die vorgenannten Kreditunternehmungen kommen überein, sich gegenseitig zu verständigen, wenn von einer ihrer Stellen die Kontoverbindung mit einem Kunden wegen der wiederholten Ausstellung von ungedeckten Schecks aufgelöst wird«, stand in einem Rundbrief, der am 7. Dezember 1965 ausgeschickt wurde. 20 Tage später umfaßte die Liste der Institute, die sich gegenseitig mit negativen Kundeninformationen versorgen, 39 österreichische Banken.

Erst 30 Jahre später wurde die Existenz dieser geheimen »schwarzen Liste« bekannt, die mittlerweile von sämtlichen Bankinstituten mit Daten beliefert wird. Auch sind nicht nur Scheckkartenbetrüger auf der UKV zu finden, sondern mitunter »Unschuldige«. Wer in der UKV steht, ist mit einem Negativsymbol behaftet. AUF bedeutet Scheckkarten- bzw. Bankomatmißbrauch, VBC ist das Kürzel für Versuchter Betrug, G steht für Girokontoüberziehung, C für Kreditkartenüberziehung, der Buchstabe B heißt, daß der Betroffene Bürge ist.

Seit 1996 gibt es Versuche, die UKV zu legalisieren, »denn eigentlich hilft sie ja dem Kunden«, meint ein Banker. »Wir bewahren Kunden davor, daß sie unvermutet in eine finanzielle Krise schlittern.« Mit der Verwaltung der Liste soll der Kreditschutzverband betraut werden. Die UKV könnte in den KKK (Klein-Kreditnehmer-Kataster bzw. Klein-Kreditnehmer-Kartei) eingebaut werden.

## Die legale Kartei der Schuldner

Wer einen Kredit beantragt, wird immer mit der Frage des Bankangestellten konfrontiert: »Haben Sie schon irgendwo einen Kredit laufen?« Die Frage ist eine reine Formsache, denn Bankangestellte informieren sich ohnehin im Computer, wenn es darum geht, einen Kredit zu genehmigen. Neben dem schon erwähnten Credit-Scoring sind vor allem jene Informationen interessant, die in Österreich in der Klein-Kreditnehmer-Kartei (KKK) bzw. Klein-Kreditnehmer-Evidenz (KKE) des Kreditschutzverbandes (KSV) bzw. in Deutschland bei der Schutzgemeinschaft für allgemeine Kreditsicherung (SCHUFA) gespeichert sind.

In der SCHUFA-Kartei bzw. KKK sind all jene gespeichert, die in Deutschland bzw. Österreich einen Kredit laufen haben. Früher waren die Informationen auf Microfilm gespeichert, jetzt gibt es Online-Verbindungen, telefonische oder auch schriftliche Auskünfte.

Die beiden Dateien werden aber nicht nur von den Banken mit Material »gefüttert«, sondern auch von Versicherungen, Leasingunternehmen und Versandhäusern. Aber es sind nicht nur laufende Kreditverträge aufgelistet nach Höhe, Vertragsbeginn und Ende.



»Mitunter stehen in der SCHUFA Kredite, die noch gar nicht vergeben wurden«, ärgert sich auch der Direktor eines führenden Unternehmens in Darmstadt. Bei einem Besuch in der SCHUFA-Zenrrale in der Kronprinzenstraße in Wiesbaden forderte er Akteneinsicht. »Zu meinem Erstaunen war bereits ein ßausparkredit als vergeben gespeichert, der noch gar nicht vergeben war.« Eine übliche Methode, rechtfertigt man sich bei der SCHUFA. Die allerdings negative Folgen für einen Kunden haben kann, kontern Datenschützer. Abgesehen davon, daß jemand als Schuldner bezeichnet wird, obwohl er keiner ist, könnte dieser Eintrag das Verhandeln mit mehreren Banken, wenn es darum geht, den günstigsten Zinssatz für einen Kredit zu erhalten, entscheidend erschweren.

Die SCHUFA-Liste und die KKK sind in der heutigen Zeit zu einer unverzichtbaren Informationsquelle geworden. Wer ein Handy anmelden möchte, über den werden im Rahmen der Bonitätsprüfung Informationen über die SCHUFA bzw. über den KSV eingeholt. Jeder Leasingvertrag, jeder Antrag auf eine Kreditkarte wird zuerst mit diesen Listen abgeglichen.

Grundsätzlich sind in der SCHUFA-Listc und in der KKK Kredite mit Betrag, Ratenzahl und Ratenbeginn, bzw. mit Betrag, Laufzeitbeginn und Laufzeit, gespeichert. Hypothekarkredite, Leasing-Geschäfte mit Leasinghöhe, Mietdauer und Beginn, Bürgschaften, Ausgabe von Kreditkarten und Girokonten.

Auch jedes »nichtvertragsgemäße« Verhalten von Kunden, sogenannte negative Daten, werden gespeichert: gerichtliche Maßnahmen wie Sach- oder Gehaltsexekutionen, Pfändungen etc.

Anders als in Österreich wurde in Deutschland das Archivieren von Vergehen wie Scheck- oder Kreditkartenmißbrauch auf eine legale Basis gestellt. Diese Informationen sind Teil einer SCHUFA-Auskunft.

Etwa 50 Millionen Deutsche sind bei der SCHUFA aktenkundig, insgesamt existieren über die Deutschen 220 Millionen Eintragungen. In Österreich sind 1,5 Millionen Menschen auf der KKK gespeichert.

Normalerweise wird jeder Eintrag bis drei Jahre nach der Tilgung eines Kredits gespeichert. »Langjährige Erfahrungen bestätigen, daß Merkmale über ordnungsgemäß erledigte Kredite den betreffenden Kunden als kreditwürdig ausweisen und damit die beste Empfeh-

lung für die Vergabe neuer Kredite sind«, meint SCHUFA-Geschäftsführer Wulf Bach. Dieser Argumentation können sich nicht alle anschließen, da man plötzlich mit einer Frage am Bankschalter konfrontiert sein könnte, warum man denn schon wieder einen Kredit benötigt.

## Kooperationen mit und ohne Grenzen

Offiziell wird heftig dementiert, denn diese Methoden seien völlig unmöglich, da ungesetzlich. Wer mit Banken um den Zinssatz eines Kredits verhandelt, sollte nicht Banken aufsuchen, die Partner sind oder in sonst irgendeiner Form zusammenarbeiten.
Wer um einen günstigen Kredit feilscht, sollte nicht bei der Bank AB ankündigen, daß der Kredit bei der Bank AC günstiger ist. Bevorstehende oder bereits beschlossene Fusionen - und die sind in Österreich und Deutschland derzeit aktuell - machen aus zwei Geldinstituten ein System, das sich nicht bekämpft, sondern kooperiert.
Dort, wo es den Banken nützt, wird gelegentlich auch über die Firmengrenzen hinaus kooperiert, wie das Beispiel der SCHUFA-Liste oder der KKK zeigt (wobei in beiden Datenbanken zwar die Kredithöhe gespeichert wird, nicht aber, bei welchem Kreditinstitut).
Dort, wo es den einzelnen Banken Schaden bzw. ungewollt Konkurrenz bringen würde, wird gegeneinander gearbeitet. Banken weigern sich mitunter, ihre Informationen in einer Datenbank zusammenzuführen, wie das erwähnte Beispiel der fünf österreichischen Bausparkassen zeigt. Anders als in Deutschland, wo der Bausparvertrag jährlich beim Finanzamt eingereicht wird, erhält jeder Bausparer die staatliche Prämie automatisch auf seinem Bausparkonto gutgeschrieben.
Das erlaubt Österreichern theoretisch - Experten im österreichischen Finanzamt sind sogar davon überzeugt, daß es praktische Nutzer gibt -, fünf Bausparverträge gleichzeitig abzuschließen und fünfmal die staatliche Prämie zu kassieren. Vorausgesetzt, daß der Kunde nicht die monatlichen Einzahlungen mittels Dauerauftrag von seinem Konto überweisen läßt, sondern die Beiträge mit Post-Erlagscheinen einzahlt.



Bei den derzeit niedrigen Zinssätzen für Spareinlagen sind 6 Prozent, wie die Bausparverträge effektiv verzinst werden, durchaus lukrativ. Zwar gab es schon Bestrebungen, alle Bausparer in einer Datenbank zusammenzuführen, um sie so unter Kontrolle zu haben. Die Bausparkassen wehren sich allerdings, da der Konkurrenz dadurch ihre internen Daten bekannt würden.

## Wenn die Bank das Telefon ist

Obwohl die Banken immer wieder betonen, daß Telefon-, Home-, Telebariking oder Cybermoney absolut sicher sind, sind die Experten des Bundesamts für Sicherheit in der Informationstechnik (BSI) in Bonn anderer Meinung.
Voll im Trend liegt Homebanking, bei dem die Bankgeschäfte vorn Privat-PC abgewickelt werden können. Der Kunde erhält von der Bank neben der Benutzerkennung und seinem Paßwort auch 100 Transaktionsnummern (TANS). Bei jeder Überweisung muß eine dieser Nummern verwendet werden. Noch bevor die 100. aufgebraucht ist, werden von der Bank neue ausgegeben. Da diese TANS praktisch die Unterschrift ersetzen, müssen sie sorgfältig aufbewahrt werden, was manchen Kunden bei diesen nüchternen Zahlenkolonnen etwas schwerfällt. »Keinesfalls darf eine solche Liste irgendwo herumliegen«, warnt die BSI-Expertin lsabel Münch. Wie die Vergangenheit gezeigt hat, wurden bereits bei Einbruchsdiebstählen solche Listen erbeutet und auch verwendet. »Problematisch kann es auch dann werden, wenn Kunden ihre TANS im PC speichern, diese Liste nicht absichern und für jeden, der Zugriff zum Computer hat, zugänglich machen«, sagt Münch. Wenn frische TANS zurückgewiesen werden, sollten sofort die letzten Transaktionen kontrolliert werden, denn es ist bei Homebanking sogar möglich, daß sich jemand im Keller eines Wohnhauses an die Telefonleitung klemmt, die Transaktion mitverfolgt und manipuliert.
An einem neuen Sicherheitsstandard arbeiten deutsche Banken. Beim Homebanking-Computer-Interface erhalt der Kunde ausschließlich mit seiner Chipkarte Zugriff, was den Sicherheitsstandard enorm erhöhen wird. Das wiederum bedeutet, daß jeder

Haushalt entweder mit einem Chipkarten-PC oder mit einem Chipkarten-Lesegerät ausgestattet sein wird. Man wird dann nicht nur mit seiner Chipkarte Transaktionen veranlassen können, sondern auch die »elektronische Geldbörse« auffüllen bzw. den Kontostand auf der Telefonwertkarte kontrollieren können. Wie ein solches System aussehen könnte, hat der Münchner Karten- und Banknotenhersteller Giesecke & Devrient gezeigt. »Chipchecker« nennt sich der schlüsselanhängergroße Taschenkartenleser, in dem einfach eine Chipkarte eingeschoben wird und der dem Kunden den aktuellen Kontostand des Chips, die letzten drei Ladungen und die vergangenen 15 Zahlungen auflisten kann.

Weiler verbreitet - da es auch von jenen genutzt werden kann, die mit Computer keine Erfahrung haben - ist Telefonbanking. Dabei ruft der Kunde seine Bank an, um telefonisch Überweisungen zu veranlassen, seinen Kontostand abzufragen etc. Hier ortet die BSI-Expertin gleich drei Probleme. Zum einen werden bei den Paßwörtern meist »Trivial-Begriffe« verwendet, die leicht erraten werden können. Nach einer Studie der Quelle Bank sind die Paßwörter zu 39 Prozent Personennamen, zu 16 Prozent Städte- und Ländernamen und zu 8 Prozent Sternzeichen. Nur 4 Prozent der Kunden waren vor illegalen Angriffen relativ sicher - sie hatten Paßwörter gewählt, die nicht im Duden standen.

Problem zwei ist die »Kundenfreundlichkeit« der Banken. Jene Institute, die noch auf die Mensch-Mensch-Kommunikation setzen - der Kunde ist persönlich mit einem Bankangestellten verbunden -, helfen Kunden mitunter bei der »Paßwortfindung« weiter. Bei Äußerungen wie »Wie war schnell das Paßwort?« oder »Jetzt fällt's mir nicht ein«, helfen die Bankbediensteten manchmal beim Raten mit- »Könnte es nicht ein Tiername sein?« oder »Nur soviel, es ist eine Automarke.« Münch: »Wenn derjenige, der illegal auf das Konto zugreifen möchte, aus dem Familien- oder Bekanntenkreis stammt, werden solche Paßwörter mitunter leicht erraten.«

Drittes Problem sind die Call-Center selbst. Da Telefonbanking immer beliebter wird, ist in den Call-Cenrers Hektik angesagt. »Dort sitzen die Operators knapp beisammen, und da es häufig sehr laut ist, bekommt man mit, welches Paßwort der Kunde hat, der an einer anderen Leitung mit einem Bankangestellten spricht«, bestätigt Münch. Mitgehört können Telefonbanking-Gespräche



aber auch dann werden, wenn sie von einer Telefonzelle, einem Handy oder einem Schnurlostelefon geführt werden. Vor allem die analogen Schnurlostelefone bergen eine große Gefahr in sich, da sie wie bereits erwähnt, relativ leicht abgehört werden können.

## Auf Captain Kirks Spuren

Die Zukunft hat erst begonnen. Während in den EU-Staaten noch heftig diskutiert wird, wie man der Bevölkerung die Umrechnung auf den Euro erleichtern könnte, wird bereits seit einigen Jahren am sogenannten Cybermoney oder Electronic Money gebastelt. Mit diesen Systemen kann über das Internet Geld transferiert werden.

E-Money soll in bestimmten Bereichen die Kreditkarte ersetzen. Da, wie bereits besprochen, die Verbreitung der Kreditkartennummer im Internet ein sehr großes Risiko ist, wurde diese neue Methode entwickelt.

Beim E-Money werden Münzen bzw. Banknoten elektronisch nachgebildet. Beim Bezahlungsvorgang werden diese elektronischen Banknoten überwiesen, und man erhält sogar Wechselgeld retour. Aber auch hier kann es zu Problemen kommen, da E-Money kopiert werden kann.

Einen Vorteil hat E-Money in jedem Fall, zum Leidwesen der Banken. Da man echtes Geld gegen Electronic Money wechselt, wissen die Banken nicht mehr, wofür das Geld verwendet wurde. Durch diese Anonymisierung des Zahlungsverkehrs tun sich Banken künftig etwas schwerer, Kundenprofile zu erstellen und das Verhalten zu berechnen.

Milliarden-Umsätze werden für die Jahrtausendwende für den Online-Markt erwartet. Die Schlagworte der Zukunft heißen Telebanking und Teleshopping. Aber Achtung: Telebanking sollte nicht mit Telefonbanking verwechselt werden. AIs Telebanking bezeichnet man Banktransaktionen, Warenbestellungen oder Reisebuchungen via Fernsehgerät, interaktives Fernsehen ist einer jener Begriffe, die in diesem Zusammenhang immer genannt werden.

Ans TV-Gerät wird eine rechnergestützte Einheit angeschlossen, die über eine Fernbedienung gesteuert wird. Kunden werden sich künf-

tig Filme ansehen können, die sie selbst auswählen, man wird übers Fernsehen einkaufen oder die Bank kontaktieren können. Ähnliches bieten internationale Fluggesellschaften schon heute an. British Airways, Singapore Airlines oder auch Lufthansa und Lauda-Air wurden bereits 1997 mit Bord-Unterhaltungssystemen ausgestattet, die so funktionieren wie das interaktive Fernsehen der Zukunft. Das bedeutet aber wiederum, daß Unternehmen in die Wohnzimmer der Bürger schauen können. Mit einem Schlag wird nämlich nicht nur die TV-Nutzung transparent, sondern auch das Kaufverhalten.

## Wie uns die Finanz unter Kontrolle hat

Finanzbeamte und Zöllner kennen keine Grenzen. Das mußte auch ein österreichischer Tourist feststellen, der in Istanbul mit seiner Kreditkarte eingekauft hatte. Als er nach seiner Rückkehr auf dem Flughafen Wien-Schwechat durch die »Nothing to declare«-Passage gehen wollte, wurde er von den Zöllnern abgefangen. Sie wußten, daß die Einkäufe des Touristen höher als die gesetzlich erlaubte Grenze waren. Woher? Zoll- und Finanzbeamte legen auf »grenzüberschreitende Kooperation« großen Wert. Im Falle des österreichischen Touristen wurden die Österreicher von türkischen Finanzbeamten kontaktiert, die in dem Geschäft in Istanbul einen Kreditkarten-Beleg mit einer hohen Summe entdeckt hatten.

Aber es gibt nicht nur eine türkisch-österreichische Kooperation, auch eine deutsch-österreichische hat in den vergangenen Jahren so manchem Deutschen oder Österreicher eine unvorhersehbare Ausgabe beschert. Von diesen Amtshilfeersuchen wurde auch der Bundesbeauftragte für Datenschutz, Joachim Jacob, informiert. »Im Rahmen eines Amtshilfeersuchens wurde eine Zollfahndungszweigstelle von einer österreichischen Finanzbehörde ersucht, Ermittlungen zu führen, weil der Verdacht der Hinterziehung österreichischer Eingangsabgaben durch österreichische Staatsbürger entstanden war«, schrieb Jacob in seinen Tätigkeitsbericht 1995-1996. Konkret ging es um eine Kooperation zwischen Innsbruck und München. Österreicher, die in einem Pelzgeschäft in der



bayrischen Hauptstadt eingekauft hatten, wurden von der Münchner Finanz durch Besuche in dem Geschäft namentlich aufgelistet, die Listen kamen dann nach Innsbruck.

Durch Österreichs Beitritt zur EU ist zwar der Arbeitsbereich kleiner geworden, aber die Kooperation funktioniert nach wie vor. Gespeichert werden Finanz-, Zoll- sowie Import- und Exportdaten innerhalb der EU künftig in einem Zoll-Inforrnations-System (ZIS). Europaweit kann hier auf heikle Information zugegriffen werden. Wer einmal aktenkundig wird, bleibt in der Datenbank. Mindestens zehn Jahre.

Das ZIS funktioniert ähnlich wie das Information- und Auskunftssystem über Straftaten und Ordnungswidrigkeiten (Owi) der deutschen Zollverwaltung (INZOLL). Im INZOLL, das der Finanz seit 1980 zur Verfügung steht, sind beinahe eine Million Sachverhalte und mehr als eine halbe Million Personen- und Firmendatensätze gespeichert. Alle, die in dieser Datenbank stehen, sind durch ein Zollvergehen aktenkundig geworden. Wer also 1990 auf dem Flughafen Frankfurt wegen eines Zollvergehens bestraft wurde, der steht in diesem System, das, so kritisiert Jacob, ohne ausreichende Rechtsgrundlage betrieben wird. Gelöscht werden die Daten auch hier erst nach zehn Jahren.

Aber im INZOLL sind nicht nur deutsche Staatsbürger gespeichert, sondern auch Amtshilfeersuchen ausländischer Behörden registriert. Bundesdatenschützer Jacob schildert den Fall eines 20jährigen Österreichers, in dessen Auto beim Grenzübertritt elf Gramm Haschisch gefunden wurden. Da der Mann glaubwürdig versichern konnte, daß das Rauschgift eine deutsche Anhalterin im Auto hinterlassen habe, wurde das Verfahren eingestellt. Obwohl er also unschuldig war, wurden seine Daten im INZOLL gespeichert und wären erst nach zehn Jahren gelöscht worden. Auf die Kritik von Jacob antwortete das Finanzministerium, daß die Löschung der Daten »versehentlich unterblieben ist«. Die Frage, die sich daraus ergibt ist, wie viele Unschuldige noch im INZOLL gespeichert sind. Ein »Versehen« wird gerne als praktische Ausrede angesehen.

# Die Daten der Exekutive

**> Wie ein polizeilicher DNA-Test missbräuchlich verwendet werden kann.**

**> Warum jeder Selbstmörder DNA-getestet wird.**

**> Warum Versicherungen und Arbeitgeber an DNA-Tests interessiert sind.**

**X Was in den polizeilichen Datenbanken gespeichert ist.**

**> Warum auch Unschuldige in polizeilichen Datenbanken aufscheinen.**

**> Wie durch Schengen und Interpol der Bürger unter voller Kontrolle ist.**

**X Wo Zigtausende Schriften und Stimmen gespeichert sind.**

**V Warum die eigene Handschrift über Job oder Arbeitslosigkeit entscheiden kann.**

## Die DNA-Datenbank

Jene Sexualmörder, die im Wiener Bezirk Favoriten Ende der 80er, Anfang der 90er Jahre die drei Mädchen Alexandra Schriefl, Christina Beranek und Nicole Strau ermordet haben, könnten längst gefaßt sein. Die Polizei ist sicher, daß es sich um zwei verschiedene Täter handelt, einer hat Schriefl und Beranek, der zweite die sechsjährige Nicole Strau ermordet. Die einzige Spur, die es von den zwei Tätern gibt, sind ihre genetischen Codes, ihre DNA-Muster (Desoxyribo Nucleid Acid bzw. DNS für Desoxyribonucleinsäure). Sie wurden anhand von Sperma-Spuren, die am Tatort und an den Opfern gefunden wurden, erstellt. Obwohl man



damals 7000 Verdächtige einvernommen hatte, konnten die Täter nie überführt werden. Denn vor acht Jahren galten DNA-Analysen noch als teure und »exklusive« Ermittlungsmethode. Erst seit der österreichische Frauenmörder Jack Unterweger überführt werden konnte, weil man in seinem Auto ein Haar einer Ermordeten entdeckt hat, gilt die DNA-Analyse als das zuverlässigste Fahndungsmittel.

Verbrecher hinterlassen am Tatort biologische Spuren: Haare, Sperma, Speichel, Blut oder Hautpartikel. Ob Hautfetzen unter den Fingernägeln des Opfers, auf einer Zigarettenkippe oder Speichel auf einer Briefmarke. Anhand dieser kleinsten Spuren läßt sich der Bauplan eines Menschen, die DNA, analysieren. Früher benötigten die Labors eine halbe Million Spermien, um einen Vergewaltiger zu überführen. Heute genügen 20. »Wir sind um den Faktor 10000 besser geworden«, sagt der Leiter des Instituts für Rechtsmedizin in Münster, Bernd Brinkmann (»Focus«, Nr. 20/97).

»Was die DNA für Kriminaltechniker besonders wertvoll macht, ist ihre Haltbarkeit«, schrieb die »Wirtschaftswoche« (Nr. 32/97). »Anders als Blut, das schnell zerfällt und sich manchmal schon nach wenigen Tagen keiner Blutgruppe mehr zuordnen läßt, hält sich das Erbgut über Jahrzehnte.« Aus einem über 100000 Jahre alten Knochen konnten Wissenschafter der Universität München 1997 sogar das Erbgut eines Neandertalers rekonstruieren.

»Jedes DNA-Profil kommt in der Natur nur einmal vor, ausgenommen sind eineiige Zwillinge«, erklärt der am Rechtsmedizinischen Institut in Bern tätige Gerichtsmediziner Manfred Hochmeister. »Findet man am Tatort biologische Spuren und gibt es einen Verdächtigen, so kann man mit fast hundertprozentiger Sicherheit nachweisen, ob die biologischen Spuren von ihm stammen oder nicht.«

Seit 1 . Oktober 1997 steht den österreichischen Kriminalisten eine solche DNA-Datenbank als Pilotprojekt der Universität Innsbruck zur Verfügung. In dieser Sammlung werden biologische Spuren von Tatorten mit DNA-Profilen von Verdächtigen oder bereits inhaftierten Verbrechern verglichen. Eine DNA-Datenbank setzt sich aus zwei Bereichen zusammen: Im »Spurenteil« sind alle bislang analysierten Tatortspuren gespeichert, Ende 1997 waren das in Osterreich insgesamt 295. Der »erkennungsdienstliche Teil« ent-

hielt Ende 1997 die DNA-Profile von etwa 2500 Verurteilten, die wegen Mordes, Sexualverbrechen und schweren Raubes in Haft sitzen. Bis Ende 1998 sollen insgesamt 9000 DNA-Profile in der Datenbank gespeichert sein.

Diese Zahl werden die österreichischen Behörden mühelos erreichen, denn seit Oktober 1997 müssen sich Verdächtige im Zuge der erkennungsdienstlichen Behandlung - Foto, Fingerabdruck - auch zwei Mundhöhlenabstrichen unterziehen. Dieser Abstrich ist Pflicht für all jene, die eines Kapitalverbrechens (sprich: Mord, Totschlag, Sexualdelikt oder Körperverletzung mit tödlichem Ausgang) verdächtigt sind. Bei vorsätzlicher Körperverletzung, Freiheitsentziehung, erpresserischer Entführung, schwerer Nötigung, Bandendiebstahl, Einbruch, Raub, Erpressung und Suchtgifthandel können die Kriminalisten selbst entscheiden. Sie dürfen, geschützt durch Gummihandschuhe, zweimal mit einem gezahnten Zellstoffstäbchen Wangenschleimhaut aus dem Mund des Verdächtigen kratzen. Den Zellstoff schieben sie in eine mit Konservierungsflüssigkeit gefüllte Phiole, versehen diese mit einem siebenstelligen Barcode und schicken sie an das gerichtsmedizinische Institut der Universität Innsbruck. Dort wird eine Probe bei minus 80 Grad tiefgefroren, die zweite wird analysiert. Eine aufwendige Arbeit, bei der das typische DNA-Profil entsteht, ähnlich einem Strichcode im Supermarkt. DNA-Profile werden innerhalb von zwei Wochen erstellt, die Analyse von Tatort-Spuren dauert vier Wochen. Das Strichmuster des DNA-Profils kann auch als 20stelliger Zahlencode dargestellt werden. Jeder Mensch hat seinen individuellen 20stelligen Code. Zwar sind auf einzelnen Positionen die gleichen Zahlen zu finden, aber der gesamte Code kann niemals gleich sein.

»Zwischen Ermittlern und Labortechnikern verläuft eine scharfe Trennlinie«, betont der österreichische Interpol-Chef Herbert Beuchen*. Die Laboranten in Innsbruck kennen nur den siebenstelligen Barcode auf der Phiole, sie wissen nicht, welche Person sich dahinter verbirgt. Den Code mit dem Namen zu verknüpfen ist nur den Kriminalisten im Wiener Büro für Erkennungsdienst und Fahndungstechnik (EKF) möglich, dort ist die österreichische DNA-Datenbankzentrale eingerichtet. »Ich behaupte nicht, daß ein Mißbrauch völlig unmöglich ist«, meint Beuchert, der sich gewundert hat, daß es im Vorfeld der Realisierung der Datenbank in der



Österreichischen Bevölkerung und bei einigen Parteien keinen Aufschrei gegeben hat. »Eine Großbank ist auch nicht davor gefeit, daß sich der Buchhalter an der Kassa bedient.« Beuchert ist überzeugt, daß sich die zuständigen Beamten »ethisch und moralisch« richtig verhalten.

Österreich ist nach Großbritannien und Holland das dritte Land in Europa, in dem die Kriminalisten auf eine DNA-Datenbank zur Verbrechensaufklärung zugreifen können. Norwegen (1998) und Deutschland sollen folgen. Anfang des kommenden Jahrhunderts soll den Kriminalisten sogar eine EU-weite DNA-Datenbank zur Verfügung stehen.

»In Österreich werden wir Morde und Verbrechen aufklären können, die schon Jahre und Jahrzehnte zurückliegen«, ist der Generaldirektor für öffentliche Sicherheit, Michael Sika, überzeugt. Im Innenministerium erhofft man sich ähnliche Erfolge wie in Großbritannien. Dort werden seit Einführung der Datenbank pro Monat etwa 100 Verbrechen - vom Einbruch bis zum Mord - zusätzlich gelöst. Fälle, in denen es keine Verbindung zum Täter gab. Erfolgreich ist die Methode in Großbritannien auch aus einem weiteren Grund: Jeder Selbstmörder wird typisiert. Es wurde nämlich festgestellt, daß einige Selbstmörder Kapitalverbrechen begangen hatten. Auch bei den Mädchenmorden in Favoriten könnten die Kriminalisten einen neuen Versuch starten, die Verbrechen zu klären, denn auch in Favoriten gab es kurz nach den Morden zwei Selbstmorde von Männern. Diese könnten als Mörder durchaus in Frage kommen.

Erfolgreich waren die Briten sogar, als sie ihre Datenbank mit jener des Roten Kreuzes abgeglichen haben. Ein gesuchter Mörder hatte Blut gespendet und war in der Datei des Roten Kreuzes gespeichert. Und in Kanada wurde einem Frauenmörder, so schrieb das Wissenschaftsmagazin »Nature« (Nr. 386/1997), das Haaren seiner Katze »Snowball« zum Verhängnis. Auf den Kleidern des Mordopfers entdeckten die Kriminalisten Katzenhaare, die ein Katzen-DNA-Experte mit einer Wahrscheinlichkeit von 1 zu 45 Millionen »Snowball« zuordnete.

## Die Gefahr liegt im Code

In Österreich sieht man den Mundhöhlenabstrich als »erkennungsdienstliche Maßnahme«, und die ist im Sicherheitspolizeigesetz gedeckt. »Der totale Wahnsinn«, kritisieren Rechtsexperten. »In anderen Ländern wie etwa Großbritannien oder Holland wurden eigene Gesetze geschaffen, nur in Österreich behandelt man eine DNA-Analyse wie einen Fingcrabdruck.« In den USA und in England haben etwa 1 70 Juristen jahrelang an Gesetzen gearbeitet, die nun regeln, wer die Daten verwenden darf und wann sie vernichtet werden müssen.

Unbestritten ist, daß durch DNA-Datenbanken die Aufklärungsraten stark steigen, wie das Beispiel Großbritannien zeigt. Das DNA-Profil kann und darf aber mit einem Fingerabdruck nicht verglichen werden. Mit einem DNA-Profil kann nicht nur ein Täter überführt werden, das gewonnene Erbgut könnte theoretisch auch dazu verwendet werden, um den Menschen zu analysieren - Gesundheitszustand, mögliche Erkrankungen etc. Folglich könnte die gewonnene DNA mißbräuchlich verwendet werden. Theoretisch ist es auch möglich, die Injektionsnadeln, die am Wiener Karlsplatz oder am Berliner Bahnhof Zoo entdeckt werden, zu analysieren und rückfällige Drogensüchtige auszuforschen.

Für Identifikationszwecke werden zwar nur die zwischen den Genen liegenden, sich wiederholenden Abschnitte fsogenannte nichtcodierende Bereiche) der DNA analysiert, deren Bedeutung zur Zeit noch unbekannt ist. Und gespeichert wird von jedem Menschen nur sein individueller 20stelliger Zahlencode. Aber man wird vielleicht in Zukunft auch nachweisen können, daß etwa die Ziffer 6 auf der Stelle 3 bedeutet, daß der Mensch mit dieser DNA ein bestimmtes Erkrankungsrisiko in sich trägt. So konnte bereits jetzt nachgewiesen werden, daß bestimmte Muster bei Schizophrenie häufiger beobachtet wurden. Wissenschafter könnten die in der DNA-Datenbank gespeicherten Zahlencodes für Studien heranziehen.

»Unsere DNA-Datenbank ist völlig wasserdicht«, betont Interpol-Chef Beuchen*. «Immerhin ist sie auch von der Datenschutzkommission abgesegnet worden.« Beuchert hält es für ausgeschlossen, daß man durch eine Analyse des nichtcodierenden Bereichs des



DNA-Srrangs Krankheiten voraussagen kann: »Bei Blutuntersuchungen kann man viel leichter zu diesen heiklen Informationen kommen. Theoretisch kann in jedem Labor bei der Analyse einer Blutprobe zugleich auch die DNA untersucht werden.«

Diese Informationen könnten jedenfalls auch für Arbeitgeber und Versicherungen von größtem Interesse sein, wenn es um die Aufnahme neuer Mitarbeiter oder um den Abschluß von Lebensversicherungen geht. Zwar werden in Österreich die DNA-Analysen anonymisiert, sind in der Datenbank nur als Barcode gespeichert. Gesetzliche Grundlagen über die Verwendung der DNA - und was damit nicht geschehen darf- müßten aber noch geschaffen werden.

Weiteres Problem einer DNA-Datenbank ist die Speicherdauer der Daten. Wer garantiert, daß Proben von Unschuldigen nach der Analyse vernichtet werden? Wer einmal als potentieller Täter gegolten hat, bleibt in der Datenbank. Zwar gibt es die Möglichkeit, sich löschen zu lassen, aber die wenigsten machen davon Gebrauch, wie das Fingerabdrucksystem AFIS zeigt. Dort haben Tausende Österreicher »vergessen«, sich streichen zu lassen. Jetzt bleiben sie gespeichert, bis sie ein Alter von 80 Jahren erreicht haben.

## Deutsche DNA-Datenbank vor dem Start

Exakt am selben Tag, an dem in Österreich die DNA-Datenbank eröffnet wurde, unterschrieb der Richter, Regierungsrat Michael Schrott, aus dem deutschen Justizministerium in Bonn ein internes Projektpapier und schickte es zur Begutachtung an seine Ministeriums-Kollegen. Inhalt des Papiers: die juristischen Grundlagen für eine DNA-Datenbank in Deutschland. Bei ihrem Projekt schielen die deutschen Juristen und Beamten aus dem Innenministerium ein wenig nach Österreich. «Der Druck der Öffentlichkeit ist groß geworden, auch in Deutschland eine DNA-Datenbank zu installieren«, bestätigt Schrott. Mädchenmorde wie jener an der zehnjährigen Kim Kerkow am 9. Januar 1997 in Varel bei Wilhelmshaven lassen Forderungen in Deutschland laut werden. »Die offene Frage ist die Rechtsgrundlage. Ob der § 8 des BKA-Gesetzes ausreicht,

L

um von Tatverdächtigen DNA-Profile zu erstellen oder ob wir das Gesetz ändern müssen.« Gemäß § 8 kann das ßundeskriminalamt zur Erfüllung seiner Aufgaben »Personendaten von Beschuldigten und, soweit erforderlich, andere zur Identifizierung geeignete Merkmale in Dateien speichern, verändern und nutzen«. Reicht der § 8, so gilt auch in Deutschland der DNA-Test als erkennungsdienstliche Maßnahme. Schrott bezweifelt aber, daß das in Deutschland durchgeht. Gemäß § 81 e der deutschen Strafprozeß-Ordnung gibt es jedenfalls die Grundlage für die DNA-Untersuchung. Voraussetzung dafür ist aber eine richterliche Anordnung.

Wessen Daten man in einer Datenbank speichern würde, das weiß man aber im Oktober 1997 in Bonn genau: »Besonders schwere Straftäter«, erklärt Schrott. Dem Beispiel Österreichs folgend möchte man in einer deutschen DNA-Datenbank Profile von Mördern, Räubern, Sexualverbrechern und Suchtgifthändlern speichern und Inhaftierte zum Mundhöhlenabstrich zwingen. Offen ist neben der gesetzlichen Grundlage die Speicherdauer der Profile. Sollten etwa anläßlich eines Verbrechens 100 DNA-Analysen gemacht werden und einer der Verdächtigen ist der Täter, bleiben auch die 99 anderen laut Schrott in der Datenbank: »Wir müssen doch nachweisen können, daß die 99 anderen unschuldig sind.« In Großbritannien ist dies anders. Bei einem Massenscreening, bei dem die Bevölkerung ganzer Ortschaften oder Stadtteile zum DNA-Test antreten mußte, werden die Bewohner nur gegen das Verbrechen gecheckt und kommen nicht in die Datenbank.

Mit DNA-Analysen hat man in Deutschland bereits mehrfach Täter überführt. Schlagzeilen haben vor allem einige Fälle von Massenscreening gemacht. Der spektakulärste Fall ereignete sich im September 1993 in Babenhausen (Kreis Darmstadt-Dieburg). Die zweieinhalbjährige Elora McKemy, Tochter eines US-Soldaten, war in der Nähe der amerikanischen Kaserne mißbraucht und ermordet aufgefunden worden. Als Täter kamen alle männlichen Bewohner in der Umgebung der Kaserne in Frage. Polizei, Staatsanwaltschaft und Vertreter entschieden sich daraufhin für die umfangreichste DNA-Untersuchung, die es je gab: 1 899 Männer mußten sich einer DNA-Analyse unterziehen. »Nr. 531«, der US-Soldat Patrick Smith (22), wurde acht Monate später als Mörder überführt.

Ein ähnliches Massenscreening hat 1996 für Aufruhr unter den



Münchner Porsche-Fahrern gesorgt. Nach dem Mord an einer 24jährigen Frau aus dem baden-württembergischen Nehren, vor deren Wohnhaus mehrmals ein Porsche mit Münchner Kennzeichen gesehen worden war, wurden von allen Münchner Porsche-Fahrern DNA-Analysen gemacht. Nach der Beschwerde eines Porsche-Fahrers beschloß das deutsche Bundesverfassungsgericht, daß Gerichte zur Aufklärung schwerer Verbrechen eine Vielzahl von Blutproben anordnen dürfen. Selbst dann, wenn ein besonders starker Tatverdacht nicht besteht (Beschluß vom 2. 8. 1996, der Fall ist noch nicht geklärt).

Der genetische Fingerabdruck kann aber auch Unschuldige hinter Gitter bringen, wie der »Spiegel« in seiner Geschichte »Pfusch am Code« geschrieben hat (Nr. 31/94). Der 28jährige Arbeiter Rainer Gutschmidt aus Berlin saß ein halbes Jahr unschuldig in Haft. Eine DNA-Analyse hatte ihn als Mörder der 47jährigen Ost-Berlinerin Gisela Braun überführt. Erst ein von der Verteidigung angestrengter nochmaliger DNA-Test konnte das Gegenteil beweisen. Bei der Analyse im Institut für Gerichtliche Medizin im Ost-Berliner Humboldt-Institut hatte der Laborant »beim Einfüllen der Proben in das Sortiergerät offenbar winzige Mengen Erbmaterial aus dem Blut Gutschmidts mit Zellen aus der Spermaspur vermischt«. Gutschmidt wurde sofort freigelassen, der Staatsanwalt entschuldigte sich schriftlich, daß er »unschuldig Untersuchungshaft zu erleiden hatte«.

## Vom Blutstropfen zum Phantombild

Die Forschungen im Forensic Science Service im britischen Birmingham laufen auf Hochtouren. Institutsleiter Peter Gill arbeitet an einem Projekt, das, sollte es sich tatsächlich realisieren lassen, Sensation und Alptraum in einem ist: Aus einer biologischen Spur soll ein Phantombild derjenigen Person erstellt werden können, von der die Spur stammt. Aus einem DNA-Profil läßt sich detailliert herausfiltern, ob es sich um einen Mann oder eine Frau handelt, ob weiß oder schwarz, wie groß der Mensch ist, ob er abstehende Ohren, eine große Nase hat, ob er zur Glatzenbildung

oder zu Übergewicht neigt. »In Zukunft werden Gerichtsmediziner den Kriminalisten exakt sagen können, der Täter ist ein Mann, l ,85 Meter groß, blond, wahrscheinlich große abstehende Ohren, blaue Augen, sehr schlank und HIV-positiv. Die Körpergröße ist genetisch determiniert und auf einem Chromosom erkennbar, auch das Chromosom, das für die Augenfarbe verantwortlich ist, wurde bereits gefunden. Es ist nur noch eine Frage der Zeit, bis die Wissenschafter auch die anderen Positionen für Ohrengröße, Ohrenform und Nasengröße auf der DNA-Kette entdecken. Irgendwann im kommenden Jahrtausend werden mit dieser Methode Paare vor ihrer Hochzeit Informationen übereinander einholen. Anhand ihres Blut- oder auch DNA-Tests werden sie wissen, ob sich die zierliche Blondine in einigen Jahren in eine Walküre verwandelt oder der athletische Brad-Pitt-Typ in einen übergewichtigen Glatzkopf.

## *Menschenauslese via Genanalyse*

»Ihr Mitarbeiter Friedrich M. ist dynamisch, kreativ und neugierig, neigt aber zu Aggressivität und hat wenig Teamgeist.« So hätte ein Mitarbeiterprofil aussehen können, wäre die Firma Genetics Austria nicht Ende 1997 pleite gegangen. Was sich hinter dieser Firma verbarg, hat die Kriminalpolizei ebenso entrüstet wie routinierte Genforscher. Im Frühjahr 1996 hatte der Grazer Helmut Fink diese Firma gegründet und an diverse Unternehmen Werbeunterlagcn verschickt, in denen er Personalauslese via Genanalyse angeboten hatte. Mittels DNA-Code hätte er die Angestellten klassifiziert, ihre positiven und negativen Eigenschaften erhoben. Seine Genanalysen, so versprach Fink, seien »prägnant genetisch festgelegte Leistungspotentiale«. »Mittels Genanalyse sind heute schon folgende genetisch festgelegte Verhaltensweisen meßbar«, schrieb Fink in seinem Prospekt. »Die Neugierde, die Aufgeschlossenheit, Aggressionsverhalten und Kreativität.« Elf österreichische Unternehmen würden seine Methode der Mitarbeiterauslese bereits nützen. »Fehlalarm«, schrieb das »Profil« {Nr. 44/1997). »Von der Liste der Firmen, die auch namhafte Betriebe wie die steirische



Mayr-Melnhof oder die Linzer Quelle anführt, wendet kein einziger Betrieb die Programme der Genetics Austria tatsächlich an.«
»Diese Entwicklungen werden sich nicht stoppen lassen«, verkündete der gescheiterte Unternehmer. Fink könnte recht behalten, denn in den Vereinigten Staaten und in Großbritannien sind Gentests auf dem freien Markt üblich. In Österreich wurde diesem Geschäft mit dem § 67 Gentechnikgesetz ein Riegel vorgeschoben. Demnach ist es »Arbeitgebern und Versicherern verboten, Ergebnisse von Genanalysen von Arbeitnehmern, Arbeitssuchenden oder Versicherungsnehmern oder Versicherungswerbcrn zu erheben, zu verlangen, anzunehmen oder sonst zu verwerten«.
Deutsche und österreichische Genforscher halten Finks Thesen für völligen Unsinn. Der Präsident der Österreichischen Gesellschaft für Genetik und Gentechnologie, Universitätsprofessor Helmut Schwab, spricht im »Profil« sogar von »Scharlatanerie«. »Inwieweit Gene menschliches Verhalten mitbestimmen, ist derzeit noch völlig unklar. Es ist weder ein Gen für Neugierde noch für Aggressionsverhalten lokalisierbar, geschweige denn exakt rneßbar.«
Zwar sind noch keine Verhaltensmerkmale meßbar, Krankheiten können aber schon mit sehr hoher Wahrscheinlichkeit vorausgesagt werden. Theoretisch und praktisch ist es möglich, aus den DNA-Proben eine Vielzahl von Informationen über Erbkrankheiten herauszulesen, bestätigen Genforscher. Zwischen 20 und 30 Krankheiten bzw. Krankheitsveranlagungen kann man bereits anhand eines DNA-Profils feststellen. Man kann einer Frau sagen, ob sie das Erkrankungsrisiko für Brustkrebs in sich trägt, einem Mann, ob er ein potentieller Kandidat für Prostatakrebs ist. Das heißt aber nicht, daß die Krankheit tatsächlich ausbrechen wird, es bedeutet lediglich, daß die Wahrscheinlichkeit höher sein kann und man sich durch regelmäßige Vorsorgeuntersuchungen davor schützen sollte.
Obwohl die Gesetze in Deutschland und Österreich derzeit eine Genanalyse zur Erhebung von Gesundheitsdaten verbieten, sind Experten überzeugt, daß in einigen Jahren diese Hürden fallen werden und ethische und moralische Bedenken keine Rolle mehr spielen.
Dem Vorteil, eventuell ausbrechende Krankheiten im Keim zu ersticken, stehen enorm viele Nachteile gegenüber: Arbeitgeber

können sich, sollten sie im Besitz der DNA-Daten sein, gegen Bewerber aussprechen. »Nein, wir können Sie nicht einstellen, da Sie das Darmkrebs-Gen in sich tragen. Entweder wir müssen Sie früher als geplant ersetzen, oder Sie sind lange im Krankenstand.« Auch Versicherungen könnten sich diese Informationen zunutze machen, indem sie von gefährdeten Personen höhere Prämien verlangen als von ungefährdeten. In den Vereinigten Staaten ist es jetzt schon üblich, daß Versicherungsnehmer bei Vorlage eines Gentests günstige Prämien zahlen. Wenn der Test beweist, daß der Kunde keine ernstzunehmenden Krankheiten zu erwarten hat und für die Versicherung daher das Risiko geringer ist.

Irgendwann einmal könnte es so weit kommen, daß jeder Mensch automatisch genetisch typisiert wird, um ein hundertprozentiges Identifikationsmerkmal zu haben. Gleich nach der Geburt wird eine DNA-Analyse gemacht, die Daten werden dann in einer zentralen Datei gespeichert. Wenn ein Verbrechen begangen wird, läßt man einfach Tatortspuren gegen diese Mega-DNA-Datenbank laufen. Damit hat man die volle Kontrolle über uns Menschen. Wird dann auch noch eine Genanalyse gemacht, so könnte die ungefähre Lebenserwartung festgestellt werden. Welche Krankheiten der Mensch zu erwarten hat und wie »teuer« die medizinische Versorgung seines Lebens sein wird.

## Die Mörderseele im Computer

Der Fragebogen umfaßt 262 Fragen. Peinlich genau wird jedes Detail, das die Kriminalisten am Tatort erkennen können, dokumentiert, im Zentralcomputer gespeichert, verglichen und ausgewertet: Informationen über Opfer, Täter, Tatort, mögliche Täter-Opfer-Beziehungen etc. Das Computerprogramm heißt »Viclas« und steht für Violent Crime Linkage Analysis System. Mit Hilfe von Viclas lassen sich psychologische Verhaltensmuster aufzeichnen und Sexualstraftaten sowie andere Gewaltverbrechen als Seriendelikte erkennen. »Jedes noch so kleine Detail an einem Tatort kann wichtig sein, denn der Ort eines Verbrechens spiegelt das Verhalten des Täters wider«, meint Kriminalpsychologe Thomas Müller.



Im Viclas-System sind alle Sexualmorde gespeichert, alle Formen sexueller Angriffe zwischen Personen, die einander nicht kennen, Vergewaltigungen, nichtidentifizierte Leichen und Leichenteile sowie Vermißte und Entführte. Anhand des Computerprogramms können Parallelen aufgezeigt werden, aber auch bestimmte Eigenheiten des Täters.

1991 wurde Viclas in Kanada von der Royal Canadian Mounted Police eingeführt, vier Jahre später wurde die Viclas-Software vom Kriminalpsychologischen Dienst der Interpol-Wien ins Deutsche übersetzt, seit 1996 ist Viclas in drei Sprachen einsetzbar - Englisch, Französisch und Deutsch.

Im Viclas-System sind derzeit 180 ungeklärte Morde aus Österreich, 20 Fälle aus Deutschland sowie zehn ungeklärte Morde aus Belgien, Polen und Großbritannien gespeichert. Wie wichtig es ist, Verbrechen miteinander zu verknüpfen und Parallelen aufzudecken, hat die Münchner Mordkommission im April 1995 erkannt. Dort hatte man sich anhand des Kriminalfalles Horst David von der Funktionalität des Viclas-Systems überzeugt. David hatte ab 1975 sieben Frauen ermordet. 20 Jahre blieb er unentdeckt, bis den Fahndern Parallelen auffielen.

Viclas wird in den kommenden Jahren in ganz Europa eingesetzt. Neben Österreich ist Viclas in Großbritannien, Belgien und den Niederlanden im Einsatz, auch das BKA in Wiesbaden zeigt großes Interesse. »Gerade für ein Europa mit den zahlreichen Sprachen und den zunehmend offeneren Grenzen wäre dieses System ein wertvolles Hilfsmittel zur Verbrechensbekämpfung«, meint Thomas Müller. Viclas kommt der Mobilität eines Täters, der Montag einen Mord in Frankfurt, Mittwoch in Wien und am Freitag in Rom begeht, auf die Spur. Müller: »Mit Hilfe von Viclas können Verbrecherrouten aufgezeigt und die Polizeiarbeit verbessert werden.«

## Ein Druck für den Fingerabdruck

Die meisten Deutschen und Österreicher kennen die Prozedur nur aus Kriminalfilmen: Der Verdächtige drückt seine Finger zuerst in

ein schwarzes Stempelkissen und dann auf einen Bogen Papier. Für etwa 2,3 Millionen Deutsche und 630000 Österreicher ist dieser Vorgang bereits einmal Realität geworden. So groß ist die Anzahl derer, die in den nationalen AFIS-Systemen (Automatisiertes-Fingerabdruck-Identifizierungs-System) beim Bundeskriminalamt in Wiesbaden bzw. beim Büro für Erkennungsdienst und Fahndungstechnik (EKF) in Wien gespeichert sind. In dieser Zahl sind aber auch Asylwerber und ausländische Straffällige enthalten. Rechnet man die Fingerabdrücke hinzu, die an Tatorten gesammelt wurden, so sind sogar 4,5 Millionen Daten im AFIS des BKA.

Im AFIS-Computer sind bei BKA und EKF seit 1992 die Fingerabdrücke digital gespeichert. Jedes »Zehnfingerabdruck-Blatt« und jeder an Tatorten gefundene Fingerabdruck wird von den Landeskriminalämtern nach Wiesbaden geschickt und eingescannt. Dort werden die besonderen anatomischen Merkmale (Minuzien) bezeichnet. Insgesamt unterscheiden die Spurensicherer 11 verschiedene Kategorien an Merkmalen - die Zahl 1 steht beispielsweise für »Beginn und Ende«, die 5 bedeutet eine »Gabelung«, 7 »Auge« und 8 »Insel«.

Das AFIS-System hat die Erfolgsquote der Kriminalisten bedeutend erhöht. »Früher mußte jedes Zehnfingerabdruck-Blatt händisch kontrolliert werden«, erklärt Oberst Franz Kößler vom Büro für Erkennungsdienst und Fahndungstechnik. Vor der Computerisierung konnten in Österreich jährlich 60 Fälle geklärt werden. Kößler: »jetzt landen wir im Durchschnitt 1 800 bis 2000 Treffer pro Jahr.« Deutsche Kriminalisten können sich über eine ähnlich hohe Erfolgsqoute freuen. Jährlich werden mehr als 8000 Fälle durch AFIS geklärt.

Unter den im AFIS gespeicherten Daten von Deutschen und Österreichern befindet sich aber eine große Zahl von Unbescholtenen. 50000 Personen werden in Österreich pro Jahr erkennungsdienstlich behandelt, nur etwa 100 stellen jährlich ein »Ersuchen um Tilgung«. Viele wissen gar nicht, daß ihre Fingerabdrücke im AFIS gespeichert bleiben. Sogar dann, wenn sie nichts verbrochen haben bzw. irrtümlich zum Verdächtigenkreis gezählt wurden. Denn in Österreich werden die Daten erst dann automatisch gelöscht, wenn die Person das 80. Lebensjahr erreicht hat. Wann sie in Deutschland gelöscht werden, ist unklar. Offiziell werden die



Daten von Erwachsenen zehn und von Kindern fünf Jahre lang gespeichert. »Gelöscht werden die Daten erst dann, wenn uns das zuständige Landeskriminalamt bittet, sie zu löschen«, bestätigt ein BKA-Sprecher. Wie oft solche Lösch-Ersuchen in Wiesbaden einlangen, kann und möchte niemand beantworten. Selbst Bundesdatenschützer Joachim Jacob kritisierte die gegenwärtige Undurchsichtigkeit von AFIS: »Es mangelt noch immer an einer vom Innenministerium endgültig genehmigten Errichtungsanordnung.« Unter dieser Errichtungsanordnung muß geklärt sein, wer auf Daten zugreifen darf, wann sie gelöscht werden etc. Seit 1992 arbeiten die deutschen Kriminalisten praktisch mit einer provisorischen Genehmigung. Jacob: »Eine weitere Verzögerung des Erlasses wäre ein Verstoß gegen das Datenschutzgesetz.«

Künftig werden Fingerabdrücke innerhalb Europas auch auf Reisen geschickt. Vor allem jene von Asylwerbern. EURODAC nennt sich das System, in dem die Fingerabdrücke aller Asylwerber innerhalb der EU gespeichert sind. In welchem EU-Land diese zentrale Stelle eingerichtet wird, ist noch unklar. In dieser AFIS-Zentraldatei sollen nur Fingerabdrücke, keine Personalien gespeichert werden. Leitet ein Land die Fingerabdrücke seiner Asylwerber weiter, werden die Daten mit einer Kenn-Nummer versehen. Erst nach dem Identifizieren wird der Name zur Nummer geliefert.

## Ein Computer, der Stimmen speichert

Ein hochkompliziertes Computersystem steht den Kriminalisten des Bundeskriminalamtes in Wiesbaden auch bei der Ausforschung von Urkundenfälschern zur Verfügung. Jeder Erpresserbrief, jeder gefälschte Scheck wandert in das FISH. 40000 verschiedene Schriftproben sind im »Forensischen Informations-System Handschriften« gespeichert. Ins FISH werden Handschriftenproben eingelesen und digitalisiert, ein Ausschnitt von 6,5 Zentimetern reicht, um die Schrift analysieren und mit anderen vergleichen zu können. Jede Schrift wird typisiert, bestimmte Merkmale wie Schräglage, Unterlängen etc. werden genau beschrieben. Der Leiter der Fachgruppe Schrift-Sprache-Stimme im BKA, Manfred Hecker, ist

überzeugt, daß sich in Zukunft auch Eigenschaften des Schreibers, wie etwa Bildungsstand oder soziale Herkunft herauslesen lassen. Eine Differenzierung sei schon heute mit Leichtigkeit möglich, nämlich ob es sich bei dem Schreiber um eine Frau oder um einen Mann handelt.

Gespeichert werden im Bundeskriminalamt nicht nur Erpresserbriefe, sondern auch Schreiben von Bürgern, die dem BKA Verbrechen ankündigen, »aufklären« wollen oder Verbrecher nennen. Diese Briefe werden 5 jähre aufgehoben. »Wir brauchten einen eigenen Verrückten-Sachbearbeiter«, meint ein Sprecher des BKA. »Denn bei Vollmond häufen sich solche Schreiben.«

So ausgeklügelt das FISH auch ist, »leider hinterlassen auch Erpresser immer seltener schriftliche Spuren«, wie Christian Weber im »Focus« (Nr. 20/97) feststellt. »Nur einen Fehler begehen sie alle irgendwann: sie telefonieren.« Denn im BKA wurde bereits ein Spracherkennungs-Computer entwickelt, mit dem Stimmen gespeichert, analysiert und verglichen werden können. Die Sprache hat sich bei jedem Menschen in einem Lernprozeß herangebildet. Jeder Mensch hat seine unverwechselbare Art zu sprechen, jeder Mensch hinterläßt daher seinen individuellen Stimmabdruck, der mit einem Fingerabdruck verglichen werden kann. Auch wenn Erpresser ihre Stimme verstellen, bleibt der Stimmabdruck gleich. Langt ein Erpresser- oder Drohanruf ein, so wird dieser gespeichert und mit Hilfe von Filter- und Spezialprogrammen analysiert. Ergebnis ist ein Stimmabdruck in Linien- oder Konturenform, der sich zwar immer ändert, aber im Grundmuster gleichbleibt. Und diese Grundmusterwerden miteinander verglichen. Entwickelt wurde im BKA auch eine Dialekt-Datenbank, in der die regionalen Dialekte bis auf 20 Kilometer genau lokalisiert werden können. Erpresser können mit Hilfe dieser Datenbank einer bestimmten Region Deutschlands zugeordnet werden.

## *Die Handschrift als Karriere-Hemmschuh*

Achtung! Ihre Handschrift kann über Karriere oder Nicht-Karriere, über Job und Arbeitslosigkeit entscheiden. Immer mehr deutsche



und österreichische Unternehmen ziehen bei der Besetzung von Führungsposten und bei der Aufnahme neuer Bewerber Schriftpsychologen (Grafologen) zu Rate. In Gutachten wird entschieden, ob ein Kandidat oder eine Kandidatin für einen Posten im Unternehmen überhaupt geeignet ist. Eine hingekritzelte Notiz, ein schlampig geschriebener Lebenslauf kann über die berufliche Zukunft entscheiden.

Bei der Bestellung des neuen Finanzchefs der Münchner Heilit & Woerner BauAG hatten Grafologen ihre Hand im Spiel. Wer bei BMW, Siemens oder Osram befördert wird, dessen Schrift wurde - mit, aber mitunter auch ohne dessen Wissen - von Schriftpsychologen analysiert. »Aus der Handschrift lassen sich Rückschlüsse auf die Persönlichkeit eines Schreibers ziehen«, erklärt der Vorsitzende des Berufsverbands der Grafologen mit Sitz in München, Dr. Helmut Ploog. Die Schrift verrät den Charakter, die Intelligenz, Arbeitseigenschaften und die Eignung für Führungsaufgaben. Grafologen können das Persönlichkeitsformat, die Durchsetzungskrait, das menschliche Verständnis und die Autorität beurteilen. Wichtigstes Kriterium: die Bewegungsdynamik in der Schrift. Sie verrät, so sind Grafologen überzeugt, ob jemand Energie hat oder nicht.

Eine Unterschrift alleine reicht für ein seriöses grafologisches Gutachten normalerweise nicht aus. Meist werden entweder handgeschriebene Lebensläufe oder mindestens eine A4-Seite lange Notizen aus dem Berufsalltag des Kandidaten beurteilt.

In Frankreich werden bei 85 Prozent der Entscheidungen für Posten »ganz oben« Grafologen herangezogen, in der deutschsprachigen Schweiz sind es bereits 70 Prozent. Ob beim Schweizerischen Bankverein, bei der Swissair oder bei der Helvetia-Versicherung - keine Entscheidung wird hier ohne schriftpsychologisches Gutachten gefällt. In Deutschland und Österreich ist die Bereitschaft, Grafologen mitentscheiden zu lassen, noch gering. In Deutschland werden bei etwa 20 Prozent der Entscheidungen Grafologen kontaktiert, in Österreich bei etwa 10 Prozent - meist sind es in Osterreich Schweizer Konzerne oder große deutsche Unternehmen wie BMW oder Siemens. Kritiker hingegen vergleichen die Schriftpsychologie mit Astrologie oder Kaffeesudlesen.

Die Tendenz geht aber bereits dorthin, nicht nur Führungsposten,

sondern auch Neubewerber anhand ihrer Schrift auszusieben. Anders als bei Führungsposten werden hier Kandidaten für einen Sekretärinnen- oder Assistentenjob vorselektiert, indem ihre Unterschrift analysiert wird - fünf Zentimeter sind entscheidend. »Anhand der Schriftdynamik sieht man die Leistungsenergie«, bestätigt die österreichische Grafologin, Dr. Ursula Hansmann. »Bei einem Sekretariatsposten kann man aus dem Stand heraus ein Urteil fällen, da sieht man auf den ersten Blick, was los ist.« In Österreich fallen acht von zehn Bewerbern für einen Job wegen ihrer Unterschrift durch. Beim verbliebenen Rest wird eine Erfolgsquote von 70 Prozent erzielt.

## Die Datenbank der Fahnder

Die EDV-Zentralen im BKA und im österreichischen Innenministerium gehören zu den bestbewachten Deutschlands und Österreichs. Videokameras haben Eingänge im Visier, Türen lassen sich nur mit Codes bzw. Chipkarten öffnen und die Personalien von Besuchern werden, zumindest im BKA, mit den vorhandenen Daten im Zentralcomputer verglichen. Die strengen Sicherheitsvorkehrungen sind verständlich. Wenn die Informationen, die hier gespeichert sind und verarbeitet werden, der organisierten Kriminalität in die Hände fallen, gerät die Sicherheit einer Nation ins Wanken.

2,8 Millionen Kriminalakten von in Deutschland straffällig gewordenen Personen, 660000 Festnahmeersuchen und 7,4 Millionen Gegenstände, nach denen gefahndet wird - darunter 350000 Pkw, 150000 Mopeds, 840000 Fahrräder und 3,4 Millionen Ausweise wie Führerscheine oder Reisepässe: INPOL, das elektronische Informationssystem der Polizei, ist wohl die größte Datenbank der Exekutive Deutschlands. Seit 1972 wird diese Datensammlung von den Landeskriminalämtern und dem Bundeskriminalamt in Wiesbaden mit Informationen versorgt. Online haben die Polizeibehörden des Landes Zugriff auf den Zentralcomputer. Seit Ende 1996 wird INPOL neu strukturiert. Die Datenübermittlung soll künftig verschlüsselt ablaufen, um eventuellen »Datenklau« zu verhindern.



Ein Vorteil für den Bürger, ein Nachteil für die Exekutive ist die Tatsache, daß in Deutschland diverse Informationen über Straftäter in den Landeskriminalämtern gespeichert sind und dem BKA nicht übermittelt werden.

»Viele deutsche Kriminalisten beneiden uns um unser zentralistisches System«, meint der Leiter der EDV-Zentrale im Innenministerium, Nikolaus Schwab. Er ist der Chef des größten Rechenzentrums in der öffentlichen Verwaltung Österreichs. Drei Großrechner verwalten die heikelsten Daten der Republik. Neben dem Elektronischen Kriminalpolizeilichen Informationssystem (EKIS) das Kfz-Zentralregister, den Schengen-Computer und das gesamte Büro-Automatisationssystem des Innenministeriums. Speicherkapazität 1 Terabyte.

Das EKIS umfaßt insgesamt elf Datensammlungen - beginnend mit dem Strafregister über die Personen-, Sach- und Kulturgutfahndung bis hin zum Kfz-Zentralregister und dem Automatisierten Fingerabdruck-Identifikationssystcm. Auf diese Informationen haben Polizei- und Gendarmeriebeamte Zugriff, innerhalb von wenigen Sekunden erhalten sie die gewünschte Information. Ab Mitte 1998 ist die Computerisierung der Polizeikommissariate und Gendarmerieposten abgeschlossen. Von 10000 PCs, die über ganz Österreich verstreut sind, können die Exekutivbeamten zugreifen. Damit müssen Kritiker, die der Exekutive lange vorwarfen, das Computerzeitalter verschlafen zu haben und weiterhin der Schreibmaschinen-Ära anzugehören, verstummen. Genau diese Kritiker müssen sich aber auch bewußt sein, daß der Staatsbürger umso strenger überwacht werden kann, je schneller und je besser die Polizei vernetzt ist. Denn das österreichische Innenministerium hat nicht nur einen Online-Zugriff auf die Daten des Hauptverbandes der Sozialversicherungsträger - und das sind insgesamt 85 Millionen Datensätze -, auf Knopfdruck ist man auch mit dem Firmenbuch und dem Grundbuch verbunden. Natürlich auch mit den Verwaltungsdaten, und die beinhalten das Computersystern mit den Anonymanzeigen ebenso wie die zentrale Wählerevidenz oder das Waffenregister.

## Nase Nr. 7 und Augenbrauen Nr. 11

Ein Verbrechen, wie es in Deutschland und Österreich pro Tag unzählige Male passiert: Eine Frau wird überfallen und vergewaltigt, der Täter kann unerkannt flüchten. Der Anzeige auf dem Kommissariat folgt die Fahndung. Der Beamte gibt sein Paßwort in den Computer, eine Suchmaske erscheint. Ganz oben tippt er die Zwei-Buchstaben-Abkürzung jener Dateien ein, die miteinander verknüpft werden sollen. Dann folgen die Personenbeschreibungen. Alter: 20 bis 30, Größe: 1,75 bis 1,85 Meter, Augenfarbe: blau-grau. Als besonderes Kennzeichen ist dem Opfer eine Narbe aufgefallen. Der Polizeibeamte öffnet das Menü »besondere Merkmale«, klickt »Narbe« an und wählt dann in einem Untermenü die Stelle am Körper aus, an der sich die Narbe befunden hat - »Handrücken rechts«. »Wir können in unserem System Personenbeschreibungen mit grafischen Informationen verknüpfen«, erklärt der Leiter der EDV-Zentrale im österreichischen Innenministerium, Nikolaus Schwab. In einem Zeichenmenü kann die Frau unter verschiedenen Augenbrauen, Nasen- und Ohrenformen wählen. Sie entscheidet sich für die Nase mit der Nr. 7, die Augenbrauen mit der Nr. 1 1 und die 2er Ohren. Der Polizeibeamte drückt die Enter-Taste. Innerhalb von zwei Sekunden erscheint die Trefferzahl 28 auf dem Bildschirm. 28 Personen, auf die die Beschreibung der Frau zutreffen könnten, listet der Computer auf. Personen, die entweder einmal straffällig geworden oder erkennungsdienstlich behandelt worden sind.

Das EKIS-System kann freilich auch mißbraucht werden, wie ein Fall in der steirischen Landeshauptstadt Graz gezeigt hat. Zwei Polizisten, die das Alter einer hübschen Grün-Abgeordneten wissen wollten, holten sich die gewünschte Information aus dem Polizei-Fahndungscomputer, indem sie das Kennzeichen des Autos der Abgeordneten ins EKIS tippten. Die Beamten hatten Pech: Jeder Zugriff auf das System wird genau protokolliert, die Datenschutzabteilung im Innenministerium überprüft stichprobenartig, ob die Zugriffe berechtigt erfolgt sind. Bei 30 Millionen Anfragen an den Polizeicomputer hatten sie sogar ziemliches Pech.



## Das größte Oberwachungssystem Europas

Eine der gewaltigsten Datenbanken Europas ist das Schengener Informationssystem (SIS). Durch den Abbau der Grenzkontrollen zwischen den EU-Mitgliedsstaaten, die das Schengener Abkommen unterzeichnet haben, ist SIS notwendig geworden. Ende 1997 belieferten insgesamt zehn EU-Staaten den Zentralcomputer in Straßburg mit Informationen, die insgesamt 5 Millionen Datensätze umfassen. Darin enthalten sind etwa 1,3 Millionen Personenfahndungen und 3,7 Millionen Sachfahndungen,

Mit dem SIS sind die Polizeizentralen der einzelnen Länder online verbunden. Jedes Land hat sein eigenes nationales SIS und beliefert die anderen mit Informationen, von denen man annimmt, daß sie benötigt werden könnten. Die Informationen werden aber nicht direkt von einem Land ins andere geschickt, sondern via Straßburg verteilt.

Deutsche Polizisten nutzen den schnellen Rechner 4 Millionen Mal pro Monat, schrieb die »Zeit« (9. 5. 1997). »Europas erstes Fahndungsnetz war deutschen Behörden zwischen März 1995 und März 1996 mehr als 12000 Mal hilfreich: Asylwerber mit Aufenthaltsverbot in anderen EU-Ländern, mit Haftbefehl gesuchte Straftäter, Zeugen, Vermißte und verdächtige Fahrzeuge konnten dank des Eurocomputers identifiziert werden.«

Beat Leuthardt ortet in seinem Buch »Leben Online« beim SIS neue Möglichkeiten heimlicher Überwachung. »Die Gefahr, daß Persönlichkeitsbilder von Unschuldigen und Unverdächtigen gezeichnet werden, ist wohl bei keinem anderen der derzeit in Betrieb befindlichen Systeme größer.« 8 Millionen Datensätze können im SIS gespeichert sein. Von beinahe 35000 PCs in ganz Europa können diese Informationen abgerufen werden. Polizeistationen, Grenz- und Zollstationen sowie zahlreiche andere Behörden haben Zugriff auf Personendaten. Bei 8 Millionen Datensätzen ist anzunehmen, daß auch Unbescholtene in dieser Datei gespeichert sind. Denn die in Europa wegen schwerer Delikte dringend Tatverdächtigen machen nur einen Bruchteil dieser Zahl aus.

Angriffspunkt der Gegner ist der Artikel 99 im Schengener Zusatzübereinkommen. Darin wird die »verdeckte Registrierung« geregelt. »Der Artikel 99 erlaubt alles und verbietet nichts«, schreibt

Beat Leuthardt. Denn wer eine »außergewöhnlich schwere Straftat plant oder begeht«, kann im SIS gespeichert werden. Für eine Eintragung im SIS genügen »tatsächliche Anhaltspunkte«. Leuthardt kritisiert zu Recht, daß normalerweise ein »konkreter« oder »dringender« Tatverdacht üblich ist.

Wer im SIS gespeichert ist, dessen Daten liegen auf dem europäischen Serviertablett. Denn Heiner Busch ortet in seinem Buch »Grenzenlose Polizei?« einen weiteren Nachteil, daß nämlich Informationen ausgetauscht werden, die je nach den unterschiedlichen nationalen Gesetzen im eigenen Land nicht legal zu erfahren gewesen wären.

## *Der »Schengener Datenklau«*

Der Skandal hätte vertuscht werden sollen. Nur so ist erklärbar, daß der Mitte Dezember 1997 bekanntgewordene »Schengener Datenklau« erst dreieinhalb Wochen nach der Verhaftung des mutmaßlichen Täters am 20. November 1997 an die Öffentlichkeit gelangt ist. Ein belgischer Kriminalist hatte geheime Daten aus dem Schengen-Computer an das Organisierte Verbrechen verkauft. Mit den Einnahmen hatte der drogenabhängige Polizist seine Sucht finanziert.

Das Schengener Informationssystem ist das Herzstück des Schengener Vertrages. An das SIS sind alle Schengenländer über ein nationales Sirene-Büro angeschlossen. Es funktioniert nach dem sogenannten »hit«-oder-»no-hit«-Prinzip. Gibt ein deutscher Beamter auf dem Flughafen Frankfurt den Namen einer Person ein, so kann er einen »Nicht-Treffer« oder, sollte die Person zur Fahndung ausgeschrieben sein, einen »Treffer« landen. Nähere Informationen sind aber nicht im SIS gespeichert, sondern müssen aus dem Sirene-Cornputer abgerufen werden, in dem die noch heikleren Daten gespeichert sind.

Beim Schengener Datenklau hatte der belgische Polizist Daten aus dem belgischen Sirene-Computer gestohlen und weiterverkauft. Theoretisch hätte er auch Informationen abrufen können, die deutsche, italienische oder französische Beamte cingegeben haben.



Offiziell hat der Belgier die Geheiminformationen an Verbrecherbanden weitergegeben, inoffiziell aber an Anwälte, die mit der Verteidigung von international tätigen Kriminellen betraut sind.

Obwohl sowohl der deutsche Innenminister Manfred Kanther als auch sein österreichischer Kollege Karl Schlögl von einem Einzelfall sprechen, sind Datenschützer anderer Meinung. »Das größte Problem bei diesen Großrechnern, die europaweit verknüpft sind, sind die Innentäter«, sagt der Bonner Datenschützer Ministerialrat Werner Schmidt. Wer an der Quelle von heiklen und für manche sehr wertvollen Daten sitzt, kann leichter manipulieren und ist auch leichter manipulierbar, wenn die Kontrollen nicht ausreichend genug sind. Selbst der deutsche Innenminister Kanther war bei einer Pressekonferenz am 16. Dezember 1997 der Meinung, daß der »Mißbrauch durch Berechtigte nie völlig ausgeschlossen werden kann«. Vor allem dann nicht, wenn es sich um einen süchtigen Beamten handelt, meint Datenschützer Schmidt: »Eine Sucht ist ein Sicherheitsrisiko, ganz gleich ob jemand drogensüchtig, spielsüchtig oder Alkoholiker ist. Das sollte auch jenen bewußt sein, die mit solchen Kollegen zusammenarbeiten.« Das Problem dabei ist, daß Polizisten gegen den eigenen Kollegen kaum vorgehen.

Daß Innentäter eine große Gefahr sind, hat auch der Datenklau aus dem Zentralcomputer des österreichischen Innenministeriums gezeigt: FPÖ-Chef Jörg Haider hatte bei einer Pressekonferenz Ende Dezember 1997 Daten aus dem Polizeicomputer präsentiert, aus denen hervorgeht, daß Abschiebungen erst mit zeitlicher Verzögerung von bis zu zehn Tagen irn Computer erfaßt werden - für Haider der Beweis, daß »Verbrecher wieder einsickern und untertauchen können«. Die Daten hatte Haider von einem Salzburger Polizeibeamten erhalten, der einen Mitarbeiter zur Computeranfrage angestiftet hatte. Der Polizeibeamte wurde bereits wenige Tage nach Haiders »Enthüllung« suspendiert. Anhand des Abfragedatums konnte genau nachgewiesen werden, wer sich die Informationen ausdrucken hatte lassen. Unklar war im Dezember 1997, ob der Salzburger Polizeibeamte die Informationen aus eigenem Antrieb besorgen ließ oder ebenfalls angestiftet worden war.

## Das europäische FBI

Informationen, die im Kampf gegen »Terrorismus«, »illegalen Drogenhandel« und »sonstige schwerwiegende Formen der internationalen Kriminalität« benötigt werden, sind im Europol-Computer in Den Haag gespeichert. Bereits 1991 haben sich die 15 Staats- und Regierungschefs der EU-Länder darauf geeinigt, ihre Bürger unter eine zentrale Polizeiaufsicht zu stellen und Europol zu gründen. Europol ist das »europäische FBI«, wie es der deutsche Kanzler Helmut Kohl bezeichnet hat. Die Euro-Polizisten wollen die Organisierte Kriminalität (OK) das Fürchten lehren. Mit allen Mitteln.

Etwa 200 Beamte kämpfen unter der Leitung des Deutschen Jürgen Storbeck gegen Drogenhandel, Schlepperwesen, Kfz-Schieberbanden und Kindesmißbrauch.

Unumstritten sind die Euro-Cops freilich nicht, denn Kritiker befürchten, daß die mit allen Privilegien und Immunität ausgerüstete Truppe durch den Kontinent zieht und in James-Bond-Manier Verbrecher verfolgt. Im Kampf gegen die Organisierte Kriminalität steht den Euro-Polizisten ab Ende 1998 ein Super-Computer zur Verfügung. Im TECS, wie der Mega-Rechner »The European Computer System« abgekürzt wird, werden alle großen Kriminalfälle der Mitgliedsländer gespeichert und können von jedem EU-Land abgefragt werden: Zehntausende Verbrechen, Hunderttausende Namen. Es werden aber auch OK-relevante Daten aus Drittländern gesammelt.

Der Speicher des Super-Computers wird eine Million Datensätze umfassen. »Das Europol-Prinzip: vorsorgliches Mißtrauen gegen alles und jeden, komplette Dossiers über Ungerechte wie Gerechte« (»Spiegel« Nr. 31/95). Europol darf Angaben über Personen speichern, »bei denen bestimmte schwerwiegende Tatsachen … die Annahme rechtfertigen, daß sie Straftaten begehen werden«. Gespeichert für den Fall des Falles. Das hat Datenschützer auf den Plan gerufen, die den Euro-Polizisten spöttisch vorwarfen, von einer Straftat zu wissen, bevor sie begangen wird. Bedenklich ist der Europol-Computer noch aus einem anderen Grund: Neben dem »Verdächtigenspeicher« gibt es auch eine »Arbeitsdatei zu Analysezwecken«. Auch Rasterfahndungen sind mit TECS kein



Problem, da alle Fälle nach bestimmten Kriterien abgelegt und verknüpft werden können. »Die Mosaiksteinchen des täglichen Geschäfts setzen acht Europol-Analytiker zusammen, um die Netzwerke der Organisierten Kriminalität aufzuzeigen«, schrieb die »Zeit« (9. 5. 1997). Die Euro-Polizisten können Verbindungen zwischen Delikten, Tätern und Gruppierungen herstellen und so Schmuggelrouten und Geldwäschekanäle aufdecken.

In dieser »Arbeitsdatei zu Analysezwecken«, so befürchten Gegner, könnten auch unbescholtene Bürger erfaßt werden. Nämlich dann, wenn sie bei den polizeilichen Ermittlungen mithelfen können: sei es als V-Männer, Zeugen oder als potentielle Opfer künftiger Straftaten.

Internationale Kooperation gibt es bei der Exekutive schon seit langem. 177 Staaten sind Teil von Interpol. Auch wenn die Kooperation mit manchen Staaten oft langwierig und nicht sehr effektiv ist, da die Auffassungen über bestimmte Straftaten differieren, gab es schon in der Vergangenheit den internationalen Datenaustausch. Das BKA übesetzt im Rahmen des polizeilichen Nachrichtenaustauschs mit Fahndern in aller Welt etwa 70000 Aktenseiten ins Englische, Französische und Spanische. Faszinierend die Statistik des Nachrichtenaustauschs: Obwohl 177 Staaten das Interpol-Abkommen unterzeichnet haben, macht der Anteil des BKA an den international verbreiteten Informationen beinahe ein Drittel aus.

# Im Visier der Rasterfahnder

**> Wie die Rasterfahndung wirklich funktioniert.**

**> Wie in der österreichischen Briefbomben-Causa gerastert worden wäre.**

**> Warum man in Deutschland mit der Rasterfahndung Probleme hat.**

**> Wie uns die Privatwirtschaft ausspioniert.**

**> Warum Supermärkte wissen, was wir am kommenden Wochenende kaufen.**

**> Wo die Daten von Scanner-Kassen landen.**

**> Was der Haken an sogenannten Sonderangeboten ist.**

**> Wie McDonald's Standorte für seine Fast-food-Kette**

**S U C H T**

## Kommissar Zufall und die Rasterfahndung

Den österreichischen Beamten der Sonderkommission Briefbomben machte »Kommissar Zufall« einen Strich durch die Rechnung. ]ust in der Woche, ab der in Österreich die Rasterfahndung gesetzlich erlaubt gewesen wäre, wurde der mutmaßliche Briefbomben-Täter gefaßt. Bei einer Verkehrskontrolle verlor der 48jährige Franz Fuchs aus der kleinen steirischen Ortschaft Gralla bei Leibnitz die Nerven und zündete eine selbstgebaute Rohrbombe. Die »Bajuwarische Befreiungsarmee«, die vermutlich nur aus Franz Fuchs bestand, hatte seit Dezember 1993 insgesamt 25 Briefbomben verschickt *(zwei* davon nach Deutschland) und drei weitere Bombenattentate verübt. Die Bilanz: vier Tote und 15 Verletzte.



Die ungelöste Briefbomben-Causa hatte den Ruf nach der neuen Ermittlungsmethode laut werden lassen. Vor allem Kriminalisten waren überzeugt, daß man mit Hilfe der Rasterfahndung dem Bomben-Hirn auf die Spur kommen könnte. »Wir wären im Zuge der Rasterfahndung ganz sicher auf Fuchs gestoßen«, meint der Generaldirektor für die öffentliche Sicherheit, Michael Sika. »Es hätte nur ein wenig länger gedauert.« Die Panikreaktion bei der Verkehrskontrolle deutet sogar darauf hin, »daß die Rasterfahndung indirekt die Festnahme von Fuchs herbeigeführt hat«, vermutet Sika. »Das hat er uns in den Einvernahmen sogar bestätigt. Er hatte gedacht, daß wir bereits vor dem 1. Oktober 1997 vorrastern und am 1. Oktober ein Ergebnis präsentieren.«

Von den neuen Ermittlungsmethoden Rasterfahndung und Lauschangriff sind aber nicht alle begeistert. Gegner orten Eingriffe in die Grundrechte des Bürgers. Man befürchtet, daß bei der Rasterfahndung viele Unschuldige im Fahndungsnetz hängenbleiben. Menschen, die überhaupt nichts mit Straftaten zu tun haben. Die Ängste sind begründet. Wer dem Täterprofil entspricht, wird zum Gegenstand der Ermittlungen. Und diese können für einen unschuldig Verdächtigten unangenehm werden und soziale Folgen nach sich ziehen, die sich nur sehr schwer bereinigen lassen. Durch die Befragung von Familienmitgliedern, Freunden und Bekannten wird man von Nachbarn rasch als Verbrecher abgestempelt, und man wird automatisch in den Polizeicomputer aufgenommen. Die Bedenken teilt auch Michael Siebrecht in seinem Buch »Rasterfahndung«: »Rechtsprobleme wirft die Rasterfahndung insbesondere deshalb auf, weil regelmäßig auf eine unbestimmte Vielzahl von Personen Zugriff genommen wird, die weder Beschuldigte, Zeugen noch Augenscheinsobjekte sind. Es ist daher zu prüfen, ob dieser Personenkreis verfassungsrechtlich überhaupt Adressat strafprozessualer Maßnahmen sein darf.« Auf diese Kritik hat ein Kriminalist die passende Antwort parat: «Wenn auf jemanden gewisse Kriterien zutreffen, ist er automatisch im Verdächtigenkreis und wird von uns befragt. Die Rasterfahndung hilft uns, daß wir nicht nach einem Jahr, sondern schon früher kommen.«

In Osterreich wurde deshalb ein eigener Rechtsschutzbeauftragter für die neuen Ermittlungsmethoden Rasterfahndung und Lausch-

angriff ernannt. Der frühere Rechtsanwalt und Verfassungsrichter Rudolf Machacek prüft sämtliche Anträge auf Lauschangriff und Rasterfahndung. Er wird aber auch alle Beschwerden behandeln, wenn sich Menschen unschuldig verdächtigt fühlen oder wenn die Exekutive »verbotene« Dateien wie Kirchenregister oder Spitalsdaten verwendet.

## Rasterfahndung »made in Germany«

In Deutschland steht man der Rasterfahndung aufgeschlossener gegenüber. Immerhin ist sie bereits seit Mitte der 70er Jahre ein gängiges Fahndungsmittel. Man setzte sie im Kampf gegen die RAF-Terroristen ein und erzielte auch Erfolge, obwohl diese selten mit der Verhaftung der Terroristen endeten.

1975 wurde in Frankfurt nach RAF-Wohnungen gefahndet. Man ging davon aus, daß Terroristen eine Wohnung unter einem falschen Namen mieten. Unter dieser falschen Identität müssen sie nicht nur die Miete zahlen, sondern auch Strom und Telefon. Da die Überweisung von einem Konto auf das Konto der Strom- oder Telefongesellschaft ein großes Risiko gewesen wäre (da die Polizei leichter eine Spur hätte aufnehmen können), nahmen die Kriminalisten weiters an, daß Terroristen die Rechnungen bar einzahlen.

In einem ersten Schritt ließen sich die Fahnder vom Elektrizitätswerk die Namen und Adressen jener Kunden geben, die bar zahlen. In einem zweiten Schritt wurden die Daten jener Behörden herangezogen, die »echte Namen« verwalten, wie etwa Meldeamt, Grundbuch, Rentenversicherung. In einem dritten Schritt wurde die Datei mit den echten Namen über jene Datei mit den Strom-Bar-zahlern gelegt. Die, die übrigblieben, wurden mit konventionellen Methoden überprüft, sprich: jede Wohnung wurde einzeln aufgesucht.

Ähnlich verlief in Deutschland eine Rasterfahndung Anfang der 90er Jahre. Die Kriminalisten suchten Schwerverbrecher, von denen man wußte, daß sie sich in bestimmten Bundesländern aufhalten, wenig Geld haben, in konspirativen Wohnungen wohnen und die »Bahncard« der deutschen Bundesbahn benützen.



Konspirative Wohnungen sind solche, in denen unter einem Decknamen Kriminalisten, Agenten, aber auch Verbrecher wohnen. Man ersuchte die Deutsche Bahn um Bekanntgabe jener »Bahncard«-Besitzer, bei denen die Zustellung des Ausweises wegen einer falschen Adresse nicht möglich war und der Betroffene sich die Karte persönlich abgeholt hat. Diese Daten wurden mit den Melde- und Kfz-Zulassungsdaten verglichen. Von jenen, die nirgends gemeldet waren, wurden die 25- bis 40jährigen herausgefiltert. Übrig blieb ein enger Verdächtigenkreis, und man fand den Täter.

## Positive und negative Rasterfahndung

Grundsätzlich stehen den Kriminalisten zwei Arten von Rasterfahndung zur Auswahl: positive und negative. Bei der positiven Rasterfahndung werden Dateien auf Eigenschaften und Merkmale durchsucht, die auf den Tater zutreffen könnten. Ist etwa bekannt, daß der Straftäter einen roten Audi A3 fuhr und einen bestimmten Mantel eines Versandhauses trug, so könnten in einem ersten Schritt von den Kfz-Zulassungsstellen sämtliche Autobesitzer eines roten Audi A3 herausgefiltert werden. In einem zweiten Schritt könnte das Versandhaus anhand der Artikelnummer des Mantels und der Kundenkartei sämtliche Käufer des Mantels bekanntgeben. Werden nun in einem dritten Schritt diese Dateien verglichen, bleiben jene hängen, auf die beides zutrifft. Diese werden dann mit den herkömmlichen Methoden überprüft.

Die positive Rasterfahndung kann aber nicht bei der Bekämpfung der Organisierten Kriminalität oder des Terrorismus eingesetzt werden, da sowohl Mitglieder der OK als auch Terroristen in der Anonymität untertauchen. Deshalb gibt es die negative Rasterfahndung. Bei diesem Verfahren werden Definitionen erstellt, die auf den Täter *nicht* zutreffen. Eine Datei, in der sich der mutmaßliche Täter befinden soll, wird durch Löschen jener Personen, die nicht als Täter in Frage kommen, auf eine kleine Gruppe von »Verdächtigen« eingeschränkt. Im Falle der RAF-Terroristen wurde die große Gruppe der Stromkunden auf die kleine »Verdächtigen-Gruppe« der Barzahler verkleinert. Diese Methode wird mit anderen Datei-

en wiederholt, bis eine überschaubare Anzahl von Verdächtigen vorliegt. »Eine Rasterfahndung macht nur dann einen Sinn, wenn die Gruppe der zu überprüfenden Personen relativ klein ist«, bestätigt ein Kriminalist des BKA in Wiesbaden. Wenn 100 bis 150 Verdächtige übrigbleiben, dann »kann man damit etwas anfangen«.

## *Kleine und große Rasterfahndung*

Doch so einfach ist die Rasterfahndung nicht zu realisieren. »85 Prozent sind Ermittlungsarbeit, nur 15 Prozent EDV-Arbeit«, erklärt Generaldirektor Michael Sika. Es geht darum, zu klären, welche Daten benötigt werden, wo sich diese befinden und wie sie aussehen. »Es kommt auf die Aufbereitung der Daten an«, betont Sika. Bevor die Dateien gerastert werden können, müssen sie in eine einheitliche Struktur gebracht werden. Die Dateien für eine Rasterfahndung können sich die Kriminalisten fast überall besorgen. Bei der kleinen Rasterfahndung - Strafrahmen ab drei jähre - dürfen nur öffentliche Dateien miteinander verknüpft werden. So etwa das Kfz-Zulassungsregister, die Wählerevidenz und die Datenbank des Hauptverbandes der Sozialversicherungsträger. Bei der großen Rasterfahndung - Strafrahmen über zehn Jahre (Kapitalverbrechen) - können die Ermittler auch auf »private« Dateien zurückgreifen, wie etwa Kundendateien von Versandhäusern, von Fotohandelsketten, Sportgeschäften oder Supermärkten.

Aber gerade hier entsteht das Problem. Denn die vielen »privaten« Datenbanken haben auch unterschiedliche Betriebssysteme. Dafür sind Konvertierungsprogramme notwendig. Jede Rasterfahndung setzt sich folglich aus Hunderten Teilschritten zusammen. Die meiste Arbeit kommt auf die EDV-Beweissicherungsgruppe zu, die sich zuerst im Österreichischen Datenverarbeitungsregister informieren muß, wer welche Daten verarbeitet. Dann wird entschieden, von welchen Unternehmen Informationen benötigt werden. Die Datenbankbesitzer wiederum, ob Supermarkt oder Fußballverein, müssen ihre Daten vorselektieren. Die Gefahr dabei: gewisse Personen könnten aus der Datei gelöscht werden. Sika: »Eine große



Rasterfahndung nimmt etwa neun Monate in Anspruch.« Auf Knopfdruck geht gar nichts. Außerdem können die Kriminalisten nicht von sich aus aktiv werden. Für die kleine Rasterfahndung ist der Beschluß eines U-Richters notwendig, bei der großen die Zustimmung eines Dreier-Richtersenats. Daten über die rassische Herkunft, religiöse Überzeugungen, Gesundheit oder Sexualgewohnheiten dürfen für keinen Datenabgleich herangezogen werden.

Welcher ungelöste Kriminalfall in Österreich künftig mit Hilfe der Rasterfahndung geklärt werden soll, steht noch nicht fest. Was auch einigen verdeckten Drogenfahndern, Mitgliedern der Staatspolizei und Agenten des Heeresnachrichtenamtes (HNA) und Heeresabwehramtes (HAA) zu einer Verschnaufpause verhilft. Denn im Zuge von Rasterfahndungen werden immer wieder konspirative Wohnungen von Under-Cover-Agenten und Kriminalisten als solche enttarnt. Drogenfahnder, die, um Infos aus der Szene zu bekommen, unter einer anderen Identität leben, würden ungewollt von den eigenen Kollegen entlarvt. Denn konspirative Wohnungen sind so geheim, daß nicht einmal die obersten Polizeidienststellen davon etwas wissen dürfen.

## *»Völlig veraltet und inkompatibel«*

Im Bundeskriminalamt in Wiesbaden versteht man die Aufregung, die die Rasterfahndung im Vorfeld des Beschlusses in Österreich ausgelöst hat, überhaupt nicht. »Das ist eine ganz normale Ermittlungsmethode«, erklärt BKA-Sprecher Jürgen Stoltenow. Für deutsche Kriminalisten ist der »automationsunterstützte Datenabgleich«, wie die Rasterfahndung juristisch genannt wird, nichts Besonderes.

In Deutschland liegt die letzte Rasterfahndung aber schon Jahre zurück. Offiziell ist es der Datenschutz, der den Kriminalisten jede Rasterfahndung untersagt; außerdem gebe es ohnehin keinen Bedarf für große Rasterfahndungen, da die Zeit des Terrorismus vorbei sei und Fahndungsansätze wie Barzahler nicht mehr aktuell seien. Inoffiziell aber ist es die rasante Weiterentwicklung der

Computertechnik, die deutschen Kriminalisten eine Methode verwehrt, die sie selbst erfunden haben. Es gibt große Probleme mit dem Großrechner INPOL, dem elektronischen Informationssystem der Polizei. Das Betriebssystem des Siemens BS2000-Rechners ist »völlig veraltet« und »inkompatibel mit jeder Software, die es auf der Welt gibt«, bestätigt ein Insider. Die großen Rasterfahndungs-Erfolge wurden in Deutschland zu einer Zeit erzielt, in der deutsche Großfirmen zur Förderung der heimischen Wirtschaft nur Siemens-Systeme in Betrieb hatten. Jetzt sind überall Rechner im Einsatz, die von Erzeugern auf der ganzen Welt stammen.

Trotzdem: »Die Rasterfahndung wird die Ermittlungsmethode der Zukunft.« Kriminalisten sind überzeugt, daß bei der Verfolgung von Straftätern der Datenabgleich das Instrument schlechthin wird. In Zeiten, in denen das ganze Leben automatisiert abläuft, kommt den in den Datenbanken gespeicherten Informationen eine wichtige Rolle zu. Ob Daten von Kredit- oder Bankomatkarten, ob Kundenkarten in den Supermärkten oder Mitglieds-Cards vom Fitneß-Club. Auf der Jagd nach Tätern wird die Exekutive im EDV-Zeitalter zeitgemäße Methoden anwenden. Was jetzt noch Gegner auf den Plan ruft, wird in einigen Jahren ganz normaler Polizeialltag.

## *Die tägliche Rasterfahndung in der Privatwirtschaft*

»Welche meiner Kunden haben blaue Augen, wie viele neigen zu übermäßigem Alkoholgenuß, sind zwischen 30 und 35 Jahre alt oder kaufen Mineralwasser immer dann, wenn sie auch Bier kaufen.« So fragen schon jetzt Marketingstrategen und Wirtschaftsexperten großer Firmen ihre Datenbanken ab, wenn sie mehr über ihre Kunden wissen wollen. Auf Knopfdruck wird eine Liste ausgedruckt, auf der all jene aufscheinen, die dem Suchkriterium entsprechen. Das Ergebnis beinhaltet zum Teil anonyme Daten, zum Teil aber auch Namen und Adressen, wenn die betreffenden Personen Kundenkarten besitzen. Firmen wie Rewe, Merkur, Tengelmann oder Billa haben ihre Kunden schon längst durchschaut. Der Kunde das Unternehmen allerdings nicht. Die angewandten Praktiken sind nur Insidern bekannt.



Gegner der polizeilichen Rasterfahndung sind sich offenbar nicht bewußt, daß in der Privatwirtschaft täglich gerastert wird, daß Unternehmen - von der Supermarktkette über das Versandhaus bis zum Mobilfunkunternehmen - die Informationen, die sie über ihre Kunden speichern, auch akribisch genau auswerten. Das Instrument, das diese Zusammenhänge, Trends und Eigenschaften überhaupt aufzeigt, nennt sich Data-Mining (»Daten-Analyse«}. Und Data-Mining ist exakt dieselbe Technologie, die auch bei der polizeilichen Rasterfahndung verwendet wird.

Der Unterschied liegt darin, daß nicht Zulassungs-, Melde- und kriminalpolizeiliche Daten verglichen werden, sondern Kaufdaten von Kunden. »Wir haben unser Programm dem Innenministerium angeboten, denn ob ich Kundendaten rastere oder kriminalpolizeiliche Informationen, macht vom System her keinen Unterschied«, bestätigt Gerhard Graf von SAS Institute, dem weltweit führenden Anbieter von Data-Mining-Programmen. SAS Institute ist Marktführer sowohl in Deutschland als auch in Österreich.

Data-Mining ist, bildlich beschrieben, ein »Suchhund, den man von der Kette läßt«. Beim Data-Mining analysieren hochkomplizierte Computerprogramme die Datenmengen in den Rechnern und filtern (bzw. rastern) jene Information heraus, die für ein Unternehmen interessant sind. Wenn die Kassierin bei Rewe, Spar oder Merkur die gekauften Waren über die Scannerkasse zieht, scheinen diese Daten nicht nur in Form einer Rechnung auf, sondern landen im Zentralrechner. Mit diesen Daten kann das Kaufverhalten »berechnet« werden. Sind zusätzlich auch Kundendaten bekannt, kann ,sogar vorhergesagt werden, was Frau X am kommenden Wochenende mit hoher Wahrscheinlichkeit kaufen wird.

Mit Hilfe von Data-Mining wird beispielsweise festgestellt, daß viele Kunden Sekt immer gemeinsam mit Orangensaft oder Bier gleichzeitig mit Mineralwasser kaufen. Das gleiche Prinzip wird bei diversen anderen Produktkombinationen angewandt. Bei Sonderangeboten gibt es deshalb immer den entsprechenden »Gegenartikel«. Wenn bei Produkt A der Preis durch ein Sonderangebot nach unten geht, wird er gleichzeitig bei B angehoben. Damit können die Konzerne immer gleiche Gewinne einkalkulieren. Wer also in einem Supermarkt vom Bier-Angebot verlockt wird, sollte den Mineralwasser-Preis kontrollieren.

## Wie Kunden gescannt werden

Beinahe keine große Supermarktkette vertraut heute noch auf die gute, alte Methode, bei der die Kassierin den Warenpreis in die Kassa eintippt. Nur Hofer in Österreich macht hier eine Ausnahme. Scanner-Kassen, bei denen der Strichcode über einen Laserstrahl gezogen wird, haben die Arbeit in fast allen anderen Großmärkten sehr vereinfacht und gleichzeitig auch die Möglichkeiten der Marketingstrategen verbessert. Wöchentlich werden die Scanning-Daten von etwa 2000 Supermarktfilialen in Deutschland und 300 in Österreich zu den Marktforschern vom Full-Service-Marktforschungsunternehmen ACNielscn geschickt. Online. Dort werden die Daten analysiert und ausgewertet. Denn die einzelnen Filialen von Tengelmann, Spar oder Edeka werden nicht alle mit denselben Produkten bestückt. Abhängig von der Bevölkerung, die in dem Einzugsgebiet wohnt, werden sie mit unterschiedlichen Mengen versorgt. In Gebieten mit vielen Arbeitslosen oder Wcnigverdienern werden mehr Billigprodukte in den Regalen zu finden sein.
Mit den Scanning-Daten wird übrigens auch die Toleranzgrenze von Preisen ausgelotet: bei welchem Preis Konsumenten eine Ware kaufen, und bei welchen Preis sie im Regal liegenblcibt.

## Die Methoden des Data-Mining

»Grundsätzlich stehen beim Data-Mining zwei Möglichkeiten zur Auswahl«, erklärt Gerhard Graf. Bei Variante 1 werden alle Kunden nach bestimmten Kriterien segmentiert und das Kundcnverhalten der Gruppe analysiert. Nach dem Motto »guter Kunde/schlechter Kunde« schaut man: Wer bringt dem Unternehmen viel Geld, wer wenig? Welche Kunden kaufen wann und wo diese oder jene Produkte. Die britische Warenhauskette Woolworth hat z. B. die Verkaufsdaten von 80 Wochen in ihrem System gespeichert und kann damit zwei gleiche Saisonen vergleichen, Abweichungen analysieren und darauf reagieren.
Es ist kein Zufall, daß der österreichische Mobilfunkanbieter max.mobil bei seiner Handy-Telefonwertkarte einen »Mondschein-



Tarif« anbietet. Der Tarif, der mit 3 Schilling pro Minute als sensationell bezeichnet werden kann und der auch lautstark beworben wird, hat allerdings einen ziemlich großen Haken: Durch Data-Mining wurde das max.mobil-Kundenverhalten analysiert. Das Ergebnis: In der Zeit, in der der Mondschein-Tarif gilt, zwischen 10 Uhr abends und 4 Uhr früh, fällt nur 1 Prozent aller Gespräche an. Die meisten Kunden, die sich von dieser Werbebotschaft haben fangen lassen, werden vermutlich nie den Mondschein-Tarif nutzen.
Variante 2 beim Data-Mining ist auf den einzelnen Menschen ausgerichtet, der namentlich bekannt ist. Eine »Big-Brother-is-watching-you«-Methode. Diese Daten sind für die deutsche Telekom genauso interessant wie für die Post und Telekom Austria. In einer Zeit, in der viele private Telefonbctreiber auf dem Markt präsent sind, wollen Telekom und PTA ihre Kunden »besser kennen«. Mit speziellen Kundenprogrammen möchte man jene an das Unternehmen binden, die viel telefonieren und dem Unternehmen deshalb viel Geld bringen. Die Deutsche Telekom hat in einer Datenbank mit 13 Terabyte die Daten aller Telefongespräche der vergangenen 80 Tage im Online-Zugriff und kann das Telefonierverhalten genau analysieren. Sie kann z. B. mit ihren Daten nicht nur generelle Trends erkennen - etwa wie viele Kunden zu welcher Zeit in die USA telefonieren -, sie kann auch das Gesprächsverhalten jedes einzelnen, namentlich bekannten Kunden analysieren.
Eine Horrorvision für Österreichs Ärzte wird im Laufe des Jahres 1998 Realität: 1997 wurde in der Steiermark und in Oberösterreich mit einem Versuchsprojekt begonnen, bei dem die sogenannten Ärztefolgekosten unter die Lupe genommen werden - welcher Arzt verschreibt welche Medikamente? Ein Arzt, der überdurchschnittlich große Mengen vom Schlafmittel Rohypnol verschreibt, wird kontrolliert. Ein Mediziner, der seine Patienten nicht zum Physiotherapeuten, sondern ständig auf teure Kuren schickt, macht sich ebenfalls »verdächtig«.
»Mit Hilfe von Data-Mining werden schwarze Schafe ausgeforscht«, erklärt ein Experte. »Verschreibt ein Arzt nur Medikamente von Bayer oder Hoffmann-La Röche, läßt das bestimmte Rückschlüsse zu.« Steuerzahler sind von diesem Projekt, das von allen

Krankenkassen Österreichs realisiert wird, begeistert. Die Ärzteschaft sieht das freilich anders.

»Mit Hilfe von Data-Mining werden wir ohne unser Wissen durchleuchtet und für ein Unternehmen, eine Organisation oder eine Behörde zum >gläsernen Kunden.« »Diesen Ausdruck höre ich nicht gerne, da ich die Technologie kenne, die dahinter steckt«, meint der Experte. Aber selbst er ist sich des Problems bewußt: »Man wird immer mehr Informationen über uns sammeln. Alles, was an Daten über jemanden aufzutreiben ist, wird gespeichert und analysiert.« Seine Hoffnung: »Es wird eines Tages so viel Information über uns geben, daß man die Menge gar nicht mehr überblicken kann.« Der Mensch hat diesen Überblick schon lange verloren, hochtechnische Computersysteme hingegen nicht. Ihnen wurde bereits beigebracht, selbst zu denken.

## Wenn der Computer selbständig denkt

Das Computerprogramm wird trainiert wie ein Sportler. Anhand eines konkreten Beispiels zeigen die Data-Mining-Experten dem Programm, wie es sich verhalten soll, und lassen es dann auf den gesamten Datenbestand los. »Neuronale Netze«, so der Fachausdruck, sprengten alle bisher dagewesenen Visionen. Ein Computerprogramm, das selbständig denkt und laufend dazulernt, wandert durch einen Rechner und sammelt alle Informationen, die zu einer Person gehören. Werden beispielsweise 20 verschiedene Datenbanken miteinander verknüpft, sammelt das neuronale Netz alle Informationen: Es wird mit einem Namen auf Reisen geschickt und kommt mit einer großen Datenmenge retour. Ist der Name Karl Muster und ein bestimmtes Geburtsdatum die Ausgangsinformation, so sucht das Programm alle Dateien nach einem Karl Muster mit diesem Geburtsdatum ab. Das ist noch nichts Besonderes. Findet das neuronale Netz in einer Datei Zusatzinformationen zu diesem Karl Muster, wird mit diesen Zusatzinformationen weitergesucht. Das Ergebnis ist ein Karl Muster, von dem man mehr weiß als der Betroffene selbst.

Die Neckermann Versand AG setzt auf neuronale Netze in der



Bonitätsprüfung. Die etwa 8 Millionen Neckermann-Kunden geben pro Tag im Durchschnitt 50000 Bestellungen auf. Etwa 8000 Bestellungen betreffen Neu- bzw. Kreditkunden. Durch neuronale Netze kann Neckermann 80 Kunden zusätzlich richtig einschätzen und als »gut« klassifizieren. Vor dem Einsatz dieser Technologie wurden sie als »schlecht« klassifiziert, hatten also keine Kredite erhalten. Bei einem durchschnittlichen Bestellwert von 250 bis 2500 Mark und 300 Bestelltagen im ]ahr hat Neckermann durch die neuronalen Netze mehrere hunderttausend bis mehrere Millionen Mark durch nicht eingetretene Forderungsausfälle eingespart.

Wie die neuronalen Netze bei Neckermann arbeiten, ist einfach erklärt: Ruft ein Kunde an, werden Name und Adresse im Rechnersystem auf Reisen geschickt. In der Neckermann-Datenbank werden sie mit Kaufkraftdaten, statistischen Erhebungen, Nielsen-Daten verglichen und dann mit der Kundendatenbank abgestimmt, ob schon einmal ein Kunde mit demselben Namen bestellt hat. Pech können potentielle Kunden schon aus einem simplen Grund haben. Wenn sie etwa an einer »schlechten Adresse« oder in »berüchtigten Vierteln« wohnen, wo es viele Arbeitslose, Vorbestrafte oder auch nur ein geringes Einkommensniveau gibt.

Falcon (Falke) nennt sich jenes System, das bei der deutschen Gesellschaft für Zahlungssysteme (GZS) seit 1995 Kreditkartenbetrüger überführen soll. Das neuronale Netz, das selbstdenkend die Kreditkartenabrechnungen durchsucht, deckt dabei Unregelmäßigkeiten auf.

Da die Zahl der Kreditkartenmißbräuche ständig steigt, setzt die GZS seit 1996 zusätzlich die beiden Systeme »Falcon-Realtime« und »Falcon-Expert« ein. »Beim Kreditkartenmißbrauch haben wir es meist mit organisierten Banden zu tun«, bestätigt eine GZS-Sprecherin. »Nur wenn wir rasch reagieren können, haben wir auch eine Chance.«

Falcon-Realtime erhöht die Reaktionsgeschwindigkeit, Falcon-Expert erkennt »Betrugsmuster«. Der neuronale Falke errechnet während eines Autorisierungsprozcsses - das ist jener Vorgang, bei dem die Daten von einem Terminal etwa in einem Geschäft an die Zentrale im Heimatland übermittelt und genehmigt bzw. abgelehnt werden -, wie hoch die Wahrscheinlichkeit eines Mißbrauchs ist.

Durch das Falcon-System konnte die GZS feststellen, in welchen Ländern und bei welchen Partnern sich Mißbräuche konzentrieren. Die meisten Betrügereien mit deutschen Karten finden übrigens im Ausland statt.

## Im Visier der Marketing-Strategen

Es ist kein Zufall, wo McDonald's seine Burger-Restaurants errichtet, wo Tankstellen, Bankfilialen oder ßaumärkte gebaut werden. Es ist auch kein Zufall, wo ein Plakat hängt, auf dem für ein neues Automodell geworben oder wo die Eröffnung eines Mübelmarktes angekündigt wird. Immer öfter verlassen sich Marketingstrategen großer Unternehmen auf Geo-Marketing.

Hinter diesem fast vertraulich klingenden Begriff steckt ein relativ leicht durchschaubares und völlig logisches Marketing-System. Beim Geo-Marketing werden elektronische Landkarten mit statistischen Informationen aus der Volkszählung und mit Daten einiger anderer Erhebungen verknüpft. Diese Informationen beinhalten Kaufkraftdaten, Bevölkerungsdaten und Informationen, an die wir nicht denken. Diese werden dazu genutzt, um uns zu durchschauen, um uns sogar ein wenig zu manipulieren.

Als Mercedes im Winter 1996/97 sein neues Allradmodell auf den Markt brachte, versuchte man, die Autos mit gezielter Werbung an den Mann zu bringen. Mit Geo-Marketing hatte man den gewünschten Erfolg: Man besorgte sich Daten von Gebieten, in denen überdurchschnittlich viele Besserverdiener wie Ärzte, Rechtsanwälte und Akademiker wohnen. Diese Information kombinierte man mit geografischen Daten. Man wählte höherliegende Gegenden mit steileren Straßen aus, in denen zum einen überdurchschnittlich viel Schnee fällt und zum anderen der Schnee lange liegen bleibt. Als in jenen Gebieten Deutschlands und Österreichs, auf die all diese Gemeinsamkeiten zutrafen, heftiger Schneefall einsetzte, wurden alle Bewohner aus diesem Zielgebiet direkt angeschrieben und über den neuen Mercedes-Allrad informiert. Der Ansturm auf die Mercedes-Händler blieb nicht aus.

»Geo-Marketing hat eine völlig neue Welt eröffnet«, sagt der



St Pöltner Ziviltechniker Hanns Schubert. »80 Prozent der Entscheidungen des Menschen haben einen Raumbezug, Menschen mit ähnlichen Einstellungen leben in ähnlicher Umgebung.«

Bis vor wenigen Jahren war die kleinste geografische Einheit eines Landes die Gemeinde bzw. die Katastralgemeinde. Damit waren die Marketing-Experten nicht zufrieden, denn eine Gemeinde kann 50 Einwohner haben, wie Gramais in Tirol oder 50000 wie St. Polten oder gar 1,7 Millionen wie Hamburg. »Auch Postleitzahlen sind für Markcting-Zwecke völlig ungeeignet«, erklärt Schubert. Unter der Postleitzahl A-6452 Hochsölden sind ganze 15 Postfächer zu finden. Unter der Postleitzahl A-1100 Wien-Favoriten scheinen 86256 Zustelladressen auf.

In Österreich ist heute die kleinste geografische Einheit der Zählsprengel. Exakt 8817 gibt es davon, in jedem gibt es im Durchschnitt 350 Haushalte, in denen 1 000 Menschen wohnen. In Deutschland gibt es ähnliche Einheiten. Und deren Daten kennt man ganz genau - Alter und Geschlecht, Bildung, Familienstand, Haushaltsgrößen, Gebäudenutzung, Ausstattungskategorie der Wohnung etc. Eigentlich alles, bis auf den Namen.

Die demografischen Daten stammen aus der Volkszählung und sind sehr genau. Auf Knopfdruck wissen Geo-Marketing-Experten, wie viele geschiedene, verwitwete oder ledige Menschen in einem Gebiet wohnen. Ein Mausklick, und die Information, ob ein Haus zwei, drei oder vier Wohnungen hat, ob diese mit Bad/Dusche und WC ausgestattet sind und wie viele Menschen darin leben, erscheint auf dem Computerbildschirm. Für Geo-Marketing-Experten ist der Bürger ein offenes Buch, ein »gläserner Mensch«. Denn die kleinste Einheit ist für ihn der Häuserblock; er hal eine Adresse, und diese kann - theoretisch und auch praktisch - mit einer Datei verknüpft werden, in der Adressen und Narnen aufscheinen - dem Telefonbuch. Zwar sind einige Bürger nicht im Telefonbuch, da sie auf einen Eintrag verzichtet haben, dennoch ergeben die verbliebenen Eintragungen Informationen, von denen sich ganz einfach Schlüsse ableiten lassen. Durch die auf dem Markt erhältlichen Telefon-CDs läßt sich diese Kombination von statistischen und personenbezogenen Informationen sehr leicht realisieren, da die gewünschten Daten schon im Computerforrnat vorhanden sind. Freilich widerspricht dies dem Datenschutz. »Wir machen es nicht.

Ob es andere tun, weiß ich nicht«, rechtfertigt sich Schubert. Er verkauft zwar Geo-Marketing-Programme, »aber der Messerhersteller ist ja auch nicht der Mörder«.

»Geo-Marketing - First Step« nennt sich das auf den österreichischen Markt zugeschnittene Produkt aus dem ArcAustria-Programm. Das Paket, das 50000 Schilling kostet, beinhaltet keine demografischen Daten, zeigt aber, wie viele Haushalte es in den definierten Gebieten gibt und wie viele Einwohner darin leben.

Geo-Marketing gehört ebenso wie Data-Mining zum Standard-Repertoire großer Konzerne. McDonald's beispielsweise verwendet Geo-Marketing zur Standortsuche. Bevor McDonald's ein neues Fast-food-Eokal eröffnet, wird unter anderem exakt erhoben, wo wie viele Jugendliche wohnen, wo es wie viele Schulen und Kindergärten gibt, wo ein Einkaufszentrum in der Nähe ist, von dessen Kundenstrom man profitieren könnte. Ohne Geo-Marketing waren fünf von zehn neuen Standorten optimal, mit Geo-Marketing sind es acht von zehn.

Auf dieselbe Art und Weise gehen auch Boutiquen vor. Sie wollen wissen, ob innerhalb von fünf bis zehn Gehminuten um einen Standort genügend junge Menschen zwischen 14 und 18 Jahren wohnen, die sich für Mode interessieren und genügend Geld haben. Mit Geo-Marketing scheinen auf einer Landkarte nicht nur die gewünschten Informationen auf, sondern dazu noch die Schulen der Umgebung, Bus-, U-Bahn- oder Schnellbahn-Stationen und sogar Geschäfte der Konkurrenz.

»Experten gehen davon aus, daß bis zum Jahr 2000 rund 400 Milliarden Dollar weltweit in diese Informationssysteme gesteckt werden«, schrieb der »Kurier« bereits am 27. Oktober 1994. Vier Jahre später wird diese Prognose von den Experten korrigiert: Man rechnet sogar mit 500 bis 600 Milliarden weltweit.

## Mit Geo-Marketing Verbrechern auf der Spur

Verbrechen vorhersagen? Würden die Innenministerien Geo-Marketing nützen, so könnten bestimmte Verbrechen verhindert werden. Durch Geo-Marketing kann nämlich exakt festgestellt



werden, wo sich Vergewaltigungen häufen, wo Einbrüche zunehmen, wo Betrüger besonders erfolgreich sind etc. Voraussetzung dafür sind aber exakte Angaben, die die Polizisten in ihren Protokollen berücksichtigen müßten. Sobald es einheitliche Kriterien gibt, können die Fälle untereinander verglichen und Parallelen aufgezeigt werden.

Genauso wie im wirtschaftlichen Bereich könnten Schmuggelrouten oder die Einbrechertouren prognostiziert werden. »Man kann dann mit ziemlicher Sicherheit sagen, wo das nächste Verbrechen stattfinden wird«, erklärt der St. Pöltner Ziviltechniker Hanns Schubert. »Kriminelle verhalten sich nach einem bestimmten Schema, haben gewisse Gewohnheiten und verhalten sich nach dem >Gleich-und-gleich-gesellt-sich-gern-Muster<.« In den Vereinigten Staaten werden Verbrechen bereits auf diese Art »berechnet« und gefährdete Gebiete oder Stadtteile unter besonderen Schutz gestellt.

## Vom Handy-Kunden bis zum Weinliebhaber

Wer sich ärgert, weil D2, D1 oder Mobilkom keine GSM-Funkstation in seiner Nähe baut und er deshalb mit dem Handy nicht telefonieren kann, ist vermutlich Opfer des Geo-Marketings geworden. Denn bei der Planung von Leitungen wird dieses System angewandt. Gemeinden, in denen Menschen wohnen, die mobiler sind, mehr verdienen und deren Bildungsstand höher ist, bekommen eher eine Funkstation vor ihre Nase gesetzt als Gemeinden oder Bezirke mit Arbeitervierteln.

In der Chefetage der deutschen Weinhandelskette Jacques Weindepot ist das Geo-Marketing bereits unentbehrlich. Durch zielgenaue Werbekampagnen in Form von Postwurfsendungen wurde der Kundenzustrom verdreifacht. Wer also an seiner Haustür ein Flugblatt von Jacques Weindepot vorfindet, kann erleichtert sein - er gehört zur kaufkräftigen Elite des Landes. Will man potentielle Kunden auf eine Weinaktion aufmerksam machen, so sucht man in einem ersten Schritt Gebiete mit hohem Anteil an Maturanten und Akademikern und einem hohen Anteil von Männern im Alter

zwischen 40 und 60 Jahren (in dieser Kategorie sind angeblich die meisten Weingenießer zu finden). Gebiete, in denen beide Merkmale vorkommen, werden auf einer elektronischen Landkarte extra ausgewiesen. Möchte man aber nur eine bestimmte Anzahl von Flugblättern verschicken, so werden die einzelnen Gebiete nach Wertigkeit sortiert, um das Zielgebiet zu verkleinern. Danach wird ein Werbemittelverteiler-Unternehmen engagiert, das diese Gebiete auch in anderen Fällen mit Postwurfsendungen versorgt.

Wer sich wundert, warum in seiner Möbelhaus-Filiale nur billige Möbel angeboten werden, in jener 50 Kilometer entfernten, aber qualitativ und preislich gehobenere Kästen, Schränke und Sitzgarnituren, hat unbewußt mit Geo-Marketing Bekanntschaft gemacht. Mit einer Form aber, bei der auch Namen im Spiel sind. Ein Standort wird dabei mit den Adressen der Kunden verknüpft, um das Einzugsgebiet darzustellen. Auf einer elektronischen Landkarte wird farblich dargestellt, woher die Käufer kommen - je dunkler, desto mehr Kunden kommen aus dem betreffenden Gebiet. Diese Daten werden dann mit den Kaufkraftdaten verglichen. Ergibt die Analyse, daß im Einzugsgebiet der Filiale ein hoher Anteil an Arbeitern, Pensionisten sowie Single- und Zwei-Personen-Haushalten festzustellen ist, wird in der Filiale das Sortiment auf diese Bevölkerungsschicht abgestimmt, und das bedeutet billige Möbel. Ähnlich werden auch Plakatstellen errechnet - Rasenmäher werden dort beworben, wo es viele Grünflächen gibt, ebenso Kamingriller oder Gartenmöbel.

Wenn in den kommenden Jahren durch die Fusion zwischen der Bank Auslria und der CA einige Filialen verschwinden, wird dies mit Geo-Marketing passieren. Der Standort der Filialen wird mit statistischen Daten der Volkszählung und Kundendaten kombiniert. Filialen bleiben dort bestehen, wo das Einzugsgebiet am größten ist. Aber auch dort, wo die Gefahr besteht, daß Kunden zu einem anderen Bankinstitut abwandern.

# Kranksein ist gefährlich

> Wie lange die Gesundheitsdaten gespeichert werden.

> Wie anonym die »anonyme« Aidsstatistik wirklich ist.

> Welche Unternehmen HIV-Tests bei Bewerbern legal oder illegal vornehmen.

> Wie via Telefon aus den USA Krankendaten aufgelesen werden können.

> Warum im Wiener Allgemeinen Krankenhaus die PCs mit Stahlseilen befestigt werden.

> Wie oft Hacker in die Datenbanken der Spitäler einbrechen.

> Warum eine Fernoperation die Gesundheit gefährden kann.

## Die HIV-Tests des österreichischen Außenministeriums

Für manch österreichische Bundesbehörde gilt das Verbot, HIV-Tests ohne Einwilligung der Betroffenen durchzuführen, offenbar nicht. Regelmäßig läßt ein Ministerium seine Mitarbeiter ohne ihr Wissen testen. Konkret ist es das österreichische Außenministerium.

Jene Beamte, die als Botschafter, Attaches oder auch Botschaftsangehörige ins Ausland geschickt werden sollen, werden »routinemäßig«, wie ein Mediziner bestätigt, untersucht: Im Zuge der Tropentauglichkeitsuntersuchung wird auch ein HIV-Test gemacht.

»HIV-positiv ist ein regelmäßiger Befund«, bestätigt der Mediziner. Von den etwa 100 Ergebnissen pro ]ahr sind etwa ein bis zwei positiv.

Die Tests werden damit begründet, daß das Außenministerium vor

allem bei jungen Diplomaten und Akademikern über Infektionen Bescheid wissen muß, damit nicht Zeitplan und Ablöse-Rhythmus durcheinandergeraten. Einen Beamten früher als geplant ersetzen zu müssen sei mit enormem bürokratischem Aufwand verbunden. Das österreichische Außenministerium ist kein Einzelfall. Viele Konzerne und Unternehmen, die international tätig sind, lassen ihre Mitarbeiter auf Tropenlauglichkeit und damit auch auf HIV testen. Ulrich Marcus, Sprecher des Berliner Robert-Koch-Instituts, kritisiert diese Tests, die zum Teil mit, aber auch ohne Einwilligung der Betroffenen durchgeführt werden. Auch Lufthansa und AUA veranlassen bei Bewerbern im Rahmen der Einstellungsuntersuchungen HIV-Tests. Ab 1999 läßt die AUA sogar Cholesterinwerte testen. Die Begründung: Durch die Übersee-Einsätze müßte man über Infektionen Bescheid wissen. »Diese Argumentation halte ich nicht für ganz einleuchtend«, meint Ulrich Marcus. »Auch ein HIV-Positiver kann einen solchen Beruf ausüben. Mit den derzeitigen Behandlungsmethoden kann die Krankheit mindestens zehn Jahre unterdrückt werden.«

Marcus ortet in Deutschland eine Art Diskriminierungsgesetzgebung, einen »Graubereich«, in dem die Unternehmen die HIV-Tests durchführen. »Ein Musterprozeß gegen die Lufthansa wäre ideal«, meint der Sprecher des Robert-Koch-Instituts. Das Problem dabei ist aber, daß jene, die HIV-negativ sind, kein Interesse an einem Prozeß haben, weil es sie nicht betrifft. Marcus: »Die HIV-Positiven wollen nicht vor Gericht, damit ihre Infektion nicht publik wird.«

Schon einmal ging ein Patient, bei dem ohne dessen Wissen ein HIV-Test gemacht worden war, vor Gericht. Und gewann. Ein Hautarzt hatte einem 40jährigen am 1 1 . Oktober 1989 Blut entnehmen und dieses auf HIV-Antikörper untersuchen lassen. Die Klage auf Zahlung von Schmerzensgeld wurde am 8. Februar 1995 vom Landesgericht Köln (25 O 308/92) bestätigt. Das Gericht kam zum Schluß, daß »die Vornahme/das Veranlassen eines HIV-Antikörper-Tests ohne Einwilligung des betreffenden Patienten wie jede andere diagnostische Maßnahme, die ohne Einwilligung des Patienten vorgenommen wird, ein Verstoß gegen das Selbstbestimmungsrecht dieses Patienten ist. Ob nach dem damaligen Krankheitsbild aus der Sicht des Beklagten ein solcher Test medizinisch indiziert war, ist in diesem Zusammenhang unerheblich. Die Indikation kann die Einwilligung des Patienten nicht ersetzen.« Die Verletzung des Selbstbestimmungsrechts sei eine schwere Persönlichkeitsverletzung. Dem Klager wurden 1 500 Mark Schmerzensgeld zuerkannt. HIV-Tests sind nur für Prostituierte zwingend vorgeschrieben. Sie müssen sich im Abstand von mindestens drei Monaten einem HIV-Test unterziehen.



Die Zahl der illegal durchgeführten HIV-Tests wird sich in Zukunft weiter steigern. Wer in seiner Krankengeschichte oder auf einem Befund zufällig die Worte »ELIZA« oder »Wcsternplot« liest - das sind die Bezeichnungen der derzeit gängigen HIV-Tests -, weiß, daß sein Blut auf HIV untersucht wurde.

Wie groß die Angst vor Aids ist, beweisen Versuche einiger Staaten, HIV-Tests für Touristen einzuführen. 1996 hatte man in Rußland diese Idee und wollte auf dem Flughafen von jedem ankommenden Passagier Blut abnehmen. Abgesehen davon, daß die hygienischen Zustände in Rußland einiges zu wünschen übriglassen, sind diese Tests Eingriffe in die Menschenrechte. Ärzte berichten, daß 1996 viele Reisegruppen und auch Firmen, die beruflich nach Rußland reisen mußten, »zur Sicherheit« eigene Blutabnahmegeräte mit im Reisegepäck hatten, damit sie nicht von den dortigen Mchrwegspritzen infiziert werden - für den Fall des Falles.

Die russischen Behörden realisierten ihre Idee unter dem Druck des Auslands nicht. In einigen Staaten, vor allem im arabischen Raum, wird von den Regierungen ein negativer HIV-Test aber für Langzeit-Besucher verlangt - ausgenommen von dieser Regelung sind Diplomaten aufgrund ihrer Immunität.

## *Das fast anonyme Aids-Register*

Eigentlich könnte man es, flapsig formuliert, als »Augenauswischerei« bezeichnen. Sowohl in Deutschland als auch in Österreich ist Aids eine meldepflichtige Krankheit. In beiden Staaten sind die Meldungen anonym. Aber bei genauer Betrachtung schwindet die Anonymität - vor allem in Österreich.

Von positiven HIV-Fällen muß das Gesundheitsministerium gemäß § 2 Aidsgesetz unterrichtet werden. Derzeit stehen die Namen von

1763 Aids-Kranken im Register, 1130 von ihnen sind bereits verstorben.

Die Meldung umfaßt zum einen den Namen des behandelnden Arztes, das Geschlecht des Infizierten, seine Initialen und das Geburtsdatum (Tag-Monat-)ahr).

Anhand dieser Daten ist ein Österreicher genau identifizier- und sein Name mit Leichtigkeit feststellbar. Denn täglich werden in Österreich im Durchschnitt 240 Menschen geboren. Wenn man davon ausgeht, daß etwa 50 Prozent weiblich und 50 Prozent männlich sind, so läßt sich die Gruppe aufgrund des Geburtsdatums und aufgrund des Geschlechtes reduzieren. Berücksichtigt man die Initialen, so wird die Gruppe noch kleiner. Bei zufällig namensgleichen Personen kann man über die Adresse des Arztes, von dem die Meldung kommt, den HIV-Infizierten geografisch zuordnen. »Diese Verknüpfung machen wir nicht, wollen wir auch gar nicht herstellen«, meint der Gruppenleiter der Sektion 8/D im Gesundheitsministerium, Ministerialrat Gerhard Aigner. Von der anonymen Meldung dennoch zum Namen zu kommen lasse sich viel einfacher realisieren. Aigner: »Die Sozialversicherung weiß, daß bei einer Behandlung einige bestimmte Medikamente notwendig sind. Aus diesen Daten lassen sich Schlüsse ziehen.«

Wirklich anonym sind dagegen die Meldungen im Deutschen Aids-Register, das sich eigentlich aus zwei verschiedenen Dateien zusammensetzt. Zum einen gibt es das Laborberichtsregister, in der mehr als 80000 HIV-Tests gespeichert sind, zum anderen das Aids-Fall-Register mit etwa 17000 registrierten Fällen.

Anders als in Österreich begnügt man sich in Deutschland bei einer Meldung ans Laborberichtsregister mit dem Geschlecht, den ersten drei Stellen der Postleitzahl und dem Alter des Getesteten. Das Geburtsjahr fehlt. Der österreichische Usus - das exakte Geburtsdatum - wäre den Experten im Robert-Koch-Institut auch lieber, aber »diese Informationen sind heiß«. 80000 HIV-Tests heißt aber nicht, daß es in Deutschland 80000 HIV-Positivc gibt. Jeder HIV-Positive läßt sich statistisch gesehen 3,3 Mal testen. Die Experten des Aids-Zentrums schätzen, daß es in Deutschland zwischen 50000 und 60000 HIV-Positive gibt.

So wie in Österreich auch, lassen sich über die verschriebenen Medikamente Rückschlüsse ziehen. Im Aids-Fall-Regisrer ist man



aber auf Anonymität bedacht. Im Robert-Koch-Institut wird ein Patientencode benutzt, der sich aus Buchstaben und Zahlen zusammensetzt: der dritte Buchstabe des Vornamens, die Anzahl der Buchstaben des Vornamens, das Geburtsjahr und das Geschlecht. Würde der Aids-Kranke Friedrich S. heißen, geboren 1958, würde der Code folgendermaßen lauten: » 1 9 1 9 5 8 M«

## Das Register der Organspender

Das Zentralregister wird in irgendeiner jener Behörden installiert, die zum Gesundheitsministerium gehören. Das könnte das Bundesinstitut für Arzneimittel genauso sein wie das Bundesinstitut für übertragbare Krankheiten. Das seit 1. November 1997 gültige Transplantationsgesetz sieht vor, daß ein deutsches Transplantationsregister eingerichtet wird. Anders als in Österreich wird das deutsche Zentralregister ein »Einwilligungsregister« sein, jeder, der spenden möchte, muß sich hier eintragen lassen. Das deutsche Transplantationsgesetz sieht aber eine »erweiterte Zustimmungslösung« vor. Wenn weder Zustimmung noch ein Widerspruch vorliegen, so muß der nächste Angehörige gefragt werden, ob ihm eine sogenannte Willensäußerung des Verstorbenen bekannt ist.

Obwohl Ende 1997 noch nicht feststand, wo das Zentralregister eingerichtet wird, liefen die Vorbereitungen bereits auf Hochtouren. Konkret war vorgesehen, daß in dieser Datenbank alle »General-Einwilligungen« und »Beschränkten Einwilligungen« (nur bestimmte Organe dürfen verwendet werden) gespeichert sind.

Die Zentraldatei soll die derzeit üblichen Organspenderausweise ersetzen. Nur 3 Prozent der Deutschen führen einen solchen mit sich. Ebenfalls nur 3 Prozent der freiwilligen Spender kommen tatsächlich als Spender in Frage. Bei 97 Prozent der in Deutschland durchgeführten 3000 Transplantationen wird die Zustimmung von Angehörigen eingeholt.

In Österreich gibt es seit 1. Januar 1995 ein »Widerspruchsregister«. Jeder, der seine Organe im Todesfall nicht spenden möchte, ist hier gespeichert. 3200 waren es Ende 1997, wobei die meisten Eintragungen von Wienern, Niederösterreichern, Steirern und Salz-

burgern beantragt wurde. Kurz nach der Einrichtung des österreichischen Organspende-Registers, das übrigens im Österreichischen Bundesinstitut für Gesundheitswesen (OBIG) dem Computer in der Vergiftungszentrale angefügt ist, wurden sämtliche praktischen Ärzte angeschrieben, um ihre Patienten von der Existenz einer solchen Datenbank und einer möglichen Eintragung zu informieren. Dies hatte zur Folge, daß sich vor allem Ärzte in das Register eintragen haben lassen.

36 Spitäler, die mit den entsprechenden medizinischen Geräten ausgestattet sind, müssen vor einer Organentnahme telefonisch beim Widerspruchsregister anfragen. Mit einem bestimmten Code-Wort erhalten sie die gewünschte Information. Das Code-Wort, das übrigens nur dann geändert wird, wenn die Transplantationsbeauftragten in den 36 Krankenhäusern und Kliniken der Meinung sind, daß es wieder geändert werden müsse, ist meist »ein Name oder ein Phantasieausdruck«, wie etwa »Leberzirrhose«. »Es kommt vor, daß mit falschen Codewörtern Informationen abgefragt werden wollen«, bestätigt ein ÖBIG-Vertreter.

## Digitales Krankenhaus

In einigen Jahren werden die schriftlichen Befunde, Diagnoseformulare und Überweisungsbriefe völlig verschwunden sein. »Im Jahr 2010«, so rechnet der Verwaltungsdirektor des Klinikums Großhadern in München, Franz Stadier, »wird es in Spitälern kein Papier mehr geben.« Im »digitalen Krankenhaus« werden die Krankengeschichten in elektronischer Form von PC zu PC geschickt, Krankengeschichten von ehemaligen Patienten, die vor 30 Jahren behandelt wurden, können auf Knopfdruck ausgedruckt werden. Denn 30 Jahre lang werden die Krankenakten in den Spitälern gelagert, dann läuft die gesetzliche Frist ab und sie müssen vernichtet werden. Oder auch nicht, denn in Wien gibt es Obduktionsberichte und Krankengeschichten, die 100 Jahre oder noch älter sind.

In den Spitälern ist man seit einigen Jahren damit beschäftigt, die Krankengeschichten zu digitalisieren. 200000 Krankengeschichten



waren in Wien Ende 1997 eingescannt. 1990/91, bei der Übersiedlung vom alten Spitalsgebäude des Allgemeinen Krankenhauses (AKH) ins neue, hatte man mit der langwierigen Arbeit begonnen. Klinik für Klinik werden die Diagnoseblätter eingescannt, parallel dazu auch noch jene der etwa 74000 Patienten, die jährlich stationär aufgenommen werden. Im neurologischen Bereich haben Krankengeschichten aber oft einen Umfang bis zu 1 000 Seiten.

Das Krankenhaus-Informations-System (KIS), wie die Datenbanken in den Spitälern unter einem Begriff zusammengefaßt werden, umfaßt Großrechner, Dateien und Betriebssysteme.

Die Hauptpfeiler sind neben dem Patienten-Management-System eine Statistikdatenbank, in der »Patientendaten auch durch den EDV-Laien flexibel und rasch ausgewertet werden können«, wie AKH-Verwaltungsdirektor Prof. Horst Ingruber erklärt.

Das »digitale Krankenhaus« birgt aber auch einige Gefahren in sich, denn die gesamte Kommunikation läuft auf elektronischem Weg ab. Ärzte, Labors und andere Spitäler schicken Gesundheitsdaten auf der Datenautobahn auf Reisen. Abgesehen von der Gefahr, daß gewisse Befunde oder Krankendaten nur zur Hälfte ankommen, können sie auf dem Weg vom Arzt ins Spital kopiert oder verändert werden oder ganz verschwinden.

Walter Peissl, Hilda Tellioglu und Claudia Wild orten in ihrer, im Januar 1997 präsentierten »Technikfolgenabschätzung moderner Telekommunikationstechnologien im Krankenhaus« mehrere Probleme. Daten im Medizinbereich seien »sensibel« und »die Kosten zur Implementierung von Datensicherungsmechanismen relativ gering im Verhältnis zum potentiellen Schaden«.

Paßwortschutz sei nicht mehr Stand der Technik, Paßwörter seien nur im krankenhausinternen Bereich akzeptabel, bei telemedizinischen Vernetzungen müßten Verschlüsselungstechniken (Kryptografie) angewendet werden. »Kryptografie bietet genug Möglichkeiten, Patientinnendaten sicher zu speichern und vor allem zu übertragen«, kommen die drei Studienautoren zum Schluß. »Wirksamer Datenschutz in offenen Systemen ist nur mit Hilfe kryptografischer Methoden zu erreichen. Daneben ist aber insbesondere der Schaffung eines entsprechenden Bewußtseins für die Datenschutzproblematik bei den Nutzerinnen hohe Wichtigkeit zuzuordnen.«

In München versuchte 1997 ein niederländischer Hacker in die Datenbank des Forschungszentrums des Klinikums Großhadern einzubrechen. »Die Datenbank, die er knacken wollte, enthielt aber keine sensiblen Daten«, beruhigt Verwaltungsdirektor Stadler. Die Zukunft könnte Patienten aber auch etwas bescheren, das bei Tieren bereits Realität ist-der Chip im Körper. So. wie einem Hund mit einer kleinen Kanüle ein Chip unter die Haut implantiert wird, so könnte auch unter der Haut eines Menschen, an einer sicheren ' Stelle, ein Chip »deponiert« werden, der alles speichert, was man über den Menschen wissen muß. Von dieser Horrorvision sind wir zum Glück noch weit entfernt, wenn man bedenkt, welche Diskussionen und Probleme die Einführung einer Gesundheits-Chipkarte in Deutschland und Österreich ausgelöst hat, und dabei hat es sich »nur« um eine Plastikkarte mit einem Chip gehandelt.

## *Chirurg in Amerika, Patient in Europa*

Der Chirurg sitzt in Los Angeles vor einem Bildschirm, der Patient liegt in einem Operationssaal im Großklinikum Aachen oder im AKH in Wien. Via Satellit sind die beiden miteinander verbunden. Computer liefern dem Arzt die Daten des Patienten, eine Kamera das dazugehörige Bild. Im Körperinneren hantiert ein Roboter, der vom Chirurgen mit einem Joystick gesteuert wird - wie bei einem Nintendo-Computerspiel.

Operationen via Datenhighway. Noch vor der Jahrtausendwende wird die erste Fernoperation stattfinden, sind Experten wie der Schweizer Physiker Prof. Christof Burckhardt überzeugt. Er hält die Roborter-Medizin für die Methode der Zukunft. Burckhardt hat am Institut für Mikrotechnik der Technischen Universität in Lausanne einen Roboter entwickelt, der Gehirnoperationen durchführt. Während der Patient in einem Scanner liegt, wird er operiert. Der Arzt verfolgt die Operation via Bildschirm und gibt seine Anweisungen über Knopfdruck an den Roboter weiter. Mehrere Sicherheitssysteme verhindern Fehlfunktionen.

Fernoperationen gehören wohl zu den spektakulärsten medizinischen Anwendungsgebieten. Vor allem in den Vereinigten Staaten



wird eifrig daran geforscht, Operationen über Tausende Kilometer durchführen zu können. Das große Interesse der Amerikaner liegt darin begründet, daß sie die Roboter-Medizin in Kriegsgebieten anwenden wollen. Dort, wo Militärärzte überfordert sind, wenn Verletzungen zu spezifisch sind und eigentlich Spezialisten notwendig wären, sollen die Experten in den USA einspringen.

So spektakulär diese Entwicklung, so problematisch kann sie auch werden. Der Datenfluß läuft über Satellit bzw. über den Datenhighway. Auch wenn eine Fernoperation möglich ist, so bleibt die Datensicherheit als große Unbekannte im Raum stehen. »Primarius Robodoc« hat deshalb nicht überall Fans unter der Ärzteschaft. Wenn sich Chirurg und Patient im selben Operationssaal befinden, kann im Notfall der Chirurg persönlich eingreifen. Bei einer Fcrnoperation kann es zu einem Crash auf der Datenautobahn, zu einem gezielten System-Zusammenbruch kommen, bei dem der Patient zum Opfer wird - im Kriegsfall ausgelöst durch die gegnerische Seite, im Zivilleben durch einen kriminellen Saboteur oder einen Geisteskranken.

Weit verbreiteter als Fernoperationen sind Ferndiagnosen. Große deutsche Kliniken, ob Aachen, München oder Heidelberg, kooperieren mit kleinen Spitälern genauso wie das Allgemeine Krankenhaus in Wien oder die Universitätsklinik Innsbruck.

Die Uni Innsbruck etwa ist per lSDN-Leitung mit dem vergleichsweise kleinen niederösterreichischen Krankenhaus Zwettl verbunden und hilft bei der Diagnose. Nacht- und Wochenenddicnste in Zwettl werden im Bereich der Radiologie von Innsbruck aus gemacht. Wird beispielsweise ein Patient mit einem Schädel-Hirn-Trauma eingeliefert, wird dieser vom dicnsthabenden Arzt in einen Computertomografen geschoben, die Daten werden nach Innsbruck Übermittel. Der Spezialist in Innsbruck erstellt eine Diagnose aus der Entfernung.

Ähnlich funktioniert auch jene Kooperationsmethode, die in Fachkreisen als »Second Opinion« bezeichnet wird. Seit Dezember 1995 ist die Uni-Klinik für Anästhesie und Intensivmedizin am Wiener AKH mit der Duke University in Durham, North Carolina, via Telefon und Satellit verbunden.

Die Daten aus den Geräten, an denen der Intensiv-Patient hängt, werden direkt ins System gespielt und in die Vereinigten Staaten

übermittelt. »Den US-Spezialisten sind aber nur die Krankendaten bekannt, den Namen des Patienten kennen sie nicht«, erklärt Universitätsprofessor Michael Zimpfer, der das Projekt »Telemedizin« initiiert hat. Bei VideoKonferenzen setzen sich dann die behandelnden Wiener Ärzte und die US-Spezialisten zusammen und besprechen problematische Fälle. Waren es 1996 exakt 18 Video-Konferenzen, bei denen der Rat der US-Ärzte eingeholt wurde, so stieg die Anzahl der Konferenzen 1997 bereits auf 50. Tendenz weiter stark steigend. Denn in einigen Jahren, so ist Prof. Zimpfer überzeugt sind sämtliche bedeutenden Kliniken auf der ganzen Welt miteinander via Datenleitung verknüpft. Das bedeutet aber wiederum, daß Patientendaten von einem Kontinent auf den anderen überspielt werden. Zum Teil verschlüsselt, zum Teil unverschlüsselt. Und »Paradefälle« werden, ähnlich wie in medizinischen Vorlesungen, bald im Fernsehen besprochen. Auch Live-Übertragungen von Operationen sind geplant.

Seit 1. September 1997 sendet in den USA ein eigener Gesundheits-Fernsehkanal, der im Laufe des Jahres 1998 nicht nur in Europa empfangen werden kann, sondern in dem auch europäische Fälle aus Deutschland und Österreich besprochen und gezeigt werden sollen. Das Projekt »The Health Channel« des Baylor College of Medicine in Houston und des Williams Learning Network ist ein Fortbildungsfernsehen für Ärzte auf der ganzen Welt. In einigen Jahren wird eine Herzoperation an Patient Huber in Berlin via TV in Japan, die Trennung siamesischer Zwillinge in Wien via »Health-Channel« in Kapstadt zu beobachten sein. Für den Gesundheitskanal, der mit einem Decoder empfangen werden kann, zeigten 1997 in Deutschland sowohl die Leo-Kirch- als auch die Bertelsmann-Gruppe Interesse.

Kunden des Cesundheitskanals sind vor allem niedergelassene Ärzte in Deutschland und Österreich, die aus Zeitgründen Kongresse nicht besuchen können, sich aber dennoch fortbilden wollen. Die einmalige Anschlußgebühr wird etwa 220 Mark kosten, die monatliche Gebühr beträgt etwa 40 bis 80 Mark.

Für weit problematischer halten Datenschützer den administrativen Datenaustausch zwischen Ärzten und Spitälern oder Krankenhäusern untereinander. »Oft läuft dieser Datenaustausch unverschlüsselt ab«, kritisiert Buchautor Walter Peissl vom Institut für Technikfolgen-Abschätzung an der Österreichischen Akademie der Wissenschaften. »Die Frage des Datenschutzes und der Datensicherheit sind nicht befriedigend gelöst.« Häufig würden Befunde via Fax oder E-Mail von einem Spital ins andere gesendet und sind damit für jedermann zugänglich. Auch die Datenübertragung via ISDN-Leitung von Spitälern in einem Verbund ist oft unsicher. Vor allem bei jenen Krankenhäuser, die das Internet als Übertragungsschiene benutzen und Befunde und Krankendaten ohne Verschlüsselung verschicken. Elektronisch übermittelte Befunde müßten so übertragen werden, wie es etwa die steirische Ärztekammer realisiert hat: In der Steiermark erhalten Patienten bei landesweit etwa 1500 niedergelassenen Ärzten keinen Arzlbrief mehr in die Hand. Die Diagnose wird per elektronischer Post übermittell. Beim »elektronischen Befundübermittlungssystem« wurde, so schrieb die »Presse« (22. 9. 1997), »besonderer Wert auf Datenschutz und Zuverlässigkeit des Systems gelegt«. Mit einer »elektronischen Unterschrift« - ein bestimmter Zahlencode, der nur dem Arzt bekannt ist - sowie einer mehrstufigen Verschlüsselung werden Manipulationen und unbefugte Datenabfragen verhindert.



## Wie krank ist der Präsident?

Der Techniker sitzt irgendwo im kalifornischen Palo Alto vor einem Computerbildschirm und ist mit Wien verbunden. Wild tippt er auf die Tastatur seines PC, gibt Ziffern, Codes und Buchstaben ein und spielt aktualisierte Software, sogenannte Updates, ins Programm der High-Tech-Apparate im Wiener AKH.

Die Geräte und Computersysteme in den Spitälern sind nicht nur teuer, sie sind hochkompliziert und bedürfen ständiger Betreuung. Fernwartung nennt sich jener Vorgang, während dem für einen gewissen Zeitraum die gesamte Datenbank eines Spitals, von heiklen Krankendaten bis zu Personalinformationen, frei zugänglich ist. Fernwartung öffnet ein »Tor zur Außenwelt«, wie es Walter Peissl bezeichnet, durch welches das gesamte System plötzlich geöffnet wird. Je komplizierter die Systeme, desto öfter müssen sie ferngewartet werden. Die Entwicklungen gehen auch im medizini-

sehen Bereich so rasant weiter wie auf dem Home-PC-Markt. Ein Computer heute gekauft, ist morgen schon wieder überholt.

»Unser Patientendaten-Managernent-System bricht regelmäßig zusammen«, bestätigt ein Mediziner aus dem Allgemeinen Krankenhaus. Das PMS, wie es abgekürzt wird, ist eines jener Systeme, das online, via ISDN-Leitung, von US-Spezialisten gewartet wird. Offiziell wird das freilich vom Leiter der EDV-Abteilung, Dipl.-Ing. Norbert Weidinger, bestritten. »Eine Fernwartung über Modem kommt nur selten vor.« -»Oft genug«, kontern Insider. In dieser Zeit hat der Techniker Zugriff auf sämtliche Daten des Spitals. Auch auf jene, die mit einer Zugriffsperre belegt wurden, weil es sich etwa um einen Prominenten handelt.

Keine Firma kann von sich aus das AKH-System anwählen. Wie in anderen großen Kliniken Deutschlands und Österreichs auch üblich, wird dem Techniker eine bestimmte Leitung über Rückwahlmodus geöffnet. Er ruft an, wird zurückgerufen und ist dann über Modem mit dem Gerät verbunden. Solange er im System arbeitet, wird jeder Schritt protokolliert, beruhigen die EDV-Experten.

In der Münchner Klinik Großhadern, mit Wien punkto Größe und der Kombination Spital/Forschung/Universität vergleichbar, ist es 1997 zweimal zu Fernwartungen gekommen. Das Münchner Rechnersystem ist eine Siemens-Nixdorf-Anlage, ein eigenes Siemens-Team ist ständig vor Ort, um anfallende Systemarbeiten bei den beiden Rechnern RM 600 und RM 400 durchzuführen. Für Fernwartungsfälle stehen den Technikern zwei eigene Telefonleitungen zur Verfügung. »Bei Fernwartungen wird der Techniker über eine festeinprogrammierte Telefonnummer zur Siemens-Nixdorf-Zentrale verbunden«, erklärt der stellvertretende Leiter des Rechenzentrums, Herbert Seidel. »Wenn er Zugang zum Route benötigt, ändern wir kurzfristig das Route-Paßwort (General-Paßwort, Anm.) und setzen es nach der Wartung wieder auf das ursprüngliche retour.«

Bricht das System am Wochenende zusammen, so wird das im Tresor deponierte Route-Paßwort dem Techniker bekanntgegeben. Erst am nächsten Arbeitstag wird der Code völlig geändert. Seidel ist sich bewußt, »daß ein Techniker mit dem Route-Paßwort alles machen kann. Das ist sehr schwer zu kontrollieren, aber wir haben ja die Möglichkeit, zuzuschauen.« Ob diese Kontrollmöglichkeit genützt wird oder ob man den Technikern, mit denen man schon lange arbeitet und die einen eigenen Sicherheitscheck über sich ergehen lassen müssen, vertraut, will er allerdings nicht beantworten.



Fernwartungen soll es auch während des Spitalsaufenthalts von Bundespräsident Thomas Klestil gegeben haben. Ob in dieser Zeit dessen Krankendaten ausspioniert wurden, ist nicht zu beweisen. Daß aber das Interesse am Gesundheitszustand von Staatspräsidenten groß ist, zeigt die Tatsache, daß manche Staatspräsidenten ihre »biologischen Abfälle« (sprich: Kot) nicht in Gastländern lassen. Durch eine Untersuchung von Kot und Urin kann man sich nämlich über den Gesundheitszustand des Präsidenten informieren. Hartnäckig hält sich z. B. jenes Gerücht, wonach bei einem Besuch des chinesischen Staatspräsidenten in Wien dessen Kot in Säckchen abgepackt nach China wieder mitgenommen wurde.

»Auf jeden Fall ist es leichter, einen Ferndiagnose-Techniker in den USA zu bestechen, der mit Österreich wenig am Hut hat, als einen Österreicher, der mit dem Land verbunden ist und der große Probleme bekommen kann, weil er gegen das Datenschutzgesetz verstößt«, meint ein Insider. Im Nachsatz: »Außerdem sind die Amerikaner, wie man weiß, neugierig und interessieren sich für diverse Daten und Informationen.« Nicht nur die Amerikaner haben Geheimdienste, die in aller Welt bekannt und berüchtigt sind, auch der deutsche BND genießt einen hervorragenden Ruf…

Daß das Interesse an den Krankendaten groß ist, beweisen auch die unzähligen Hack-Versuche, die bei den Wiener Gemeindespitälern (darunter das AKH) registriert werden. Pro Monat sind das zwischen drei und fünf. »Diese Attacken werden protokolliert«, bestätigt Senatsrat Johann Mittheisz. »Noch ist ein Einbruch nicht gelungen, aber wir werden die Sicherheitsvorkehrungen verschärfen müssen.«

Datensicherheit wird im Allgemeinen Krankenhaus offenbar nicht überall groß geschrieben. Für das Rechenzentrum, das nur eine ganz kleine Gruppe von Berechtigten betreten darf, gibt es Handflächenscanner.

So sicher das Rechenzentrum ist, so unsicher sind die 2500 PCs, die in dem riesigen Gebäudekomplex in den diversen Büros, Stationen und Instituten stehen. 1997 wurde damit begonnen, die PCs

mit Stahlseilen im Boden zu verankern. Diese unübliche und auch kostenintensive Methode hat einen Grund: dem AKH sind in den vergangenen Jahren etwa 140 PCs abhanden gekommen, sie wurden einfach aus dem Spital getragen. Und mit den Bildschirmen und Rechnern auch so manch heikle Patientendaten, die sich auf den Festplatten befunden haben, weil sie dort zwischengespeichert waren.

# Stadt und Staat schauen genau

**> Wie man feststellen kann, ob Ihre Wohnung leer steht.**

**> Wie »gute« Spitäler und »schlechte« Spitäler errechnet werden.**

**> Wie man feststellen kann, wie viele Medikamente ein Mensch im Laufe seines Lebens geschluckt hat.**

**> Warum Privat-Pkw im Kriegsfall einrücken müssen und wie sie ausgewählt werden.**

**> Welche Parteien und Anwälte Zugriff auf Sozialversicherungsdaten haben.**

**> Wie viele Bürger in den Schwarzfahrerlisten und im Faischparkerregister gespeichert sind.**

**> Warum Großgemeinden wie München oder Wien die totale Kontrolle über die Bürger haben.**

## Die Mega-Datenbank und die »schwarze Kugel«

Auf ihre Daten würden wohl alle gerne zugreifen. Die Sozialversicherung (SV), exakt der Hauptverband der österreichischen Sozialversicherungsträger, hat die größte Informationssammlung der Republik: Beinahe 60 Millionen Datensätze sind im SV-Rechner gespeichert - darunter 12,4 Millionen Versicherungsnummern, 39,7 Millionen Arbeitsverhältnisse etc. Rekordhalter ist ein Buchprüfer mit 16 Arbeitsverhältnissen gleichzeitig. 99 Prozent der Österreicher sind in dieser Datenbank gespeichert. Der verbliebene Prozentsatz lebt als »U-Boot« im Land.
Gelöscht werden die Informationen, die über einen Bürger im SV-

Rechner gespeichert sind, praktisch nie. »Wir behalten die Daten so lange wie unbedingt notwendig«, erklärt ein Insider. Zuerst das ganze Arbeitsleben eines Versicherten lang, danach noch so lange, bis dessen Hinterbliebene gestorben bzw. ins Pensionsalter gelangt sind. »Das sind etwa 100 Jahre.« Das ist jener Zeitraum, in dem Hinterbliebene noch Forderungen stellen könnten.

Im SV-Rechner sind sämtliche Versicherungszeiten gespeichert, jeder Arbeitgeber, bei dem ein Österreicher im Laufe seines Lebens gearbeitet hat. Da manche Österreicher Arbeitsbestätigungen von ehemaligen Arbeitsplätzen verlieren, muß die Sozialversicherung das Arbeitsleben sofort wieder rekonstruieren können.

An den Daten der Sozialversicherungen sind nicht nur Innenministerium und Justizressort interessiert. Auch für Privatdetektive, die von Firmen zum Einbringen ausständiger Schulden engagiert werden, wären die Daten im SV-Rechner eine »heiße Sache«.

Da es in Österreich kein zentrales Melderegister gibt, ein Mensch aber dort, wo er gemeldet ist, nicht wohnen muß, sind die Adressen von aktuellen Arbeitgebern jene Orte, wo Schuldner mit ziemlich großer Sicherheit angetroffen werden.

Nicht zuletzt deshalb gibt es Ideen, den SV-Datenpool für ein zentrales Melderegister zu nutzen, da der Arbeitgeber die richtige Adresse eines Arbeitnehmers kennen muß. Wird der Arbeitgeber verpflichtet, die aktuelle Wohnadresse der SV bekanntzugeben, so wäre mit einem Schlag ohne großen Aufwand ein zentrales Melderegister geschaffen.

Eine Kooperation zwischen einem SV-Beamten und einem Privatdetektiv gab es schon einmal, angeblich tatsächlich nur einmal, so wird bei der SV verlautet. Aber dieser Vorfall hätte sich zu einer Zeit ereignet, in der es noch keinen Zentralcomputer gegeben habe und alle Informationen auf Karteikarten gesammelt wurden. Der SV-Beamte versorgte den Detektiv mit Arbeitgeberadressen und half ihm so, Schulden einzutreiben. Auch an einen zweiten Fall kann man sich erinnern. Bei diesem kam es zu einer »Kooperation« zwischen einem Anwalt und einem SV-Mitarbeiter.

Heute soll dies durch die sogenannte »schwarze Kugel« verhindert werden - ein Zufallsgenerator, der aus allen Computeranfragen eine bestimmte Menge auswählt und die Berechtigung sowie den »Werdegang« überprüft. Wie viele der 3 Millionen Direktabfragen



von der »schwarzen Kugel« kontrolliert werden, wird nicht verraten. »Wir wollen nicht, daß es heißt: >Mit dieser kleinen Kontrollmenge soll das funktionieren«, erklärt man in der Sozialversicherung. Die Wahrscheinlichkeit, ertappt zu werden, dürfte nicht sehr hoch sein. Im Handbuch der Sozialversicherung 1997 steht schwarz auf weiß: »Alle Auskünfte aus der zentralen Versicherungsdatenspeicherung werden protokolliert. Die anfragenden Stellen sind verpflichtet, stichprobenartig die Rechtmäßigkeit des Zugriffes zu überprüfen.« Die Frage, die sich daraus ergibt, ist, ob eine Stelle, die sich Informationen besorgt, überhaupt Interesse und Muße hat, ihre Mitarbeiter zu überprüfen.

Daß man die SV-Daten sehr gut nutzen kann, haben auch das Innenministerium und das Justizressort schon vor Jahren erkannt. Im Innenministerium haben insgesamt 310 Terminals Zugriff auf die SV-Datenbank. Mitarbeiter und Standort der Bildschirme, von wo aus der Zugriff möglich ist, mußten der SV bekanntgegeben werden. Auch das Justizressort - erst seit kurzem Online mit der SV-Zentrale verbunden - nutzt die Informationsquelle häufig. Vor allem für Gehaltsexekutionen werden die SV-Daten benötigt. 1996 wurde insgesamt 1 037400 Mal angefragt. Und außerdem ist neben dem Finanzministerium (660495 Mal holte man sich Daten aus dem SV-Rechner) auch das Verteidigungsministcrium neugierig: es benötigt pro Monat zwischen 10000 und 15000 Mal Informationen.

Interessant ist auch die - dreiseitige - Liste jener, die neben den Ministerien einen SV-Online-Zugriff haben: der SPÖ-Parlamentsklub, die Rechtsanwaltskanzlei Taborstraßc, Dr. Peter Schütz, die Wirtschaftsuniversität Wien, die EDV GmbH, die PTA (7 Terminals) etc. Es wird betont, daß diese Organisationen unterschiedliche Zugriffsberechtigungen haben. Offiziell erhalten sie keine Versichertendaten.

## Medikamentenstatistik

»Die Österreicher sind ein gesundes Volk.« Die Behauptung des Vertreters eines großen deutschen Medikamentenherstellers ist manchen in der Sozialversicherung noch in guter Erinnerung. Auf

die Frage, wie er denn auf die Idee komme, hatte der Pharmakologe eine einfache Erklärung parat: »Die Österreicher nehmen viele Medikamente zu sich.«

Was der Vertreter des Pharmakonzerns anhand der Verkaufszahlen errechnet hat, ist auch durch eine Datenanalyse im SV-Rechner möglich: 33300 verschiedene Medikamente, teilweise in unterschiedlichen Verpackungsgrößen, können die österreichischen Ärzte verschreiben, Apotheker verkaufen bzw. Spitäler verabreichen. Da jedes Medikament mit einer eigenen Pharmanummer registriert ist, läßt sich auf Knopfdruck sagen, wie viele Medikamentenpackungen Rohypnol, Thomapyrin, Immodium etc. verabreicht wurden. »Die Daten müssen wir wissen, denn sie sind Basis für unsere Vertragsverhandlungen. Nur wenn wir die genaue Anzahl kennen, die von einem Medikament verabreicht worden ist, können wir einen Rabatt verlangen.«

Rein theoretisch wäre es sogar möglich, festzustellen, welcher Sozialversicherte welche Medikamente eingenommen hat - im abgelaufenen Jahr, theoretisch sogar im Laufe seines Lebens. »Exakt aus diesen Gründen werden diese Daten nach spätestens vier Jahren gelöscht«, wird argumentiert. Man möchte verhindern, daß eine sogenannte »Medikamentenkarriere« erstellt werden kann. Denn immer wieder gibt es Bestrebungen von Ökonomen im eigenen Haus, aber auch von externen Wirtschaftsfachleuten, auch den Medikamentenverbrauch eines einzelnen Menschen unter die Lupe zu nehmen. »Das wäre aber nicht gut«, ist ein SV-Experte überzeugt. »Dann wäre nämlich dem Mißbrauch dieser Informationen Tür und Tor geöffnet. Vor allem für Menschen, die in der Öffentlichkeit stehen, könnte eine solche Medikamentenkarriere große Nachteile bringen. Ein politischer Kandidat wäre dann plötzlich in seinem Wahlkampf mit dem Vorwurf konfrontiert, daß er in seinem Leben bereits Psychopharmaka zu sich genommen hat oder ständig Beruhigungsmittel schluckt.«

Ausgestanden sind die Angriffe der Statistiker und Ökonomen noch nicht, denn solche Statistiken können durch die vielen Datenbanken als »Abfallprodukte« erstellt werden. In einigen Jahren schon wird man vielleicht genau sagen können, daß Herr Müller in seinem Leben Medikamente im Gesamtwert von 100000 Schilling und Frau Huber Medikamente im Wert von 2 Millionen Schilling geschluckt hat. «Wozu soll diese Information nützlich sein?«, gibt der SV-Experte zu bedenken. »Man kann deshalb ja bei anderen Patienten nicht weniger verschreiben.« Mit diesen Informationen würde ein Bürger kontrolliert. Das Bild, das der Staat von ihm hat, wäre noch genauer, noch detaillierter.



## *Die Gefahr der Güteklassen-Medizin*

Ähnlich wie der Verbrauch eines Medikaments könnten auch Operationen, Arzt- und Spitalsbehandlungen statistisch erfaßt werden, da jede Behandlung mit einem eigenen Buchstaben-Zahlencode verschlüsselt ist. Auch mit solchen Ideen war man in der Sozialversicherung bereits konfrontiert. Durch eine gezielte Abfrage ließe sich exakt sagen, in welchem Spital die meisten Patienten sterben, wie oft Operationen eines Chirurgen mit dem Tod des Operierten enden bzw. wie oft sie erfolgreich verlaufen. Auch dagegen wehrt sich die SV derzeit noch erfolgreich. Aber wie bei den Medikamenten könnte eine derartige Statistik als Nebenprodukt abfallen.

»Ein solches System würde katastrophale Folgen nach sich ziehen«, ist ein Insider überzeugt. »Damit würde eine Art Güteklassen-Medizin geschaffen.« Derzeit werden Operationen und Behandlungen nach einem österreichweit gültigen, einheitlichen Schlüssel abgerechnet. Durch eine Güteklassen-Medizin würde eine Zwei- oder sogar Drei-Klassen-Gesellschaft auch bei der Behandlung geschaffen werden. Statistisch gute Spitäler könnten teurer, ein statistisch schlechter Arzt müßte billiger werden. Es würde ähnlich wie in der Wirtschaft zu einem Preiskampf kommen. Eine Horrorvision wäre ein Katalog, in der die unterschiedlichen Preisklassen von Spitälern und Ärzten aufgelistet wären. Abhängig von der Krankenkasse müßte in einem solchen System die Putzfrau in einer Bank den billigen Arzt aufsuchen, die Bankangestellte den Mediziner in der »mittleren Preisklasse«, nur der Bankdirektor selbst könnte sich den Güteklasse-I-Arzt leisten.

## Die »Strom-Forscher«

Immer wieder verkünden Politiker, daß in den großen Städten Deutschlands und Österreichs eine Wohnungsnot herrscht. Im gleichen Atemzug erklaren sie aber auch, daß in Frankfurt, Berlin oder Wien Tausende Wohnungen leer stehen. Oft nennen sie sogar exakte Zahlen, geben auf die Hunderterstelle genau an, wie viele Wohnungen in ihrer Stadt wirklich unbenutzt sind. Wie kommen die Stadtpolitiker zu diesen Schätzungen? Es sind keine Schätzungen, soviel vorweg, es sind genaue Analysen - des Stromverbrauchs.

Um zu berechnen, wie viele Wohnungen leer stehen, muß nur der Stromverbrauch analysiert werden. Dort, wo kein Strom verbraucht wird, also nur die Grundgebühr anfällt, wohnt auch niemand. Die Wohnung steht leer. Das kann vor allem jenen zum Verhängnis werden, die eine Gemeindewohnung besitzen, denn eine solche erhält man nur, wenn man den Bedarf nachweisen kann.

Die »Strom-Forscher« sind bereits jetzt sehr aktiv, in den kommenden Jahren werden sie vermutlich ihre Arbeit intensivieren. Denn nicht nur der Staat, auch die Städte müssen sparen und beim Wohnungsneubau kann man sparen.

Bei einer Eigentumswohnung oder einer Hauptmietwohnung hat eine Gemeinde freilich keine Chance, den Besitzer bzw. Mieter dazu zu zwingen, seine Wohnung zu vermieten. Bei Cemeindewohnungen wird die Nichtbenützung geahndet. Immer öfter strengen Gemeinden Mietrechtsverfahren gegen jene an, die ihre Wohnungen leer stehen lassen. Als Beweis wird neben der Aussage des Hausmeisters auch die Stromabrechnung vorgelegt. Erfolgreich sind meist nur jene, die in ihrer Wohnung ständig einen Kühlschrank, ein Radio oder einen anderen »Stromverbraucher« in Betrieb haben.

## 3000 Lücken im Münchner Magistrat

Der Beschluß des Münchner Stadtrates war unmißverständlich. Der Magistrat wird sich für die Bürger öffnen. Jeder muß mit dem



für ihn zuständigen Beamten online in Kontakt treten und jeder Beamte muß sich im Internet informieren können. Der Stadtrat hat den Datenverarbeitern im Magistrat mit diesem Beschluß eine Arbeit bereitet, die einen Crash des Computersystems auslösen kann. »Die Hacker-Gefahr ist ziemlich groß«, gibt sogar der Leiter des Amts für Information und Datenverarbeitung, Dipl.-Ing. Wilhelm Hoegner, zu. »Es wird zu einem Skandal kommen. Es genügt, wenn uns jemand etwas kaputt macht und die Datenverarbeitung der Stadt kurzfristig auf dem Bauch liegt.«

Schon einmal lag man auf dem Bauch. 1983 fiel das kommunale Rechenzentrum aus - sieben Stunden lang konnten weder Führerscheine noch Pässe ausgestellt werden.

Doch all diesen Gefahren zum Trotz wird sich der Münchner Magistrat Mitte 1998 auf die Datenautobahn bewegen. Das Münchner System absolut sicher zu machen ist eine fast unlösbare Aufgabe. Den Beamten wird mit ihren ca. 3000 PCs ein Online-Zugriff auf das Internet ohne Beschränkung, ohne Zensur gewahrt. Sie können Webseiten anderer Städte genauso aufrufen wie jene von Sex- und Porno-Anbietern. »Am Anfang werden manche Beamte sicherlich auch Nackerte anschauen«, meint Hoegner. »Aber sie werden lernen, mit dem Internet umzugehen, nach zwei, drei Monaten wird das Interesse, sich bestimmte Seiten anzuschauen, ohnehin abflachen. Das ist wie mit Computerspielen.« Die komplette Öffnung sei die einzig geeignete Lösung. Eine »Zensurbehörde« im Magistrat möchte er nicht schaffen, nur bestimmte Dateien hereinzulassen widerspreche dem Sinn des Internets, der globalen Vernetzung.

Aber gerade dieses Ziel, allen Beamten die gesamte Welt des Internets zu öffnen, stellt die EDV-Techniker vor eine fast unlösbare Aufgabe: das Magistratssystem, in dem heikle Daten gespeichert sind, vor illegalen Zugriffen zu schützen. Fünf Barrieren werden eingebaut, damit Hacker nicht schaffen, was viele befürchten: Systeme lahmlegen oder Daten klauen. »Wir haben den Chaos-Computer-Club beauftragt, unsere Systeme zu checken und uns auf Mängel bzw. mögliche Lücken aufmerksam zu machen«, bestätigt Hoegner.

Beim Leiter der EDV ist die Aufregung groß. Ende der 60er Jahre wurde in der bayrischen Hauptstadt mit Datenverarbeitung begonnen, Mitte der 80er hatte man drei Großrechner, 1989 hat man in

allen Referaten ein eigenes Sachgebiet »Datenverarbeitung« geschaffen.

Seit 1995 sind alle Arbeitsplätze in München vernetzt, in drei Großrechnern werden die Dateien verarbeitet. 98 Millionen Datensätze sind gespeichert. Das bedeutet, daß jeder Münchner im Durchschnitt mindestens achtmal erfaßt ist. Pro Tag wird auf 240000 bis 370000 Datensätze zugegriffen.

100 Datenbanken enthielten Ende 1997 pcrsonenbezogene Daten, aus denen sich Beamte Informationen beschaffen konnten. Vom Führerschein-Zentralregisler bis zum Einwohnermeldeamt. Hinzu kommen noch Register wie Straßennamen-, Post- oder Bankleitzahlen-Datei.

Das Besondere an München: die Münchner Polizei und das Landeskriminalamt haben einen Online-Zugriff auf die Magistrats-Daten - sieben Tage in der Woche, rund um die Uhr.

»Sie können abfragen, wann und was sie wollen, aber jeder Zugriff wird von uns protokolliert«, sagt Hoegner. »Und stichprobenweise kontrolliert.« Die Wahrscheinlichkeit, entdeckt zu werden, ist für jemanden, der sich illegal Informationen beschafft, allerdings nicht sehr hoch. Maximal eine von zehn Abfragen wird überprüft.

Aber auch die Exekutive stößt mitunter an Grenzen. Die Daten von Prominenten, Politikern und »besonders gefährdeten Personen«, wie etwa dem Ministerpräsidenten, sind gesperrt. Sie können nur von einem Beamten, dem Beauftragten des Hauptabteilungleiters »Einwohnerwesen«, geöffnet bzw. geändert werden.

Einen Sonderstatus hat auch die Personalvertretung. Sie kann in jeder Datei schnüffeln, ohne daß ihre Nachforschungen protokolliert werden. Während bei anderen Beamten sogar jeden Monat eine Rufnummernliste der geführten Telefonate ausgedruckt und überprüft wird, können Personalvertreter telefonieren, wohin und mit wem sie wollen.

In München werden die einzelnen Datenbanken jedenfalls miteinander verknüpft. So wurde z. B. anhand der Sozialhilfeempfänger-Datei und Kfz-Zulassungsregister überprüft, ob ein Sozialhilfeempfänger sich ein oder gar mehrere Autos leisten kann. Wie in Wien, kommt man auch in München jenen auf die Spur, die ihre Wohnungen leer stehen lassen. Die Methode, die ähnlich funktionieren dürfte wie die »Strom-Forschung«, hat in München noch



einen anderen Grund: das Leerstehen von Wohnungen wird dort als Zweckentfremdung bezeichnet. Steht eine Wohnung länger als drei Monate leer, muß der Eigentümer oder Mieter Bußgeld zahlen. Auch notorische Verkehrssünder lassen sich in München auf Knopfdruck auflisten. Wer häufig ohne Bezahlung in städtischen Kurzparkzonen parkt und die Tempolimits in der Stadt mißachtet - in München ist der Magistrat für die Geschwindigkeitsmessung im Stadtgebiet zuständig -, ist bald entlarvt. 130000 Verkehrssünder stehen ständig im Münchner »Bußgeld-Register«, pro Jahr sogar 400000. Wer seine Strafe zahlt, bleibt vier Monate gespeichert, wer nicht ...

## *Alles unter Kontrolle*

Der Stadt Wien entgeht so gut wie nichts. In 176 verschiedenen Datenbanken sind die Bürger der Stadt gespeichert. Von der Datenbank Nr. 001 »Standesamt« bis zu Nr. 176 »Digitale Archivierung von Krankengeschichten«. Auch für Nicht-Wiener und Touristen ist die Wahrscheinlichkeit, in einer dieser 176 Datenbanken »verewigt« zu sein, ziemlich groß. Es ist fast unmöglich, nicht in der Mega-Datenbank der Stadt zu landen.

Wer sich einmal für einen Job als Buslenker, Straßen- oder U-Bahn-Lenker beworben hat, steht in der Datenbank Nr. 163 »Wiener Linien, Eignungstests der Verkehrsbetriebe«. Kurzparksünder sind in der Datei Nr. 016 »Parkometerabgabe; Verwaltung und Verfolgung von Übertretungen« gespeichert. Wer einmal ein Buch in einer städtischen Bücherei entlehnt hat, ist in der Datei »Bibliotheksverwaltung und Entlehndienst der Städtischen Büchereien« (Nr. 050) zu finden. Und wer die Nummer des »Aktionstelcfons« gewählt hat, um sich Broschüren über die Stadt zuschicken zu lassen, ist in der Datenbank 130 »Aktionstelefon; Bestellservice für Informationsmaterial der Stadt Wien« gespeichert.

Die Wiener Magistratsbeamten sind eifrige Datensammler. 160 Datenbanken waren es 1996. Ein Jahr später waren es schon 176, wie viele es zur Jahrtausendwende sind, ist noch nicht abzuschätzen, die 200er-Marke dürfte aber überschritten werden.

Denn mit Akribie werden in der österreichischen Bundeshauptstadt Daten gesammelt und in 13 verschiedene Aufgabengebiete unterteilt, vom »Personenwesen« bis zu den «Wiener Stadtwerken«. Ing. Günter Eckel, Leiter der Magistratsabteilung 14 -ADV, ist der »Herr über die Wiener Daten«. Er ist für jene Datenverarbeitungen zuständig, die in den Magistratsbereich fallen. Die beiden anderen Großdatenbanken befinden sich bei den Wiener Stadtwerken (Verkehr, Strom, Gas) und im Wiener Krankenanstaltenverbund, der die Gemeindespitäler verwaltet.

## Auf Knopfdruck zum Bürger

Am Beispiel von Wien läßt sich erkennen, wie Stadt und Staat Informationen sammeln. Informationen, die, kombiniert mit Daten aus anderen Datenbanken, ein relativ detailliertes Bild eines Menschen ergeben. Vor allem die Wiener sind offen wie das sprichwörtliche Buch. Der Vorteil für die Datenjäger liegt darin, daß Wien sowohl Stadt als auch Bundesland ist, also zwei Institutionen in einer. Dadurch sind die Informationen umfassender und leichter abrufbar, weil sie praktisch in einer Datenbank zusammengefaßt sind.

Auf Knopfdruck läßt sich sagen, wieviel Strom oder Gas Herr Navradil verbraucht. Ob sein Wohnhaus ein Schutzzonenobjekt ist, ob er eine Jahreskarte besitzt, ein Auto, welche Hobbys er hat (z.B. Lesen), ob er Hundebesitzer ist, öfter in Spitalsbehandlung war oder Labors aufsucht, schon einmal bei Gericht Geschworener war etc. Ist Herr Navradil auch noch Gemeindebediensteter, so gibt es praktisch nichts, was die Stadt über ihn nicht weiß. Die vielzitierte »Anonymität der Großstadt« gilt im Bereich der Datensammler nicht.

Derartige Informationen wären auch für Außenstehende interessant. Sicherheitssysteme machen es aber unmöglich, solche Daten illegal zu erwerben. Die weit größere Gefahr sind jedoch nicht Außen-, sondern vor allem Innentäter, wie nicht nur in Studien behauptet wird, sondern die Realität bewiesen hat. Bestes Beispiel: der Datenklau im Schengen-Computer im November 1997.

Ein Großrechnersystem ist umso anfälliger, je mehr Computer



daran angeschlossen sind. Beinahe 6800 PC hängen am Magistrats-Großrechner. Von jedem Terminal aus lassen sich personenbezogene Daten abrufen. Zwar gibt es unterschiedliche Zugriffsberechtigungen, aber mit etwas Geschick lassen sich auch solche Hürden überwinden.

In der Gemeinde Wien traut man nicht einmal den eigenen Mitarbeitern. Um die Gefahr illegaler Zugriffe und Abfragen zu minimieren, wurde der Magistralsrechner sogar gegen die beiden anderen Datenbanken bei den Stadtwerken und dem Krankenanstaltenverbund mit einer Firewall abgeschirmt. »Wir haben unser System einem Sicherheitscheck unterzogen«, bestätigt Eckel. »Unser Rechner wurde als ziemlich sieben beurteilt.« Auch gegen Angriffe von innen? Die Mitarbeiter haben keinen ungeschränkten Zugriff auf die Datenbanken. Eckel: »Jeder Mitarbeiter darf nur auf bestimmte Daten zugreifen, außerdem hat jeder Bedienstete sein Paßwort.« Das Paßwort muß sechsstellig sein, eine der Stellen muß eine Ziffer sein. Eckel: «Wir haben sogar Paßwort-Cracker-Programme, die im Internet angeboten werden, über das System laufen lassen. Einen sechsstelligen Code zu knacken dauert mindestens 10 bis 20 Minuten.« Die Magistratsbediensteten müssen in regelmäßigen Abständen - 30 Tage - ihr Paßwort ändern.

Schwer ist es trotzdem nicht, das System des Magistrats zu knacken, der Lokalaugenschein beim »Herrn der Daten« beweist es: aus Sicherheitsgründen schaltet sich ein PC, wenn er länger nicht bedient wird, in einen Standby-Modus. Aktiviert kann der Computer erst dann wieder werden, wenn ein Paßwort eingetippt wird. Schön und gut. Das Paßwort von Ing. Günter Eckel bestand am 27. November 1997 nicht aus sechs, sondern aus zwei Stellen. Mit der Eingabe von zwei Buchstaben, vielleicht sogar »GE«, konnte das System wieder aktiviert werden.

## Von Schwarzfahrern und Schwarzarbeitern

Nr. 99 und Nr. 100. Es ist vermutlich reiner Zufall, daßdiese beiden Datenbanken gleich hintereinander geführt werden, aber in diesen Datenbanken gespeichert zu sein ist nicht unbedingt günstig.

Nr. 100 ist die »Schwarzfahrerevidenz«. Jene Datei, in der all jene namentlich aufscheinen, die in Wiener Straßenbahnen, in den städtischen Autobussen oder in der U-Bahn ohne Fahrschein angetroffen wurden. 120000 sind in dieser Datei »verewigt«, sprich etwa ein Jahr lang gespeichert. Mindestens. Vielen ist es vermutlich egal, in der Datenbank als »Schwarzfahrer« geführt zu werden. Weit problematischer kann es dagegen schon sein, in der Datenbank Nr. 99, dem »Auftragnehmerkataster« mit einem bestimmten Merkmal aufzuscheinen.

Im Auftragnehmerkataster sind all jene Firmen gespeichert, die von der Stadt Wien öffentliche Aufträge, von Straßenarbeiten bis zum Einbau von Heizung und Wasserleitung in Gemcindebauten, erhalten haben. Beinahe 18000 Firmen sind in der 99er-Datei. Etwa 9000 von ihnen haben einen sogenannten »Statusvermerk«. Und der bedeutet nicht immer Gutes. Der Auftragnehmerkataster erfüllt nämlich gleichzeitig auch die Aufgabe einer »schwarzen Liste«. Ein Statusvermerk kann zum einen heißen, daß die Firma, die für öffentliche Aufträge in Frage kommt, noch nicht von den städtischen Beamten geprüft wurde. Er kann aber auch ein »schwarzer Punkt« sein und bedeuten, daß diese Firma keinen öffentlichen Auftrag mehr erhält.

Wenn einmal ein Auftrag zur Unzufriedenheit der Magistratsbeamten erfüllt wurde, bekommt die Firma einen Statusvermerk, der anzeigt, daß sie für künftige Arbeiten nicht mehr herangezogen werden darf. Auch wenn die Firma illegal Schwarzarbeiter beschäftigt hat und dies bei einer Kontrolle durch das Arbeitsinspektorat aufgedeckt wurde, ist das Unternehmen gesperrt.

## *»Einberufungsbefehl« für einen Mercedes*

Die 16jährige Friseuse Martina Seh. aus Salzburg konnte nicht glauben, was sie da in Händen hatte, und hielt dieses Schreiben des Militärkommandos Salzburg für einen schlechten Scherz. Das Schriftstück war ein »Einberufungsbefehl« für ihr Moped. »Im Ernstfall«, so stand geschrieben, müsse sie ihr Mofa beim Militärkommando abgeben. Vollgetankt, wohlgemerkt.



So verdutzt wie Martina Seh. sind in Österreich jedes Jahr Tausende Besitzer von Autos, Mopeds und Baumaschinen. Gemäß dem Militärleistungsgesetz dürfen Zivilfahrzeuge für den Ernstfall einberufen werden.

Mehr als 18000 »Spezialfahrzeuge« stehen auf der Rekrutierungsliste des Bundesheeres. Jährlich werden zwischen 3000 und 5000 Fahrzeuge »ausgemustert« und neue Fahrzeuge »einberufen«. Die Daten der potentiellen Fahrzeuge sucht sich das Bundesheer aus dem Kfz-Zulassungsregister. Jedes Jahr übermittelt das Innenministerium dem Bundesheer eine Liste jener Fahrzeuge, die für den Bundesheer-Pool verwendet werden könnten. Gemäß Militärleistungsgesetz haben die Beamten im Verteidigungsministerium sogar das Recht, sämtliche Zulassungsdaten zu durchforsten.

Die Zivilfahrzeuge würden im Ernstfall als Bundesheerfahrzeuge verwendet. Jede Kompanie erhält drei Lkw, einen Pkw als Kommandofahrzeug, zwei Motorräder als »Verbindungsmittel« und ein Moped für einen Kraftfahrmelder.

Allein 1997 wurden 4800 Bereitstellungsbescheide ausgestellt. Wer gängige Automodelle fährt, die auch beim Bundesheer verwendet werden, wie etwa VW-Golf, VW-Polo oder Steyr-Lastwagen, darf sich nicht wundern, wenn plötzlich ein Schreiben des Verteidigungsministeriums auf dem Schreiblisch landet. Auch Luxus-Mercedes oder Geländewägen sind begehrt. Das Heer achtet auf Typenreinheit, sucht nur solche Modelle aus, deren Reparatur für die heereseigenen Mechaniker kein Problem wären und für die es genügend Ersatzteile gibt.

Wer unbedingt verhindern möchte, daß sein Fahrzeug im Ernstfall abgeliefert werden muß, der sollte auf »exotische« Automarken oder Oldtimer setzen. Einen US-Schlitten, einen Porsche oder ein Cabrio könnte das Heer nicht verwenden, auch eine Harley-Davidson ist vor einem Zugriff der Militaristen relativ sicher. Wer aber glaubt, daß ein rotes oder knallgelbes Auto mangels Tarnfarbe nicht einberufen wird, irrt. Die Fahrzeuge dürfen umlackiert werden.

# Gute Adressen sind teuer

> Wieviel Ihr Alter, Hobby und Ihre Handy-Nummer wert sind.

> Wie sich Versicherungsmakler neue Adressen beschaffen.

> Warum Beate-Uhse-Kunden heiß begehrt sind.

> Wie man mit Preisausschreiben an Ihre Adresse kommt.

> Wie ein Computer aufgrund Ihres Vornamens Ihr Alter errechnen kann.

> Wie erhoben wird, wie wertvoll Bürger als Kunden sind.

> Wie im Internet mit Ihrer Adresse gehandelt wird.

> Warum Telefon-CDs nicht nur praktisch, sondern auch gefährlich sind.

## Die Methoden der Beschaffer

Jeder Bürger Deutschlands und Österreichs isl in einer der vielen Dateien der 140 deutschen bzw. 40 österreichischen Adreßhändler vertreten. Mit Name, Titel, Adresse, Alter und Beruf. Basis der Adreßhändler sind die Telefonbücher. Seit Telefon-CD-ROMs auf dem Markt sind, hat sich die Arbeit der Adreßhändler vereinfacht. Früher mußten die Seiten des offiziellen Telefonbuchs eingescannt werden. Drei Wochen benötigte man für ganz Österreich, in maximal vier Wochen hatte man sämtliche 35 Millionen deutschen Telefonkunden im Computer. Obwohl das Datenschutzgesetz in



Deutschland eine größere Bedeutung hat als in Österreich, war die Beschaffung von Adressen um einiges leichter als in Österreich. Denn in Deutschland gibt es die Besonderheit der Adreßbücher, die es für viele Gemeinden und Kreise gibt, allerdings nicht für alle. Hamburg etwa hat keines.

Gemäß den Landesmeldegesetzen darf die Meldebehörde Adreßhändlern eine einfache Melderegisterauskunft - Name, akademischer Grad, Adresse-über sämtliche Einwohner ab 18 Jahren erteilen. Die Daten eines Bürgers werden in der Regel automatisiert an einen Adreßhändler weilergeleitet, nur dann nicht, wenn der Betroffene der Weitergabe seiner Daten rechtzeitig widersprochen hat. Vom Widerspruchsrecht machen aber die meisten Deutschen keinen Gebrauch bzw. kennen diese Möglichkeit gar nicht. »Ob das einfache Widerspruchsrecht hier noch ausreicht, ist fraglich«, meint der deutsche Bundesdatenschützer Joachim Jacob. Er fordert eine »Einwilligung des Betroffenen«.

Doch die von den Meldebehörden gespeisten Adreß- und Telefonbücher sind nicht die einzigen Quellen, aus denen jene Anschriften stammen, die - auf unliebsames Werbematerial geklebt - so manchen Bürger zur Weißglut bringen.

Wie man zu geeigneten Adressen kommt, beschreibt der »Direct Marketing Verband Österreich« (DMVÖ) in seinem 1997 erschienenen «Leitfaden«. Die Methodik, die 1:1 auf Deutschland übertragbar ist, wird darin vom Deutschen Anton Jenzer, dem geschäftsführenden Gesellschafter von Schober Direktmarketing, beschrieben: Verschiedene Institutionen, wie etwa Kammern und andere Interessenverbände, geben die Daten ihrer Mitglieder problemlos weiter. »Alle Unternehmen verfügen über firmeneigene Adressen, an die sie oft nicht denken«, erklärt Jenzer. Die Palette reicht hier von Buchhaltungslisten und Garantiekarten bis zu Reparatur- und Erlagscheinen. Auch Messekataloge sowie Ausstellungs- und Teilnehmerverzeichnisse von Tagungen werden herangezogen, um Adreßmaterial zu lukrieren.

Wer an einem Preisausschreiben teilnimmt, sollte wissen, daß für die Firmen nicht der ausgespielte Preis und nicht die freudigen Gewinner im Vordergrund stehen, sondern die Adressen der Teilnehmer. »Bei fast jedem Preisausschreiben werden die Teilnahmekarten durchforstet und Adressen lukriert«, bestätigt ein Insider und

nennt Reader's Digest, Telekabel oder den Europa Versand als Beispiele. ]e attraktiver die Preise, desto größer das Interesse und desto größer das gewonnene Datenmaterial.

Die Adressen sind auch aus einem weiteren Grund wertvoll: Sie repräsentieren die Zielgruppe, obwohl es für viele Personen beinahe ein »Sport« ist, an jedem Preisausschreiben teilzunehmen.

Wer auf dem Flughafen Frankfurt oder in Wien-Schwechat an einem Preisausschreiben teilgenommen hat, bei dem es ein im Duty-Free-Bereich ausgestelltes Auto zu gewinnen gab, darf sich nicht wundern, wenn er plötzlich Informationen von Reiseveranstaltern, Versicherungen oder Wertanlageberatern erhält- er ist Teil der Zielgruppe »Menschen, die reisen und hohe Kaufkraft haben«.

Am wertvollsten sind Adressen von sogenannten Postkunden - Personen, die gerne im Versandhandel einkaufen und sich durch einen besonderen RFMR-Wert auszeichnen. R steht für recancy (wann hat der Kunde zuletzt gekauft?), F für frequency (wie häufig kauft er?), MR für monetary ratio (wieviel gibt er bei diesen Einkäufen aus?). Je besser die Werte bei den einzelnen Kategorien, umso besser ist die Adresse. Wer nie im Versandhandel bestellt, wird auch seltener von ungewollten Zusendungen belästigt. Wer häufig via Katalog einkauft, findet volle Briefkästen vor, da seine Adresse die Runde macht. Personen, die in der Branche als »gute Adresse« gelten, bekommen mindestens dreimal pro Woche eine an sie persönlich adressierte Werbesendung.

Wobei einige Versandhäuser mit ihren Kundendaten nicht leichtfettig umgehen. Donauland oder der Universal-Versand geben ihr Adreßmaterial nicht weiter, auch Banken, Versicherungen und Kreditkartenunternehmen hülen ihre Kundenkarteien wie Juwelen. Reiner Selbstzweck, denn es wird einfach tunlichst vermieden, der Konkurrenz geheime Firmendaten zur Verfügung zu stellen.

Wer aber häufig bei Beate Uhse oder beim Orion-Verlag bestellt, gilt in der Branche als »Superadresse«. Denn die Käufer von Dessous, Erotikartikeln und Videos lassen sich auch Produkte von nichterotischen Versandhäusern gerne zuschicken - von Schuhen und Schallplatten bis zu Kleidung und Elektronik.

Besondere Aufmerksamkeit sollte man bei den diversen Gutschein-Heften walten lassen, die in regelmäßigen Abständen ins Haus flattern. Neben Rabatten beim nächsten Einkauf, streng



limitierten Porzellanpuppen oder Keramiktellern für »alle unsere Kunden« gibt es auch Preisausschreiben. So hat etwa die »Quelle Bank« 1997 ein Preisausschreiben veranstaltet, bei dem es einen BMW Z 3 zu gewinnen gab. Die »Gewinnfrage«: Man mußte lediglich sein Geburtsdatum auf der Vorderseite als Glücksnummer eintragen. Eine geschickte Methode, um an das Alter eines potentiellen Kunden zu gelangen. Und obendrein äußerst lukrativ, wenn man davon ausgeht, wieviel man für das Zusatzmerkmal Alter bezahlen müßte, würde man dieses bei einem Adreßhändler kaufen.

Aufgepaßt auf Kleingedrucktes! Wer diverse Gutscheine ausfüllt, und Informationsmaterial beschafft, sollte das Klcingedruckte beachten, denn ein gedankenloses Ausfüllen kann eine ungeahnte Werbeflut nach sich ziehen. Beim Bestellbon für einen Quelle-Katalog steht beispielsweise: »Da ich an Informationsmaterial interessiert bin, können mein Name/Adresse weitergegeben werden, insbesondere an Unternehmen des Quelle-Konzerns; ich bin zum jederzeitigen schriftlichen Widerruf berechtigt.«

Konsumentenschützer raten, das Kleingedruckte durchzustreichen, denn die Firmen müssen sich daran halten.

Der Amstettener Franz N. ist einer von Zehntausenden Österreichern und Deutschen, die 50000 Mark gewonnen, diese aber nie erhalten haben. Unseriöse Versandhäuser versprechen Millionengewinne, Autos, exklusive Urlaubsreisen etc. Die Gewinnscheine, die den Betroffenen zugeschickt werden, entpuppen sich meist als Faksimile einer Urkunde - wenn der Betroffene tatsächlich gewinnen sollte, werde der Gewinnschein so aussehen.

Obwohl die Konsumentenschützer immer wieder diese Geschäftspraktiken anprangern, lassen sich Versandhäuser nicht abhalten, Unwissenden das sprichwörtlich Blaue vom Himmel zu versprechen. Firmen, ob sie sich Euromail Ltd., Baronesse Service E.U.R.L. oder 3 Suisses nennen, haben nur ein Ziel: Sie sind auf der Jagd nach guten Adressen. Sie suchen Kunden, die auf ihre Schreiben antworten. Die Reaktion auf ein Schreiben macht aus der Adresse eine gute, die weiterverkauft werden kann.

Wer sich durch solche Schreiben belästigt fühlt bzw. wer Superpreise gewonnen hat, aber nie ausgehändigt bekam, dem raten die Konsumentenschützer zu klagen. Die Französin Madeleine D. hatte

damit Erfolg. Es sah so aus, als hätte sie bei einem von der Firma »France Direct Service« veranstalteten Glücksspiel den Hauptpreis gewonnen -einen Renault 21 oder 100000 Franc. Sie forderte den Geldbetrag an und bekam ein Schreiben retour: »Das Ihnen zugestellte Glückwunschschreiben ist lediglich ein Muster der offiziellen Benachrichtigung, die wir Ihnen zustellen, wenn Sie wirklich gewinnen.« Die Frau ging vor Gericht und bekam teilweise recht: sie erhielt 50000 Franc Schadenersatz.

## Wie unsere Kaufkraft berechnet wird

Wo leben die reichsten Deutschen, wo die ärmsten Österreicher? Seit 1965 erstellt Fessel-GfK die Kaufkraftkennziffern für alle 2377 Gemeinden in Österreich und 14620 Gemeinden in Deutschland. 100 ist der Wert für den Gesamtdurchschnitt, liegt eine Gemeinde über diesem Wert, ist die Kaufkraft überdurchschnittlich, ist die Kaufkraftkennziffer nur zweistellig, so sind die Menschen, die in diesen Gemeinden leben, ärmer.

Basis der GfK-Kaufkraftkennziffern bildet das Nettoeinkommen. Aus den Lohn- und Einkommensteuerstatistiken, Pensionen, Einkünften aus der Land- und Forstwirtschaft, aus dem Fremdenverkehr sowie aus der Arbeitsmarktsituation werden die Kennziffern errechnet. Parallel dazu werden auch soziodernografische Merkmale herangezogen.

Die reichsten Deutschen leben in Hochtaunuskreis, Starnberg, München Land und München Stadt, die ärmsten in Demmin, Uecker-Randow, Guestrow und Uckermark. Der Vergleich des reichsten Kreises mit dem ärmsten bringt eine riesige Kluft zutage. Die Kaufkraft eines Deutschen, der in Hochtaunuskreis wohnt, ist mit 141 mehr als doppelt so hoch als jene eines Bürgers aus Demmin (67). Das Ost-West-Gefälle ist bei den Kaufkraftzahlen offensichtlich. Denn im ehemaligen Ostdeutschland gibt es lediglich zwei Gemeinden, die über dem Bundesdurchschnill liegen: Berlin (102) und Kleinmachnow (107). Wer eine Kaufhauskette zuerst in einer kaufkraftstarken und dann in einer kaufkraftarmen Gemeinde besucht, erkennt durch das unterschiedliche Warenangebot sofort, wie sehr diese Kaufkraftzahlen das geschäftliche Umfeld beeinflussen.



Das gleiche Ergebnis würde durch einen Vergleich in Österreich erzielt werden. Die reichsten Österreicher leben in Lech am Arlberg (153,3). Das bedeutet, daß dem durchschnittlichen Lecher um 53 Prozent mehr Geld zur Verfügung steht als dem durchschnittlichen Österreicher. Die ärmste Gemeinde ist die Gemeinde Namlos in Tirol mit einem Pro-Kopf-lndcx von 37,4.

An der zweiten Stelle der Kaufkraft-Hitliste rangiert die oberösterreichische Gemeinde Puchenau, gefolgt von Salzburg. Am Ende der Kaufkraftskala finden sich meist kleine Gemeinden in Tirol und der Steiermark. Von den 100 ärmsten Gemeinden Österreichs befinden sich übrigens 62 in der Steiermark.

Grundsätzlich werden jene Gemeinden höher bewertet, die einen hohen Anteil an Erwerbstätigen haben, wie etwa Landes- und Bezirkshauptstädte.

## Die »schlechte Adresse«

Vor allem im Versandhandel, bei Kreditkartenunternehmen, aber auch in den Mobilfunkunternehmen werden die Daten von neuen Kunden laufend mit den bestehenden Informationen abgeglichen. Auf Datenbanken sind »schlechte Adressen«, aber auch «schlechte Namen« gespeichert. Bestimmte Straßenzüge, Häuser, Gemeindebauten sind mit einem schwarzen Punkt versehen. Bewohner dieser Häuser gelten als »schlechte« Kunden.

Die »Schlechte-Adressen-Datenbank« wird mit mehreren Informationen gefüttert. Zum einen werden die Kaufkraftdaten eingespeichert - je geringer die Kaufkraft, desto höher die Wahrscheinlichkeit, daß bei Kunden aus diesen Gebieten Zahlungsprobleme zu erwarten sind.

Zweiter Hintergrund dieser »schwarzen Liste« sind Vorfälle in der Vergangenheit. Wenn es mehrmals in den vergangenen Jahren vorgekommen ist, daß Kunden, die in dieser Gegend wohnen oder gewohnt haben, Rechnungen schuldig geblieben sind, kommen diese Adressen auf einen Index. Kunden, die etwas bestellen, erhal-

ten bei Versandhäusern die Ware nur gegen Nachnahme. Die Möglichkeit einer späteren Bezahlung mittels Erlagschein ist ausgeschlossen.
Wenn beispielsweise im Gemeindebau auf der Hauptstraße 20 mehrere Bürger Bestellungen nie bezahlt haben, erhalten sie Waren nur gegen Nachnahme oder gar nicht. Das kann aber auch jene Nachbarn treffen, die kaufkräftig sind und noch nie jemandem etwas schuldig geblieben sind.
Ende November 1997 hat der Versandhandel in Österreich eine »Aktion scharf« gestartet. Wie die »Salzburger Nachrichten« (26. 1 1 . 1997} berichteten, haben sich die vier größten Versandhäuser - Quelle, Universal-Versand, Neckermann und Otto - zu einer Notgemeinschaft zusammengeschlossen und eine gemeinsame Negativliste erstellt, in der »schlechte« Kunden aller vier Unternehmen zusammengeführt wurden. In diese Datei kamen all jene, die den Versandhäusern seit 1992 Geldbeträge schuldig geblieben sind, und sie wird weiterhin geführt.
Ende 1997 umfaßte diese schwarze Liste insgesamt 190000 Kunden. Die Namen der »schwarzen Schafe« sind beim Kreditschutzverband aus 1870 (KSV) kostenpflichtig erhältlich. Nach Bekanntwerden dieser Negativdatei haben sich mehrere branchenfremde Unternehmen dafür interessiert.

## Bausparvertrag für Neugeborene

Das Image der Adressen-Branche ist nicht das beste. Wobei der Firmenbereich relativ unproblematisch ist, da Firmendaten keine personenbezogenen Informationen beinhalten und Daten auch im Firmenbuch bzw. noch detaillierter bei der Wiesbadener SCHUFA bzw. beim Wiener Kreditschutzverband aus 1870 erhältlich sind. Bei den österreichischen Direktmarketing-Unternehmen sind Daten von insgesamt 280000 Firmen erhältlich, bei den deutschen sogar von vier Millionen Unternehmen. Bei den Firmendaten werden die Unternehmen sogar angerufen, um die Namen der Ansprechpartner zu erheben.
Bei diesem Business-to-Business-Marketing ist es vielen Unternehmen sogar recht, Werbematerial von anderen Firmen zugeschickt zu bekommen. Diese Adressen sind nach Branchen und Marktsegmenten unterteilt. Es wird unter anderem nach Herstellern, Handwerk, Bau, Handel oder Dienstleistung unterschieden.
Heikler sind die Daten von Privatpersonen. Im Privatbereich kommt es häufig zu Fällen von Mißbrauch, die Datenschützer auf die Barrikaden steigen lassen. Die Eltern eines Neugeborenen im bayrischen Würzburg waren überrascht und verärgert zugleich, als wenige Tage nach der Geburt ein Schreiben von einer Bausparkasse ins Haus flatterte, auf dem der Abschluß eines entsprechenden Vertrages für den »Neuankömmling« empfohlen wurde. Zu vergleichbaren Fällen kommt es auch in Österreich immer wieder.



## Die Adressenverfeinerer

Der Firmenchef kommt mit einem Magnetband unterm Arm zum Adreßhändler. 100000 Personen umfaßt seine Kundendatei. Die Adressen haben aber einen Makel - zum einen fehlt das Alter, zum anderen sind einige Kunden verstorben oder haben seit Jahren nicht mehr eingekauft.
Das Material wird im Großrechner der Adreßhändler verfeinert, indem die Daten von komplizierten Computerprogrammen mit diversen Dateien verrastert werden. Die Adressen werden mit einem Postleitzahl- und einem Straßenverzeichnis abgeglichen, um simple Schreibfehler auszubessern. Danach laufen die Daten über die Kaufkraftdatei, bei der jede Adresse mit dem entsprechenden Kaufkraftindex verknüpft wird. Je höher der Wert, umso mehr dürfte der Kunde ausgeben, die Adresse kann so als gut, mittel oder schlecht beurteilt werden. Um das Alter der Kunden zu eruieren, werden die Vornamen von einem Software-Programm analysiert.
Warum Adressen für die Wirtschaft eine so große Bedeutung haben, ist leicht erklärt: Mit der richtigen Adresse verkürzt sich der Weg vom Interessenten zum Käufer. Ist ein potentieller Kunde namentlich bekannt und kann er persönlich angeschrieben werden, so steigert sich die Kaufwahrscheinlichkeit um das Zehn-

fache. Durch gezieltes Direktmarketing werden die Streuverluste, die durch normale Massensendungen entstehen, minimiert und so Kosten gespart.

Die Kaufkraftklasse ist eines der wichtigsten Kriterien. Kaufkräftige Männer und Frauen werden zu Autopräsentationen oder Modeschauen eingeladen. Familien werden familienfreundliche Reisen, Möbelhaus-Aktionstage mit angeschlossenem Kinderprogramm oder Lebensversicherungen angeboten, junge Männer und Frauen werden von Sporthotels umworben, Frauen mittleren Alters zum Testen einer neuen Kosmetiklinie angeschrieben.

Verfeinert werden Adressen auch mit soziodemografischen Daten aus dem Statistischen Bundesamt in Deutschland bzw. dem Statistischen Zentralamt in Wien. Wichtiger Index-Messer ist auch der »Mietspiegel«. Personen, die in teureren Wohngegenden leben, werden als besser qualifiziert eingestuft als jene in billigeren Wohnvierteln.

Will ein Unternehmen Adressen kaufen, so wird das gewünschte Kundenprofil erhoben. »Wir besorgen uns dann Adressen vom Markt, die dem Profil entsprechen«, erklärt der geschäftsführende Gesellschafter von Schober Direktmarketing, Anton Jenzer. »Einfach gesagt, versuchen wir Kunden zu klonen, da wir wissen, welche Eigenschaften er hat.« Versandhauskunden entsprechen gewissen Charakteristika, obwohl es im Direktmarketing noch keine Typologie gibt, wie sie auch in der Werbung gebräuchlich ist.

Das Material besorgen sich die Adreßhändler von sogenannten Listbrokern. Gute Namen und Adressen werden beinahe so gehandelt wie Aktien an der New Yorker Wall Street. Ähnlich wie an der Börse sind Broker Vermittler zwischen Käufer und Verkäufer. Beim Listbroking stellt ein Adreßvermieter seine Adreßliste dem »neutralen« Broker zur Verfügung. Ist ein Kunde an neuem Datenmaterial interessiert, werden ihm nicht die Adressen des Vermieters überreicht, sondern der Broker schreibt jeden einzelnen Kunden direkt an. Diese antworten direkt dem neuen Mieter und werden dann in dessen Kundendatei gespeichert. Die sogenannten »Nichtreagierer« scheiden aus.



## Wie der Vorname Ihr Alter verrät

Sie heißen Claudia? Dann sind Sie mit relativ hoher Wahrscheinlichkeit zwischen 23 und 31 lahre alt. Der Vorname Claudia war vor allem zwischen 1967 und 1975 sehr beliebt. Helga war ein Modename, den Eltern ihren Töchtern gerne in den Jahren 1935 bis 1945 gaben. Auch der Vorname Erika war vor allem zwischen 1940 und 1945 beliebt, wer Bernd heißt, ist mit hoher Wahrscheinlichkeit zwischen 25 und 35 lahre alt.

»Alters-Zuordnung über Vornamen-Analyse« nennt sich jenes Computer-Software-Programm, das bei den deutschen und österreichischen Adreßhändlern eingesetzt wird. Wie es funktioniert, ist einfach erklärt: Es analysiert den Vornamen und grenzt das Alter ein. Erzielte Genauigkeit: 70 Prozent.

Vornamen sind häufig Modeerscheinungen. Simone, Oliver, Nicole und Corinna sind z.B. in den vergangenen zwei Jahrzehnten modern gewesen. In den Zeitungen wird am Jahresende immer die »Hitliste« der im abgelaufenen Jahr beliebtesten Vornamen veröffentlicht. Diese »Hitlisten« der vergangenen neun Jahrzehnte sind die Basis eines Computerprogramms.

Der Name Adolf beispielsweise wird seit dem Ende des Zweiten Weltkrieges nur noch sehr selten vergeben. Wer heute Adolf heißt, ist entweder vor oder während des Zweiten Weltkrieges zur Welt gekommen, oder er hat den Namen seines Vaters »geerbt«, weil es in Familien üblich ist, den Sohn nach dem Vater zu nennen.

Eine Ungenauigkeit von 30 Prozent bleibt aber bestehen. Vornamen,wie Franz, Josef, Johann oder Karl sind nur sehr schwer zeitlich zuzuordnen, da dies typisch österreichische bzw. deutsche Namen sind, die auch heute noch üblich sind.

## So viel kostet Ihr Name

Der Handel mit Adressen ist zum lukrativen Geschäft geworden. Die deutsche Direktmarketingbranche hat allein 1997 33 Milliarden Mark umgesetzt. Eine Firmenadresse kostet zwischen 30 Pfennig und eine Mark. Der Preis ist davon abhängig, ob die Adresse

auch noch mit Ansprechpartnern vervollkommnet ist, sprich: Marketingchef, Werbeleiter und Geschäftsführer.

Etwa 35 Pfennig beträgt der Grundpreis einer Privatadresse bei einer Stückzahl von 5000 Stück. Für eine Superadresse, einen »Postkäufer«, muß ein Kunde sogar etwa 60 Pfennig bezahlen. Der Einzelpreis sinkt, je mehr Adressen bestellt werden. Dieser Preis ist übrigens nur die Miete für eine einmalige Verwendung. Wer eine Adresse mehrmals verwenden oder gar kaufen möchte, muß ein Vielfaches davon bezahlen. Der Handel ist aber auch für den Mieter interessant, da er sich jene Adressen kostenlos behalten kann, die auf seine Werbeaktion persönlich reagiert haben. Der Kauf ist für Unternehmen allerdings nicht sehr sinnvoll, da die Aktualisierung und Wartung der Daten oft kostspieliger ist als die Miete von Daten, die sich ohnehin ständig auf dem neuesten Stand befinden.

Eine »nackte« Adresse enthält Narnen, Geschlecht, Adresse, Bundesland, Gemeinde, Postleitzahl, Ortsgröße und den politischen Bezirk. Jedes »Zusatzmerkmal« kostet extra, jede Telefonnummer 25 Pfennig. Apropos Zusatzmerkmal: 12 stehen zur Auswahl, »weitere Merkmale gibt es auf Anfrage«, wird in deutschen und österreichischen Prospekten geworben. Unter Zusatzmerkmalen verstehen die Adreßhändler Alter, Kaufkraft, Haushaltsgröße, Familien mit Kindern, akademische Ausbildung, Namenstage, Hausgröße, Titel, Handy-Besitzer, Postkäufer, Fax-Besitzer und Wohndauer. Alleine diese »Sammlung« beweist, daß mehr Informationen über die Bürger bekannt sind, als viele für möglich halten. Wer einen ungewünschten Brief eines Verlages, eines Versandhauses oder bereits die zehnte Gewinn-Benachrichtigung einer der unzähligen unseriösen Firmen vorfindet, muß sich bewußt sein, daß diese mehr wissen als nur Namen und Adresse. Oft auch Hobbys und private Interessen.

Wenn ein Kunde 100000 Adressen von sportinteressierten Frauen aus Hamburg im Alter von 30 bis 40 Jähren bestellt, dann erhält er sie. Wer 50000 kulturinteressierte Männer zwischen 50 und 65 sucht, die Interesse an einer neuen Karajan-CD-Sammlung haben könnten, wird auch dieses Material binnen weniger Tage erhalten. Ob Kleingarten-, Handy- oder Autobesitzer, nichts bleibt den Adreßhändlern verborgen.



Bei der Aktualisierung ihres Materials sind Adreßverlage oft nicht zimperlich, wie Bundesdatenschützer Joachim Jacob in seinem Tätigkeitsbericht 1995-1996 festgestellt hat. Aktuelle Anschriften potentieller Kunden sind für die Direktwerbung von entscheidender Bedeutung. Mit Hilfe der Post versucht die Werbebranche, möglichst akutelle Anschriften zu führen.

»Haben umziehende Bürger bei der Post einen Nachsendeantrag gestellt und in den Adressentausch »neu gegen alt« auch für Dritte eingewilligt, erhält die Firma »Deutsche PostAdress GmbH« die alten und die neuen Anschriften«, erklärt Jacob. Mit diesem Bestand können Versender und Adreßhändler ihr Adressenmaterial aktualisieren. Sechs Monate lang dürfen diese Daten gespeichert werden, dann müssen sie gelöscht werden.

Die PostAdress hatte aber versucht, aus diesem Material Kapital zu schlagen und hatte die Anschriften nach Ablauf des Nachsendeauftrages Listbrokern zur Verfügung gestellt. Jacobs Intervention bei der Deutschen Post AG hat diesem schweren Datenmißbrauch ein Ende bereitet.

## Robinsons Liste

55000 Österreicher und 360000 Deutsche - so viele stehen auf der sogenannten »Robinson-Liste«. Wer sich auf diese Liste setzen läßt, bekommt keine persönlich adressierte Werbung zugeschickt. Dieser Schritt ist notwendig, da die Post gesetzlich dazu verpflichtet ist, persönlich adressierte Briefe zuzustellen. Etwa 3000 Österreicher und 25000 Deutsche beantragten bei der Fachverband-Werbung in der Wiener Wirtschaftskammer, bzw. beim Deutschen Direktmarketing Verband (DDV} in Ditzingen in den Robinson-Eintrag und verzichten damit jedes Jahr auf Dutzende Briefe und Informationsschreiben.

Seit 1993 sind die Adreßhändler verpflichtet, schon bestehendes Adreßmateria! mit der Robinson-Liste abzugleichen. Viermal im Jahr werden aus den Beständen unerwünschte Namen gestrichen. Freilich sind die Adreßhändler über die Robinson-Liste nicht ganz erfreut, intern trägt sie den Namen »Negativdatei«.

Aber nicht jeder Eintrag auf diese Liste hat Erfolg, denn die eigenen Kunden muß eine Firma nicht streichen.

Auf keinen Fall aber sollten persönlich adressierte Sendungen, vor allem Versandhaus-Kataloge, im Müll landen. Im Sommer 1997 wurde in Wien nämlich eine Jugoslawen-ßande aufgedeckt, die sich Versandhauskataloge aus dem Altpapier-Container besorgt und Waren auf Kosten anderer bestellt hatte.

Die siebenköpfige Bande durchstöberte die Container nach Namen, Adressen und Kundennummern. Die Bestellungen ließen sie sich an leerstehende Wohnungen schicken, die Rechnungen gingen an den rechtmäßigen Kunden. Etwa 200 Kunden, die ihre Kataloge achtlos weggeworfen hatten, mußten so Rechnungen für Artikel bezahlen, die sie nie bestellt hatten. Der Schaden ging in die Millionen.

Ein Eintrag auf der Robinson-Liste verschont einen Haushalt aber nicht von Flugblättern und nichtadressierter Werbung, von der pro Jahr beinahe 100 Kilogramm in jedem Briefkasten landen. Wer sich davor »schützen« möchte, kann beim Verein für Konsumenteninformation einen »Werbung unerwünscht«- oder »Bitte kein Reklamematerial«-Kleber anfordern. Die Kleber haben eine Registriernummer, die Verteiler haben diesen Wunsch zu respektieren. Wenn nicht, droht dem Werbemittelverteiler eine Besitzstörungsklage.

Auch Zusendungen, die »An einen Haushalt« gehen, kann man verhindern. Seit 1990 hat die österreichische Post ein eigenes Formular aufgelegt, auf der der Bürger erklärt, solche Information nicht in Empfang nehmen zu müssen. Zuschriften von Behörden, Ämtern oder Parteien, die »An einen Haushalt« ergehen, sind von dieser Regelung ausgenommen und werden dennoch zugestellt.

## Adreßhändler im Internet

Die unerwünschte Werbung ist in den vergangenen Jahren um eine Facette reicher geworden, die vor allem Internet-User betrifft: Wer durchs Internet surft, hinterläßt seine Spuren, die von findigen Adreßhändlern gesammelt und dann verkauft werden. Die Folge sind E-Mail-Briefkästen, die vor Online-Werbung überquellen.



»Der elektronische Briefkasten hat mit seinem Gegenstück an der Haustür leider eines gemeinsam«, schrieb die »Computerwelt« (Nr. 15/97). »Er ist offen für Werbung aller Art. Immer mehr Firmen verbreiten ihre Werbung nach Flugblattmanier im Internet.« Schnell und billig wird ein vorselektiertes Publikum, eine Zielgruppe erreicht: Bürger, die einen PC besitzen und das Internet nutzen. Auch »Focus« (Nr. 47/97) hat auf den »Reklamemüll per Datennetz« aufmerksam gemacht und auf die Problematik der E-Mail-Werbung hingewiesen.

Wer am morgen seinen Computer in Betrieb nimmt, der wird in Zukunft immer öfter neben diversen geschäftlichen und privaten E-Mails auch Werbe-E-Mails vorfinden. Auf die 5 Millionen deutschen und etwa 500000 österreichischen Online-User kommen mitunter teure Zeiten zu. »Wenn allein das Adreßfeld einer sinnlosen E-Mail 350 Empfängernamen umfaßt und der Nutzer so minutenlang auf eine Megadatei warten muß, platzt vielen Surfern der Kragen«, schrieb der »Focus«. »Denn: E-Mails können nur online abgerufen werden, und jede Sekunde im Datennetz kostet Telefon- und Providergebühren.«

Der deutsche Adreßhandel hat den Trend der Zeit erkannt und Mitte 1997 begonnen, Datenbanken mit Tausenden privaten E-Mail-Adressen aufzubauen. »Woher die Adressen stammen, ist Firmengeheimnis«, so »Focus« und zitiert Bettina Höfner vom Deutschen Direktmarketing Verband. »Es ist günstiger als ein klassisches Mailing.« Höfner schätzte, daß Ende 1997 bereits bis zu 10 Prozent der deutschen Internet-User in Online-Reklamedatenbanken gespeichert sind.

Dabei gibt es ein Urteil des Landesgcrichts Traunstein, das untersagt, »Werbung an Privatleute über E-Mail ohne vorherige Zustimmung der betroffenen Personen zu senden«. Wenn eine Firma trotzdem E-Mail-Werbung verschickt, droht ihr eine Strafe bis zu 500000 Mark. In Österreich gab es 1997 noch kein vergleichbares Urteil, ein Gericht dürfte aber ähnlich entscheiden. Denn 1997 wurde unerwünschte Werbung, die über das Fax eingelangt ist, als Besitzstörung gewertet. Es sei dem »Faxbesitzer unzumutbar, für Werbung, die er nicht will, Papier zu bezahlen«, schrieb der »Kurier« (3. 1 1 . 1997). Dieses Urteil könnte 1 : 1 auf E-Mail umgelegt werden, denn anstelle von Papier fallen bei E-Mail-Werbung unge-

wollte Telefonkosten durch das Herunterladen der elektronischen Nachricht an.

Doch allen Urteilen zum Trotz wird weiter munter mit E-Mails geworben. Die »Computerwelt« (Nr. 15/97) stellte sogar Unternehmen vor, die anderen Firmen Technologien anbieten, wie sie aus E-Mails von Privaten persönliche Vorlieben und Interessen eines Surfers herauslesen können. Als Beispiel wurde die US-Firma Focalink Communications (http://www.focalink.com) vorgestellt. Diese wirbt mit einer sogenannten »Smartbanner«-Technologie, die das Benutzerprofil eines Web-Surfers erstellt. Nach der gleichen Methode arbeitet Doubleclick (http://www.doubleclick.com). Die US-Firma hat, so »Computerwelt«, die umfassendste Datenbank von Internet-Anwendern.

Es gibt aber dennoch verschiedene Möglichkeiten, E-Mail-Werbung zu verhindern. E-Mails mit unbekannten Absendern sollte man löschen, ignorieren oder ungelesen zurückschicken. Damit ist auch die schon erwähnte Gefahr, daß auf dem Home-PC Computerviren landen, gebannt.

Bei America Online (AOL) gibt es sogar einen elektronischen »Werbung unerwünscht«-Kleber. Das Program »eMailFilter« läßt E-Mails bekannter Reklameversender nicht durch. Auch CompuServe bietet eine solche Software an. Bestimmte Provider haben von sich aus entschieden, Werbe-E-Mails nicht an die Kunden weiterzuleiten. T-Online beispielsweise stoppt Massensendungen und hat damit die Provider-Konkurrenz unter Zugzwang gebracht. Ein Vorteil für Kunden, da dies vielleicht bei einigen Providern zum Umdenken führen könnte.

Wer dennoch Werbe-E-Mails erhält, sollte sich beim Provider beschweren. So wie bei persönlich adressierten Werbebriefen gibt es in Deutschland auch für das Internet eine Robinson-Liste (http://www.eRobinson.com). Der Leiter des Münchner Forschungszentrums Direktmarketing, Robert Bidmon, fordert im »Focus« (Nr. 49/97) eine Kennzeichnungspflicht für E-Mail-Werbung. »Massenmails widersprechen dem Grundgedanken im Internet.«



## Heiße Adressen auf Telefon-CDs

Mit den Informationen auf den silbernen Scheiben haben nicht nur Adreßhändler ihre Freude, auch kleine Firmen, die auf Knopfdruck potentielle Kunden in bestimmten Gegenden erreichen wollen. Seit 1996 sind in Österreich und Deutschland Telefon-CDs auf dem Markt, die mehr können als nur eine Nummer zum Namen suchen. Sie beherrschen die sogenannte Vice-versa-Abfrage, auch Inverssuche genannt.

Wer den Namen zu einer Nummer sucht, die ihm eine Dame oder ihr ein Herr zugesteckt hat, der kann mit Hilfe dieser CDs den Namen des Verehrers, der Verehrerin erforschen.

Theoretisch könnte eine Ehefrau, die im Sakko ihres Mannes einen Zettel mit einer Telefonnummer findet, mit Hilfe dieser CD herausfinden, daß das die Nummer der Geliebten ist. Auch in Niederösterreich wohnhafte Ingenieure, die mit P. beginnen, lassen sich auflisten. (Ing. P. war einer der Verdächtigen im Zuge der Ermittlungen im österreichischen Briefbomben-Kriminalfall.) Das Ordnen nach Kategorien ist zwar untersagt, aber leicht möglich.

Warum sich diese Telefon-CDs für den Adressenhandel gut nützen lassen, ist leicht erklärt: Durch gewisse Suchkriterien läßt sich die Menge der Telefonkunden - in Deutschland etwa 35 Millionen, in Österreich 4 Millionen - gut und effektiv selektieren. Wer Bauunternehmen sucht, gibt nur den Begriff »Baumeister« ein, das gewünschte Bundesland, eine Stadt oder eine Gemeinde. Binnen zwei Sekunden erhält er die gewünschten Informationen.

Auch in Deutschland gibt es eine solche CD, obwohl der Verkauf 1996 kurzfristig gestoppt wurde. Mit ihrer CD-ROM »D-Info« hatte die Mannheimer Marketinggesellschaft TopWare Marketing einen Erfolg gelandet, der erst durch Datenschützer und die Telekom-Tochter DeTeMedien gestört wurde. 600000 CD-ROMs, ä 50 Mark, hatte TopWare innerhalb von vier Monaten verkauft, als die einstweilige Verfügung das lukrative Geschäft beendete. Die 7. Zivilkammer des Landesgerichts Mannheim hatte am 19. Februar 1996 (7055/96) entschieden, daß es datenschutzrechtliche Bedenken gegen D-Info gibt. Durch die sogenannte Inverssuche kommt man nicht nur von der Nummer, sondern auch von der Adresse zum Namen. Genutzt hat das Urteil nicht viel, denn die

neueste D-Info-CD ist über einen österreichischen Vertrieb (Koch Media) weiter erhaltlich, da in Österreich die strengeren deutschen Telekom-Gesetze nicht gelten.

Neben den datenschutzrechtlichen Bedenken kam aber auch die Urheberrechtsfrage zur Sprache. DeTeMedien hatte eine Telefon-CD verkauft. Als TopWare mit ihrer CD-ROM auf den Markt kam, klagte DeTeMedien sofort, weil TopWare die Nummern von der DeTe-CD entnommen haben soll und das eine Verletzung des Urheberrechts sei.

In Deutschland hatte man schon einmal mit einer ähnlichen Telefon-CD 1995 schlechte Erfahrungen gemacht. Damit konnte ein Telefonteilnehmer nicht nur bundesweit gesucht werden - auf Knopfdruck listete der Computer alle in Deutschland lebenden Hans Müller auf -, sondern auch »komfortable Suchvarianten« waren möglich. So konnten etwa alle Telefonteilnehmer eines bestimmten Straßenzuges aufgelistet werden. Bestürzt waren die Datenschützer aber über einige Beifügungen, die bei den Adressen angeführt wurden, wie z.B. »Villengegend«. »Damit hat man Einbrechern signalisiert, daß es dort möglicherweise etwas zu holen gibt«, kritisiert Datenschützer Werner Schmidt aus dem Büro des Bundsbeauftragten Jacob.

In Deutschland gilt seit 19. Juli 1996 ein abgestuftes Widerspruchsrecht, das in Österreich freilich nicht gilt. Der Telefonkunde kann selbst entscheiden, ob überhaupt und in welcher Form er in ein Verzeichnis eingetragen werden möchte. In den internen Dateien der Netzbetreiber sind Kunden, die nicht im Telefonbuch oder auf einer CD aufscheinen wollen, mit einem * gekennzeichnet. Dadurch ist aber wieder ein anderes Problem offenkundig geworden. Zahlreiche Deutsche befürchten durch die Kennzeichnung mit dem * eine Stigmatisicrung ihrer Person, etwa als technik- und kommunikationsfeindlich.

Wie in der Adreßbranche üblich, sind sowohl in den Adreßkarteien wie auch in den Telefonbüchern »Scheinnummern«, sogenannte Dummy-Adressen, eingebaut. Jeder Adreßhändler baut seine eigenen Scheinadressen in sein Material ein, um einem unliebsamen Konkurrenten, der die Adressen kopiert, nachweisen zu können, aus welcher Quelle sie wirklich stammen. Ähnlich machen es auch Lexikahersteller. Es werden Suchbegriffe eingebaut, nach denen kein Mensch sucht. Kommt ein neues Lexikon auf den Markt, wird sofort kontrolliert, ob diese »sinnlosen Suchbegriffe« enthalten sind. Wenn ja, wird geklagt. TopWare wurden seinerzeit offenbar Dummy-Adressen zum Verhängnis, schrieb auch die »Zeit« (22. 12. 1995) und erwähnte noch einen zweiten CD-ROM-Hersteller, der von DeTeMedien geklagt worden war: Die Firma IBS hatte eine CD-ROM mit dem Namen Tele-Info auf den Markt gebracht. IBS behauptete aber, die Nummern durch Scannen der Telefonbücher erworben zu haben.



In Österreich gibt es mit den Telefon-CDs weit weniger Probleme. Im Gegenteil, die Inverssuche ist gesetzlich erlaubt, wurde mit dem neuen Telekommunikationsgesetz, das seit 1. August 1997 wirksam ist, erst möglich. Die Herold Business Data AG, die auch die österreichischen Telefonbücher erzeugt und vertreibt, hat mit ihrer CD-ROM »Österreichisches Telefonbuch« (825 Schilling) anfangs ebenso für Aufregung gesorgt. Aber selbst Datenschützer mußten bestätigen, daß dies laut Telekommunikationsgesetz erlaubt ist. Glücklich sind sie dennoch nicht, denn mit der Telefon-CD lassen sich auch Adressen nach Vornamen selektieren. Auf Knopfdruck werden alle Ibrahims oder Samuels aufgelistet. Informationen, die Rechtsradikale nützen könnten.

# Die Spione der Lütte

> **Wie vom All aus die europäischen Bauern kontrolliert werden. Wie Satelliten Zigaretten- und Alkoholschmuggler verfolgen.**

> **Wie man vom All aus in unsere Gärten schaut.**

> **Wie künftig mit Satelliten Schwarzarbeiter gejagt werden.**

> **Wie uns Konzerne via Satellit überwachen lassen.**

> **Warum Seegrundstückbesitzer vor den elektronischen Augen zittern müssen.**

> **Wie man illegale Deponien entdeckt.**

## EU is watching you

Sie haben Deutschland und bald auch Österreich im Visier. In 705 bis 832 Kilometer Höhe umkreisen die amerikanischen Fernerkundungssatelliten LandsatTM 4 und 5, die Franzosen Spot 1, 2 und 3 sowie der Inder IRS IC die Erde und machen Aufnahmen von Feldern und Weiden in den EU-Mitgliedsstaaten. Sie sind Agrarbetrügern auf der Spur: Bauern, die sich durch falsche Angaben EU-Agrarförderungsmittel erschwindeln. Denn vom All aus kann genau festgestellt werden, was auf den Feldern wächst, Weizen oder Kaps, Gerste oder Mais. »Wenn ein Bauer angibt, Raps zu pflanzen, auf dem Feld aber Weizen anbaut, so hat er 552 Mark pro Hektar an Förderungen illegal kassiert«, erklärt Landwirtschaftsoberrat Josef Eichenseer aus der Abteilung »Einzelbetriebliche Förderung« des bayrischen Landwirtschaftsministeriums. »Das muß unterbunden werden.«
1988 hat die EU das Projekt MARS (Monitoring Agriculture by



Remote Sensing, Überwachung der Landwirtschaft durch Fernerkundung) beschlossen, zwei Jahre später wurde es auch gestartet. Vier- bis fünfmal pro |ahr schießen die Satelliten ihre Bilder, tasten die Flächen unten auf der Erde mit ihren hochempfindlichen Sensoren digital ab. jede Pflanze reflektiert unterschiedliche Infrarot-bereiche. Die Ergebnisse sind für Laien unspektakuläre, da unscharfe Schwarzweiß-Rasterbilder in 256 Crauwerten. Für die Experten der deutschen Gesellschaft für Angewandte Fernerkundung (GAF) in München und des EFTAS (Fernerkundung & Techniktransfer GesmbH} in Münster, die mit der Auswertung beauftragt werden, sind diese Aufnahmen aber höchst aufschlußreich. Denn jede Pflanze am Boden hat ihr eigenes Farbmuster, also ihren eigenen Grauwert. Um die Bilder besser überprüfen zu können, werden diese Grauwerte eingefarbt, wodurch beispielsweise Sonnenblumen blau, Raps violett und Roggen rot wird. Diese Bilder werden dann mit der digitalisierten Agrarflächenmappe und den Angaben der Bauern verglichen.
Seit 1991 werden deutsche Landwirte auf diese Art via Satellit überwacht. »Gut die Hälfte von ihnen weiß gar nicht, daß sie vom All aus kontrolliert wird«, ist selbst Landwirtschaftsexperte Eichenseer überzeugt. Vor allem für die kleineren landwirtschaftlichen Betriebe ist die Spionage aus dem Weltraum noch Science-fiction. Aber wenn die Landwirte dann mit den Daten aus dem All konfrontiert werden, sind sie »beeindruckt«, wie es Eichenseer bezeichnet, und schockiert zugleich - EU is watching you.
Keiner der 354000 deutschen Bauern, die einen Antrag auf EU-Förderung gestellt haben, weiß, ob und wann seine Felder kontrolliert werden. Die Wahrscheinlichkeit, daß er bei einer Kontrolle durch den Raster fällt, beträgt 1:20, denn die Europäische Union schreibt vor, daß 5 Prozent der geförderten Bauern kontrolliert werden müssen, insgesamt also 18000. 12000 wurden 1997 mit herkömmlichen Methoden kontrolliert.
Auf knapp 6000 deutsche Bauern werfen die Spione aus dem All ihr hochempfindliches Auge. Und die Kontrollen sind scheinbar notwendig, denn 420 Bauern mußtcn 1997 nachkontrolliert werden. Bei fast allen von ihnen wurden die Förderungen gekürzt oder ganz gestrichen, weil es »Unregelmäßigkeiten« gab.
Die Satellitentechnik ist die Methode der Zukunft. Denn selbst

durch dicke Wolken können Radarbilder der europäischen Satelliten ERS 1 oder 2 fehlende digitale Aufnahmen ersetzen. Ab 1999 will man sich nur noch auf Satellitenmaterial verlassen und Vor-Ort-Kontrollen erst dann vornehmen, wenn die Aufnahmen Unregelmäßigkeiten ergeben. Andere Wissenschafter träumen sogar schon davon, daß Satelliten künftig über einen Chip verfügen, der automatisch Änderungen der Landnutzung erfaßt und zur Erde meldet. Wie die »FAZ« am 14. Juli 1997 schrieb, »besteht ein immens großes Interesse daran zu prüfen ob sich alle Staaten an die vereinbarten Verträge halten, oder ob sie in entlegenen Ecken doch den Wald roden oder eine Kernwaffenfabrik bauen«.

Die Aktion Agrarspionage ist mittlerweile in der ganzen EU verbreitet. Ausnahmen sind Luxemburg, da es dort keine Agrarflächen gibt, und Österreich, das sich bislang gegen die Satellitenüberwachung ausgesprochen hat. Der Grund: die Felder sind zu schmal. Inoffiziell spricht man aber davon, daß die Österreicher deshalb der guten alten Vor-Ort-Kontrolletreu geblieben sind, weil diese für zahlreiche Landwirte ein lukratives Nebeneinkommen darstellt (die Kontrollen werden vom Agrar-Markt-Service Austria [AMAJ organisiert). Mit den neuen, hochauflösenden US-Satelliten hat aber auch das Landwirtschaftsministerium keine Ausrede mehr, sich der Kontrolle zu verschließen. Ab 1998 werden die österreichischen Bauern also damit rechnen müssen, daß High-Tech aus Indien, USA oder Frankreich ein Auge auf sie wirft.

Michel Van de Steene von der Agrar-Sektion der EU-Kommission wehrt sich dagegen, die Agrarkontrolle via Fernerkundung als »Big-Brother-Aktion« abzustempeln: »Die Satellitentechnik ist eine objektive Methode, um den schwarzen Schafen auf die Spur zu kommen.« 3,2 Millionen Landwirte in der EU stellen jährlich einen Antrag auf Förderung. Insgesamt werden 16,2 Milliarden ECU (224 Milliarden Schilling/32 Milliarden Mark) an Beihilfen ausgeschüttet, aber nicht alle Förderungsmittel werden wahrheitsgetreu erworben. Die Satellitenspionage kostet EU-weit 20 Millionen ECU und bringt ein Vielfaches dessen herein, was sie kostet.

Dem Beispiel der EU folgend, nützen auch deutsche Gerichte die Archive der Satellitenbetreiber. Bilder vom All wurden auch einem bayrischen Landwirt aus dem Regensburgcr Raum zum Verhängnis. Er hatte 1994 behauptet, ehemals gepachtete landwirtschaftliche



Flächen von etwa 20 Hektar nicht für Milcherzeugung genutzt zu haben. Damit wollte er die Übertragung von Milchquoten an den Verpächter verhindern. Erstmals in der Geschichte ordnete dann ein Regensburger Gericht an, die Angaben des Bauern anhand von Satellitenaufnahmen zu prüfen, da man die Nutzung nahezu jeder Fläche in Bayern bis ins Jahr 1982 zurück ermitteln kann. Das Urteil des Gerichts vom 25. April 1996, Aklenzahl RO 7 K 941846, fiel vernichtend für den Bauern aus: »Er hat versucht, durch unrichtige Angaben über Art und Nutzung von Pachtflächen zu täuschen«, stellten die Richter fest. Es konnte nachgewiesen werden, daß 7,1 Hektar Grünland waren und 5,6 Hektar Mais - mehr als der Landwirt angegeben hatte. Aufgrund dieser Flächen konnte hochgerechnet werden, daß er weniger Kühe im Stall gehabt haben muß als behauptet. Der Landwirt mußte nicht nur für die Verfahrenskosten aufkommen, sondern auch die Auswertung des Satellitenmaterials in Höhe von 8500 Mark bezahlen.

Aber nicht nur die Landwirte werden vom All aus überwacht, auch die Fischer. Nach jahrelangen Verhandlungen hal sich der EU-Ministerrat 1996 geeinigt, die gesamte EU-Fischereitätigkeit durch Satelliten kontrollieren zu lassen, damit sich die stark dezimierten Fischbestände wieder erholen können, jedes Schiff ab einer Länge von zwölf Metern ist ab Mitte 1998 im Visier der elektronischen Augen aus dem Weltraum. Einzige Ausnahme: die kleine Küstenfischerei innerhalb von zwölf Seemeilen, die nicht länger als 24 Stunden auf See ist.

Aus 830 Kilometer Höhe wird festgestellt, ob sich die Schiffe in den erlaubten Gewässern befinden, ob zur richtigen Zeit gefischt wird und ob Fische auf offener See von einem Schiff aufs andere geladen werden, um die Fangquote zu umgehen. »Die Kontrolle des Fischereiwesens ist sehr einfach«, gibt ein EU-Kontrollor zu verstehen. »Jedes Schiff hat ein aktives GPS-System an Bord. Dieser Empfänger macht es uns leicht, das Schiff zu verfolgen und zu identifizieren.«

## *Schmugglerjagd vom All aus*

Aber nicht nur die Agrarkontrollore der Europäischen Union setzen auf die Spione aus dem All, auch die Betrugsbekämpfer der EU-

Kommission nutzen die Satellitentechnik im Kampf gegen Zigaretten-, Alkoholschmuggler und Zollsünder. Nachdem die EU Einnahmenausfälle in Milliardenhöhe hinnehmen mußte, wurde 1988 UCLAF ins Leben gerufen, UCLAF ist die Bezeichnung für die Direktion, die im Generalsekretariat der EU-Kommission für die Koordinierung der Betrugsbekämpfung zuständig ist. Allein durch den Zigaretten- und Alkoholschmuggel gab es 1997 Verluste in Höhe von einer Milliarde ECU, rechnet man den Abgabenentgang durch die illegale Einfuhr von Olivenöl, Computerteilen, Fleisch und Wein dazu, erhöht sich die Schadenssumme sogar auf 1,5 Milliarden ECU. Gerhard Hitzler, oberster UCLAF-Betrugsbekämpfer, gibt klar zu erkennen, welche Techniken seinem 125köpfigen Team zur Verfügung stehen: »Wir verfolgen Schiffe und Lastwagen und nutzen dabei passive und aktive Systeme, geostationäre Satelliten genauso wie die, die urn die Erde kreisen.« Im Klartext: Schiffe und Lkw werden entweder mit GPS-Sendern verfolgt, die vorher am Schiffsrumpf oder unter dem Lkw versteckt wurden, oder sie werden von Satelliten aus fotografiert.

Einen großen Coup landete UCLAF 1996 mit der »Operation Kolumbus«. Über Benelux-Häfen sollten etwa 20 Zigarettensendungen mit mehr als 220000 Kartons angeblich nach Afrika verschifft werden. Tatsächlich aber wurden die Zigaretten über den spanischen Schwarzmarkt wieder in die EU geschmuggelt. Die Betrugsbekärnpfer hatten die Schiffe und Lkw bereits im Visier.

Es ist zwar schwer, vom All aus bestimmte Lastwagen zu erkennen und sie einem bestimmten Frachter zuzuordnen. Innerhalb der UCLAF wird aber bereits darüber nachgedacht, die Transportunternehmer zu verpflichten, auf den Dächern ihrer Lkw Firmenbezeichnungen, Logos oder Kfz-Nummern anzubringen. Dadurch wären diese auch vom All aus leichter zu identifizieren. Hitzler: »Auch in New York sind auf die Dächer von städtischen Autobussen Nummern lackiert, damit die Polizei bei Unfällen oder Entführungen den Bus leichter identifizieren kann.« Was für die Amerikaner von Nutzen ist, könnte auch für Europa gut sein. Das wiederum würde aber eine umfassende Kontrolle der Spediteure bedeuten, denn parallel dazu wird überlegt, auch ein Zentralregister zu installieren. Diesem müßten dann Frachter bekanntgeben, welche Waren sie wohin führen, an wen sie ihren Lkw verliehen haben etc.



Der UCLAF, die innerhalb der Europäischen Union mit fast allen Polizei-, Zoll-, und Grenzdienststellen online verbunden ist und auch Privatdetektive engagiert, läßt an High-Tech sogar eigene Euro-Observationssatelliten im Orbit kreisen. Auflösung: 4 Meter. Im Kampf gegen das internationale Verbrechen werden aber auch Aufnahmen von Spionagesatelliten verwendet, die eine Genauigkeit von 10 Zentimetern aufweisen.

## Heiße Bilder aus dem All

Das »Abschiedsgeschenk« der Amerikaner an die Soldaten der Deutschen Bundeswehr war, zugegeben, eine Überraschung und eine Blamage zugleich. Die Amerikaner hatten das Geheimnis gelüftet, über das die Bundeswehr während ihres gesamten Einsatzes in Somalia gerätselt hatte. Die deutschen Soldaten hatten im Zuge ihrer Mission einmal fünf Lkw von Mogadischu ins Landesinnere überstellen müssen. Am Ziel angelangt, fehlte ein Lastwagen, logischerweise der letzte der kleinen Kolonne. Niemand wußte, wo er geblieben war, auch die einheimischen Fahrer hüliten sich in Schweigen. Die Antwort gaben Jahre später die Amerikaner mit ihrem »Abschiedsgeschenk«. Dieses waren nämlich Bilder, aufgenommen von amerikanischen Spionagesatelliten. Auf ihnen war klar zu erkennen, wo die Deutschen den Lkw »verloren« hatten, wo er abgebogen und weitergefahren ist und wer ihn schließlich wirklich erhalten hat. Im Verteidigungsminislerium in Bonn spricht man heute nur mit vorgehaltener Hand über diese an sich harmlose Geschichte.

Ahnlich überrascht war auch eine Gruppe österreichischer Soldaten im Rahmen ihres UN-Einsatzes auf dem Golan. Sie erhielten einst ein kleines Andenken. Von den Israeli. Fotos, die die Österreicher beim morgendlichen Fitneßtraining zeigten. Die Soldaten waren klar zu erkennen, ihre Namensschilder gut lesbar. Die Freude der Österreicher hielt sich ob dieses Präsents dennoch in Grenzen, denn die Israeli hatten die Bilder von ihrem Kontrollstützpunkt aus geschossen. Und dieser befand sich zehn Kilometer entfernt. Diese Geschichte hat sogar den Generaldirektor für öffentliche

Sicherheit im österreichischen Innenministerium, Michael Sika, entsetzt. »Es ist schier unglaublich, was mit heutiger Technologie alles machbar ist. Wir sind uns gar nicht bewußt, wie man uns kontrollieren kann.«

»Wenn es ein Hubble-Weltraum-Teleskop gibt, das weit ins All schauen und fremde Calaxien erforschen kann, warum soll es nicht auch Satelliten geben, die mit einem ähnlich guten Objektiv Vorgänge auf der Erde dokumentieren können.« Dieser Satz stammt von jemandem, der ständig den Weltraum im Auge hat. Prof. Walter Flury ist der Leiter der Sektion Analyse des European Space üperations Centre (ESOC) in Darmstadt. Mit Satelliten hat er immer dann zu tun, wenn es darum geht, Bahnen der europäischen Ariane-Rakete zu berechnen. Flury ist Weltraummüll-Experte und muß kollisionsfreie Flugbahnen errechnen. Denn 9000 Objekte schwirren im All umher, jedes genau dokumentiert und vom Boden aus kontrolliert. Aber nur 600 davon haben eine Funktion, der Rest ist Müll. Trümmerfragmente, Raketenteile, ausgebrannte Endstufen etc. Die 600 funktionierenden Objekte sind Satelliten, jeder von ihnen wird von der Erde aus kontrolliert und ist auch mit einem Code bezeichnet. Flury: »Man weiß, daß es ein Satellit ist, von vielen wissen wir auch, welche Aufgabe sie haben. Hinter einigen von ihnen steht aber ein großes Fragezeichen, wir kennen ihre Funktion nicht, können nur vermuten, warum sie oben sind.« Die Amerikaner und Russen lassen sich nicht in die Karten schauen.

Seit dem Ende des kalten Krieges haben die Russen und die Amerikaner aber einen Teil ihrer Aufklärungssatelliten, die früher zum Schutz des Friedens beigetragen haben, umfunktionieren müssen, man könnte es auch »privatisieren« nennen. Freilich wird die Gegenseite immer noch ausspioniert und überwacht, aber die Intensität hat abgenommen. Was machen Amerikaner und Russen mit der Technologie, die sich im All befindet? Kreisen manche Satelliten mit 25000 km/h ohne Aufgabe um die Erde? Sicher nicht, sind sich die Experten einig. Es werden und wurden bereits neue Arbeitsbereiche lukriert.



## Geheime Luftbilder auf dem freien Markt

Den Anfang machten zu Beginn der 90er Jahre die Russen, indem sie die Satellitenarchive öffneten. Ehemals geheimes Bildmaterial wurde auf den freien Markt geworfen. Eine Geldbeschaffungsaktion, um die staatlichen Finanzen aufzubessern. Die Amerikaner haben nachgezogen und auch ihre Archive geöffnel. Sie haben allerdings nur Bilder verkauft, die zehn Jahre oder älter waren. Die neueren Aufnahmen blieben unter Verschluß,

Die russischen Aufnahmen waren jedenfalls besser als ihr Ruf. Denn mit ihrer vermeintlich veralteten Technik erzielte die Sowjetunion eine Auflösung, von der sogar heutige Betreiber nur träumen können. Eine Auflösung von 1 bis zu 3 Metern mit Satelliten, deren Aufnahmesysteme auf fotografischer Basis funktionierten, sorgte für Ver- und auch für Bewunderung. Ein russischer Satellit konnte - viele von ihnen sind heute noch mit dieser Technik ausgestattet - so lange Aufnahmen machen, bis seine Filmpatrone voll war. Dann wurde diese via Fernzündung abgeworfen. Russische Techniker mußten zur Absturzstelle, meist ins offene Meer, vordringen und die Filmpatrone aus dem Wasser fischen. Auch auf der Raumstation MIR ist eine Kamera angebracht. Die Bilder werden mit den jeweiligen Shuttle-Flügen zur Erde gebracht.

Ein mysteriöser Zwischenfall im All, der bei der europäischen Weltraumorganisation ESA vertraulich behandelt wird und der internationalen Presse verheimlicht wurde, ist der »Verlust« des russischen Satelliten Kosmos 2343. Die Russen haben den in 250 Kilometer Höhe fliegenden Spion am 16. September 1997 mit Absicht durch eine Explosion zerstört, obwohl er erst einige Wochen im All war. Warum, darüber gibt es nur Mutmaßungen, denn von russischer Seite gab es keinen Kommentar zu dieser Aktion. Die Mission von Kosmos 2343 war von jeher unklar, aufgrund seiner niedrigen Flughöhe und der dadurch besseren Auflösung vermuten Insider aber, daß er ein Spionagesatellit war. Für militärische oder auch zivile Zwecke.

Die russische Mafia, so wird gemunkelt, soll bereits Satelliten nutzen, soll sogar eigene Systeme besitzen. Beweise dafür können die internationalen Geheimdienste offiziell aber noch keine liefern. Noch nicht. Aber daß Satelliten auch der Mafia wichtige Informationen

bringen können, ist naheliegend. Denn die Organisierte Kriminalität kämpft mit den gleichen Mitteln wie Exekutive und Militär.
Vor Jahren hat der US-Gcheimdienst CIA begonnen, Spionagesatelliten in den Dienst des Umweltschutzes sowie der Bekämpfung von Naturkatastrophen zu stellen. Die offizielle Begründung lautete, um politischer und sozialer Unstabilität vorzubeugen. In Nordkorea etwa werden Feuer, Vulkanausbrüchc oder der Ernteertrag genau überwacht. »Die nationalen Aufklärungssysteme können nicht nur die Panzer in der Wüste, sondern auch die Bewegung der Wüste selbst verfolgen«, sagte der damalige CIA-Chef John Deutch im Sommer 1996. In Zukunft sollen auch Private von den Geheimdienst-Technologien profitieren können. Ein anderer Grund für die bereitwillige Öffnung ist aber auch der Kostenfaktor. Spionagesatelliten, die sich in einer erdnahen Umlaufbahn befinden, haben eine Lebensdauer von einigen Jahrzehnten. Ein Durchschnittssatellit etwa, der in 600 Kilometer Höhe die Erde umkreist, hat eine Lebenszeit von 25 bis 30 Jahren. Jene also, die vor einem Jahrzehnt noch die Gegenseite ausspioniert haben, müssen zum Teil für andere, zivile Aufgaben herangezogen werden, damit die Programme finanzierbar und rentabel bleiben.

## *Schwarzarbeiter aufgepaßt!*

Wer aber glaubt, daß Satellitentechnik und Luftaufnahmen nur im großen Stil eingesetzt werden und der Privalbereich kaum davon betroffen ist, der irrt gewaltig. Satellitenaufnahmen werden schon lange nicht mehr nur von großen Unternehmen oder Konzernen geordert. Auch Private nutzen die Archive für ihre Recherchen. Wer wissen will, was sich hinter den Mauern des Nachbarn verbirgt, muß nur in das Archiv des Bundesamts für Eich- und Vermessungswesen in Wien oder in die deutschen Landesvermessungsämter gehen. Wer sich in Berlin, Hamburg oder Wien niederlassen möchte und eine Wohngegend sucht, wo es auch im Sommer erfrischend kühl bleibt und wo es viele Grünflächen und Bäume gibt, wird ebenso in diesen Archiven fündig. Wärmeaufnahmen diverser Großstädte zeigen klar, wo sich die attraktivsten Wohngegenden befinden.



Die Gemeinde Wien hat, kurz vor der Einführung der Kurzparkzonen-Regelung in der Innenstadt und den angrenzenden Bezirken, von der Luft aus einen Blick in die Innenhöfe Wiens geworfen. Ziel war es, festzustellen, in welchen Innenhöfen Autos parken und wie viele es sind. Auf den Bildern waren aber nicht nur Autos zu sehen, sondern auch Bauwerke und diverse andere Objekte, die mit der Parkpickerl-Erhebung überhaupt nichts zu tun hatten.
Bei Grenzstreitigkeiten zwischen Grundstücksbesitzern werden in Deutschland genauso wie in Österreich die elektronischen Augen zur Hilfe herangezogen -ein Luft- bzw. Satellitenbild und ein darübergelegter, digitaler Katasterplan bringen Klarheit. Beispiele dafür gibt es laufend. In den ländlichen Gegenden Bayerns, Tirols, aber auch Niederösterreichs wird noch immer ein »Spiel« gespielt, das auf den Stammtischen gerne »Grenzsteinversetzen« genannt wird. Ein Waldbesitzer versetzt den Grenzstein um wenige Meter, gewinnt dadurch aber, auf die Länge eines ganzen Waldes gesehen, Tausende Quadratmeter. Nicht selten werden deutsche und österreichische Zivilgeometer gerufen, um diese Grenzstreitigkeiten aufzuklären.
»Bald wird keine illegale Mülldeponie, kein Häuslbauer ohne Genehmigung der globalen Inspektion entgehen«, bringt es der Leiter des Instituts für Photogrammetrie und Fernerkundung an der TU Wien, Universitätsprofessor Karl Kraus, auf den Punkt. Vom All aus läßt sich klar feststellen, ob ein Haus im Grünland steht und wann es gebaut wurde. Wer heute die vorgeschriebene Bauflucht von 3 Metern mißachtet, ist überführt. Eine Luftaufnahme - entweder vom Flugzeug oder vom All aus aufgenommen - und eine darüberprojizierte Flächenmappe einer Gemeinde zeigen exakt auf, welche Gebäude sich auf verbotenen Flächen oder im Grünland befinden. »Das wird die Methode der Zukunft sein«, sagen Landvermesser, »denn Gemeinden, Landesregierungen und auch der Bund sind verpflichtet, die Einhaltung der Bauordnung zu überprüfen«. Irgendwann einmal werden Bauinspektorat oder Arbeitsmarktservice mit Hilfe von Satellitenbildern sogar feststellen können, ob ein Gebäude mit Schwarzarbeiterhilfe errichtet wurde. Voraussetzung dafür ist, daß Menschen auf den Bildern als solche zu erkennen sind. Wenn sich auf dem Rohbau eines Einfamilienhauses an einem Samstagnachmittag sieben Menschen befinden,

kann daraus geschlossen werden, daß nicht nur Familienmitglieder geholfen haben.

## Deponiekontrolle mit Zeitreisen

Mit Satellitenbildern lassen sich Zeitreisen machen. Wie sieht ein Landstrich heute aus, wie sah er vor fünf, zehn, 15 oder auch 20 Jahren aus. Was bei der Restaurierung von Landstrichen, der sogenannten ökologischen Rückgewinnung durchaus sinnvoll ist, kann aber auch eingesetzt werden, um in die Privatsphäre des Bürgers einzudringen. Öder gibt es einen Grund dafür, daß die Beamten auf den Magistraten, Landesregierungen oder Bezirkshauptmannschaften wissen müssen, daß im Garten von Herrn X ein nichtgenehmigungspflichtiges Gewächshaus errichtet wurde? Muß ein Finanzbeamter unbedingt wissen, daß sich Frau Y einen Swimmingpool gebaut hat? Er könnte plötzlich auf die Idee kommen, die Finanzierung dieses Projekts zu hinterfragen.

Wo diese Zeitreisen durchaus Sinn machen, ist die Kontrolle von Deponien. Anhand alter russischer Satcllitenaufnahmen und aktueller Aufnahmen des amerikanischen Fernerkundusngssatelliten Landsat werden im Auftrag des Umweltministeriums in Wien österreichweit Deponien kontrolliert. Zum einen kann genau festgestellt werden, um wieviel Volumen eine Deponie größer geworden ist, und zum anderen wird erhoben, wo neue, auch illegale Müllhalden entstanden sind. Das kommt aber so gut wie nie vor, da neue Deponien der heule ohnehin sehr kritischen Bevölkerung sofort auffallen. Fündig werden die Kontrollore aber dennoch, denn gängig ist die illegale Erweiterung bereits bestehender Müllhalden. Mit Hilfe von Radarsatelliten kann sogar festgestellt werden, was in den Deponien lagert.

Aktuelle Satelliten- und Luftbildaufnahmen sind heute in ganz Deutschland und Österreich erhältlich, auch via Internet werden die Satellitenbilder vertrieben. Luftbilder kosten, sofern sie in den Archiven liegen, zwischen 30 und 150 Mark, Dias zwischen 45 und 120 Mark. Gibt es das gewünschte Bild noch nicht, so kann man einen Luftbildflug bestellen. Noch unkomplizierter funktioniert es bei den Satellitenaufnahmen, diese kosten allerdings mindestens 4000 Mark. Bei den Anbietern liegen Satellitenflugpläne auf. Ähnlich wie der Zugsfahrplan. Paßt die Auflösung, so wird der Satellit vom Boden aus so programmiert, daß er gewisse Landstriche fotografiert. Deutschland und Österreich werden vom US-Satelliten Landsat beispielsweise alle 16 Tage überflogen, der französische Spot und der indische IRC-1C kommen alle 14 Tage. Sie können aber so umprogrammiert werden, daß sie alle fünf Tage Aufnahmen von den Zielgebieten in Deutschland und Österreich machen. Der Trick dabei: die Kameras an Bord können um 35 Grad ausgeschwenkt werden, so daß sie praktisch »Weitwinkelaufnahmen« machen.

In Deutschland und Österreich gibt es einige Anbieter von Satellitenmaterial. »Das Interesse ist groß«, bestätigt der Leiter von Geospace Salzburg, Dozent Lothar Beckel. Die Kundenklientel reicht von Großkonzernen über Universitäten und Vermessungsbüros bis zu Privatpersonen. »Wir fragen nicht nach, wofür sie die Aufnahmen brauchen«, so Beckel.



## Wenn Seen immer kleiner werden

Hier kennen die Beamten im österreichischen Landwirtschaftsministerium kein Pardon. Die bekanntesten Seen der Republik - vom Wörther See über den Millstättcr See bis zum Bodensee - sind öffentliches Gut, gehören also der Republik. Doch die Landkarten aus früheren Jahren haben mit der gegenwärtigen Realität schon lange nichts mehr zu tun, die Seen sind kleiner geworden, Buchten sind verschwunden, Uferlinien einige Meter weiter in Richtung See-Mitte gewandert. Aber nicht die globale Erwärmung oder der gesunkene Grundwasserspiegel sind dafür verantwortlich, sondern einige Seegrundstücksbesitzer. Manche sind zu wahren »Schüttmeistern« geworden. Haben, um ihr exklusives Grundstück zu vergrößern, einfach einige hundert bis zu tausend Kubikmeter aufgeschüttet. Mit jedem Quadratmeter Land, den sie auf diese Art und Weise dazugewonnen haben, ist gleichzeitig der Grundstückswert um bis zu 10000 Schilling gestiegen.

Mit Hilfe von Luftaufnahmen konnten die Beamten des österreichischen Bundesamts für Eich- und Vermessungswesen den Anrainern nachweisen, daß ihr Grundstück größer geworden ist. Es wurden Luftaufnahmen, die die amerikanischen Besatzer im Zweiten Weltkrieg gemacht haben, mit Luftaufnahmen verglichen, die in den vergangenen Jahren mit Flugzeugen und von Satelliten aus aufgenommen wurden.

Am Wörther See wurden 20 von 79 Anrainern überführt, am Ossiacher See sind 15 Verfahren im Laufen, am Millstätter See müssen sich sechs der 125 Seegrundstücksanrainer vor Gericht verantworten.

Viele haben selbst dem See einige Quadratmeter abgetrotzt, manche aber haben das »vergrößerte« Grundstück ohne ihr Wissen vom Vorbesitzer gekauft und sind nun mit einer Ausgabe konfrontiert, mit der sie wohl nicht gerechnet haben: Jeder Quadratmeter, um den das Grundstück vergrößert und der See verkleinert wurde, muß entweder von der Republik gepachtet oder gekauft werden. Da einige Grundstücke um 200 Quadratmeter oder noch mehr größer wurden, kommen auf die Anrainer Ausgaben in Höhe von 2 Millionen Schilling und mehr zu. Platz 1 unter den Seegrundstücks-Vergrößerern nimmt vermutlich ein Herr aus dem Salzkammergut ein: um 3500 Quadratmeter machte er im Laufe der ]ahre den Attersee kleiner.

## Satellitenbilder gegen den Briefbombentäter

»Sie hätten den Beweis liefern können«, ist ein hoher Beamter des österreichischen Innenministeriums überzeugt. Im Zuge der Fahndung nach dem österreichischen Briefbombentäter wollte man den US-Geheimdienst bzw. die US-Armee um ihre Mithilfe bitten. Konkret wollten die Fahnder bei den Amerikanern anfragen, ob sie vom 4./5. Februar 1994 Satellitenbilder vom Raum Oberwart in ihren Archiven haben.

Die Idee kam dem Beamten, nachdem er Anfang 1997 bei einem Besuch Luftaufnahmen gesehen hatte, die US-Aufklärungssatelliten von Österreich gemacht hatten: auf den Bildern waren jene 79 Stellen zu sehen, die Ende Februar 1997 als »CIA-Waffenlager« bekannt geworden sind. Die Munitionsdepots wurden vom CIA in der Besatzungszeit zwischen 1950 und 1953 angelegt. »Die Aufnahmen waren unglaublich präzise und gut in der Auflösung«, schildert der Beamte. »Als ob man von einem Heißluftballon aus mit einer guten Kamera und einem sehr guten Objektiv heruntergefotografiert hätte.« Die Amerikaner wurden nie um ihre Mithilfe gebeten. »Sie hätten uns die Bilder vermutlich ohnehin nicht zur Verfügung gestellt«, vermutet der Beamte. Aus einem einfachen Grund: Hätten die Amerikaner nämlich Satellitenaufnahmen von Österreich, wären sie sofort mit der Frage und dem Vorwurf konfrontiert gewesen, warum diese Aufnahmen überhaupt gemacht wurden und warum man in einem neutralen Staat in Europa spioniert.



## Satelliten über den Supermärkten

Wer in Österreich an einem Samstag um 11 Uhr bei Spar, Interspar, ADEG und wie die Lebensmittelmärkte sonst noch heißen, einkauft, sollte in Zukunft gegen den Himmel blicken und »bitte lächeln«. Im Sommer 1997 ließ nämlich ein Konzern die Parkplätze der Konkurrenten via Satellit fotografieren. Die Bilder, die der französische Fernerkundungssatellit Spot des Toulouser Unternehmens Spot Image geschossen hat, wurden für Marktanalysen herangezogen. Der Konzern wollte von den geparkten Autos vor den Geschäften ableiten, wie viele Kunden bei der Konkurrenz einkaufen. »Es werden auch andere Konzerne auf diese Idee kommen«, so der Wiener Ziviltechniker Harald Meixner. Denn in anderen Branchen wird die Satellitentechnologie schon lange genutzt. Deutsche Banken, die Projekte in Afrika und anderen Drittwelt-Ländern unterstützen, überprüfen anhand von Satellitenbild-Material, wie sich Vorhaben entwickeln, ob ihre Fördergelder zweckgewidmet verwendet werden. Auch Baukonzerne, die in Rußland und den Nachfolgestaalen der ehemaligen UdSSR tätig sind, kontrollieren auf Satellitenbildern Baufortschritte. »Sehr bald schon«, so Meixner, »werden sich Konkurrenten via Satellit ausspionieren. Man wird mit den Bildern beweisen können, daß etwa bestimmte Bauauflagen nicht eingehallen wurden und die Umwelt verseucht

wird.« Viele dieser elektronischen Augen im Weltraum sind auch mit Sensoren ausgestattet, die Emissionen messen können.

Abnehmer der Satellitenbildcr finden sich in allen Bereichen. Unternehmen aus den Bereichen Landwirtschaft, Wasserwirtschaft und Raumplanung nutzen das Bildmaterial bei der Projektierung von Großprojekten wie etwa Wasserkraftwerken, Stadtentwicklungen oder der Erschließung von Erdölfeldern. GSM-Telefon-Netze werden weltweit mit Satellitenaufnahmen geplant, ebenso wie Stromleitungen. Universitä're Einrichtungen sind in ihren Forschungsarbeiten auf Satellitenmaterial angewiesen. Die beiden europäischen Radarsatelliten ERS 1 und 2 überwachen die Trockenheit von Landstrichen, um Dürrcperioden vorhersagen zu können. Sie werfen ein Auge auf die Polkappen und auf Gletscher. Auch der Gesundheitszustand des Waldes wird vom All aus festgestellt. Ohne Satelliten hätte man auch das Ozonloch nicht entdeckt.

In den USA gibt es bereits Privatunternehmer die ihre eigenen Satelliten in den Orbit schießen lassen. EarthWatch nennt sich eines dieser ehrgeizigen Projekte. Earthwatch ist im Besitz von zwei der vier Lizenzen des US-Handelsministeriums für den Betrieb von kommerziellen Satelliten. Am 24. Dezember 1997 wurde EarlyBird ins All geschickt, Ende 1998, spätestens Anfang 1999 soll QuickBird folgen. Das sensationelle an diesem Satelliten ist seine Auflösung von 0,82 Metern. Die in Longmont, Colorado, ansässige Firma EarthWatch will das möglich machen, was heute nur Regisseure in Hollywood für realistisch halten - ein Auto vom All aus mit einer Kamera zu verfolgen. Im Film »Shadow Consptracy« - die »Schat-Lenregierung« mit Gharlie Sheen, Donald Sutherland und Linda Hamilton in den Hauptrollen - wird eine Verschwörung innerhalb der US-Regierung aufgedeckt und ein Attentat auf den Präsidenten verhindert. Dabei wird ein Auto zuerst vom All aus lokalisiert, indem der Satellit den Wagentyp und dann die dazupassende Nummer sucht. Als Draufgabe wird dieses Auto auch noch verfolgt.

»Das ist derzeit unmöglich«, sind sich deutsche und österreichische Fernerkundungsexperten einig, geben aber gleichzeitig zu bedenken: »Wir wissen nicht, was die Amerikaner wirklich drauf haben.« Man ist überzeugt, daß die US-Geheimdienste und das US-Militär der Zeit um mindestens zehn Jahre voraus sind. Wenn die USA 1998 also Satellitcnbilder anbietet, die eine Auflösung von einem



Meter haben, so kann man davon ausgehen, daß solche Aufnahmen bereits 1988 möglich waren. Demnach könnte auch in zehn Jahren die optische Verfolgung eines Autos durchaus realistisch sein und diese Technologie auf dem freien Markt angeboten werden. Verfolgt, sprich, lokalisiert, kann ein Fahrzeug ja auch schon heute werden, nämlich mit dem Global Positioning System.

»Voraussetzung für eine künftige optische Verfolgung wären entweder Satelliten mit einer extrem starken Auflösung, da nur von einer geostationärcn Umlaufbahn aus - also aus der Höhe von etwa 36000 Kilometern - ein Punkt auf der Erde ständig beobachtet werden könnte; diese Satelliten haben aber heute meist eine Auflösung von mehreren Kilometern«, meint Dipl.-Ing. Michael Franzen vom Bundesamt für Eich- und Vermessungswesen. Die zweite Möglichkeit ist ein dichtes Netz an Satelliten, die in einer Höhe von 600 bis 1 000 Kilometern um die Erde kreisen. Bei der Verfolgung eines Autos müßte von einer Bodenstation aus von einem auf den anderen »umgeschaltet« werden.

Das Satellitennetz wird jedenfalls immer dichter und die Technik immer mehr kommerzialisiert. Zur Jahrtausendwende will die NASA ihr Projekt LightSAR (Light Synthetic Aperture Radar) starten. Billigstsatelliten-einer kostet nur etwa eine Million Dollar-sollen mit einem Radarsystem die Oberfläche der Erde kontrollieren. Obwohl sie so billig sind, sollen diese Satelliten mit allen technischen Möglichkeiten und den besten Sensoren ausgestattet sein. Mit der Radartechnik kann auch durch Wolken und in der Nacht »fotografiert« werden.

1991/92 bekamen der Wiener Zivilingenieur Harald Meixner und seine US-Firma Vexcel von der amerikanischen Defence Mapping Agency (DMA) einen »heißen« Auftrag. Mit dem sogenannten Aero-Laser-Scanner wurde das Dreieck um den Amazonas Kolumbien/Peru/Brasilien aufgenommen. Mit dem Scanner kann man auch durch Bäume durchfotografieren, Gebäude erfassen, schlichtweg Bauwerke erkennen - von der Landebahn bis zum Labor. Was die Vermessungstechniker entdeckt haben, erfuhr er wenig später: Drogenlabors eines in den USA gesuchten Drogenbarons. Wie »heiß« der Auftrag wirklich war, wurde Meixner aber erst ein halbes Jahr später bewußt, als das Flugzeug einer Konkurrenzfirma in diesem Dreieck abgeschossen wurde.

# Datenschützer contra Datenjäger

**> Warum auch Politiker gegen das Datenschutzgesetz verstoßen.**

**> Wie oft in deutschen Unternehmen das Datenschutz* gesetz gebrochen wird.**

**> Warum es so selten zu einer Verurteilung kommt.**

**> Wie der Bürger seine Privatsphäre verliert.**

**> Was die neue EU-Richtlinie bringt.**

## Wenn Geheimes öffentlich wird

Wie kommen Journalisten zu heiklen und gleichzeitig »geheimen« Informationen - zu Prozeßunterlagen, *zu* Abhörprotokollen, zu Berichten des Rechnungshofes oder Bundesverfassungsgerichtshofes? Das Wort »Datenschutz« ist wohl eines jener Worte, das in Deutschland und Österreich des öfteren in den Mund genommen wird. Aber in beiden Ländern wird das Datenschutzgesetz ständig gebrochen. Von privaten Stellen genauso wie von Behörden. Und nicht nur von Journalisten oder Privatdetektiven, sondern vor allem von Juristen, Kriminalisten, Ministerialbeamten und Politikern, die diese Informationen weitergeben.

Was gewisse Politiker vom Datenschutz halten, hat die Affäre um den »Datenklau« in der Salzburger Landesregierung gezeigt. Am 24. September 1997 waren während eines Computer-Virenchecks im Großrechner der Landesregierung für eineinhalb Stunden sämtliche Dokumente aus dem Computersystem des SP-Landesrates Gerhard Buchleitner für all jene Personen zugängig, die am selben Rechnersystem angeschlossen waren. Diese »Lücke« nützte der FP-Landesrat Karl Schnell, der zwei seiner Mitarbeiter auftrug, Dokumente zu kopieren. Was ihm in die Hände fiel, war eine »Postenschacherliste« - auf dieser war dokumentiert, wer für welchen Posten in der Salzburger Landesregierung vorgesehen ist.

Der Salzburger Datenklau ist aus mehreren Gründen ein Paradefall. Zum einen war es ein Politiker, der gegen das Datenschutzgesetz verstoßen hat. Also einer derjenigen, von denen man annehmen muß, daß er sich als demokratisch gewählter Volksvertreter an Gesetze hält. Zum anderen hat dieser Politiker veranlaßt, daß diese widerrechtlich erworbene Liste mit personenbezogenen Daten via Zeitungsinserate und Internet einer breiteren Öffentlichkeit zugängig gemacht wird. Und schließlich hat der Parteivorsitzende der FP, Jörg Haider, nicht den Gesetzesbruch kritisiert, sondern jene, die diesen Datenschutzverstoß kritisiert haben.

FP-Landesrat Schnell mußte zwar den Hut nehmen, daß der »Datenklau« aber gar nicht leicht bestraft werden kann, hat die »Presse« (13. 11. 1997) dokumentiert. Denn sogar Strafrechtsexperten waren sich uneinig, nach welchen Gesetzesparagrafen der Politiker und seine Mitarbeiter belangt werden könnten.

Für den Innsbrucker Strafrechtsexperten Klaus Schwaighofer wurde dadurch ganz klar das Amtsgeheimnis verletzt. »Die Voraussetzungen des § 310 StGB, daß ein Beamter ein ihm ausschließlich kraft seines Amtes zugänglich gewordenes Geheimnis offenbart und dadurch ein berechtigtes privates Interesse verletzt, seien gegeben.« Der Wiener Universitätsprofessor Frank Höpfel schätzte in der »Presse« den Fall anders ein, der § 310 StGB schied für ihn aus, weil den geklauten Dokumenten der amtliche Charakter fehlte. Schnell und seine Mitarbeiter könnten nach § 49 des österreichischen Datenschutzgesetzes belangt werden, indem es um die widerrechtliche Verschaffung von automationsgestützten Daten geht.

Was dieses Beispiel dokumentiert, ist, daß man trotz aller Gesetze nicht davon ausgehen kann, daß Daten geschützt werden und daß jene, die sich illegal Daten besorgen, auch dafür zur Verantwortung gezogen werden. Datenschutzverstöße gelten eigentlich als Kavaliersdelikt.

## Bundesbeauftragter und Datenschutzrat

Das deutsche und österreichische System sind sich ähnlich. Ist es in Deutschland der Bundesbeauftragte für den Datenschutz, so ist in Österreich die Dalenschutzkommission im Bundeskanzleramt für Beschwerden gegen staatliche Behörden und öffentliche Stellen zustandig. In Deutschland ist der Datenschutz durch die einzelnen Landesbeauftragten sehr gut vertreten, die auch die Beschwerden über private Unternehmen annehmen. Sie kontrollieren die Einhaltung der Landesgesetze (jedes der 16 Bundesländer hat sein eigenes Datenschutzgesetz).

Der deutschen Bevölkerung sind persönliche Daten noch heilig. Gemäß einer Umfrage, die Bundesdatenschützer Joachim Jacob in seinem Jahresbericht 1995/96 zitiert, steht auf einer Skala von Bedrohungen, vor denen sich die Deutschen am ehesten fürchten, an erster Stelle und mit deutlichem Abstand die Befürchtung, daß die eigenen Daten zu Werbezwecken mißbraucht werden. Erst danach wurden in der Befragung Ängste genannt, wie etwa Opfer einer Straftat zu werden oder im Straßenverkehr zu verunglücken.

In Österreich sind die Datenschutzagenden zwar im Bundeskanzleramt in Wien zentralisiert, aber nicht so effektiv und ausgeprägt wie in Deutschland. Das hat weniger mit der Arbeit der zuständigen Beamten zu tun als mit dem Bewußtsein der Bevölkerung. Neben der Datenschutzkommission gibt es in Österreich den Datenschutzrat, der mit der Rolle des Bundesbeauftragten in Deutschland verglichen werden kann. Der Datenschutzrat ist ein rechtspolitisches Organ, das für neue Entwicklungen zuständig ist und neue Gesetzesvorschläge erarbeitet. Der Datenschutzrat kann aber nur gutachterliche Stellungnahmen abgeben.

Wie oft in Deutschland und Österreich gegen das Datenschutzgesetz verstoßen wird, darüber gibt es kaum statistisches Material, Der Bundesbeauftragte für den Datenschutz in Bonn, Joachim Jacob, erhält pro Jahr im Durchschnitt 4000 Beschwerden und Anfragen, die sich um das Persönlichkeitsrecht drehen. Mit der gleichen Anzahl an Anfragen ist auch jeder der 16 Landesdatenschützer konfrontiert, was in Summe in Deutschland etwa 60000 Anfragen pro Jahr ausmacht.



Wie oft es im privaten Bereich, sprich bei privatwirtschaftlich geführten Unternehmen zu Datenschutzverstößen kommt, darüber gibt es nur sehr vage Schätzungen.

In der Studie »Datenschutz in Deutschland«, die die Bonner Gesellschaft für Datenschutz und Datensicherung (GDD) gemeinsam mit der Herweg & Müthlein IT-Management GmbH und der Fachzeitschrift »IT-Sicherheit« 1996 durchgeführt hat, kommen erschreckende Defizite beim Datenschutz zutage. »Mehr als die Hälfte aller Datenschutzbeauftragten bzw. Datenschutzverantwortlichen beurteilten das Datenschutzniveau in den Unternehmen, Institutionen und Behörden als teilweise oder sogar generell verbesserungsbedürftig«, kamen die Studienersteller zum Schluß. Beinahe in jedem zweiten Unternehmen wurde schon einmal gegen Datenschutzvorschriften verstoßen. Vor allem in den kleinen und mittleren Unternehmen sei die Umsetzung der Datenschutzgesetze problematisch. Einen »Sonderfall« bildeten die Banken und Versicherungen. »Hier steht die Geschäftsführung dem Datenschutz häufig negativ gegenüber«, wird die landläufige Meinung der Bevölkerung in der Studie bestätigt.

Von den mehr als 1 000 befragten Unternehmen gaben 64 Prozent an, daß ihre Institution bei der zuständigen Datenschutzaufsichtsbehörde gemeldet ist, aber von dieser noch nie geprüft wurde. Die erschreckenden Defizite führen die Studienersteller auf die mangelnde Sensibilisierung der Abteilungsleiter und der Mitarbeiter zurück. Außerdem werde den Datenschutzbeauftragten zu wenig Zeit für ihre Aufgaben zur Verfügung gestellt.

Konkrete Zahlen werden in der Kriminalstatistik des deutschen Innenministeriums geliefert. 1996 kam es zu 9.33 Fällen von »Ausspähen von Daten«, 228 Fälle von »Datenveränderung« und »Computersabotage«. In welchen dieser Fälle tatsächlich auch gegen das Datenschutzgesetz verstoßen wurde, läßt sich nicht exakt klären.

In Österreich langen bei der Datenschutzkommission im Bundeskanzleramt jährlich zwischen 100 und 150 Beschwerden ein. Das aber betrifft nur staatliche Stellen, bei Verstößen privater Unternehmen sind die Verwaltungsbehörden und die Gerichte zuständig.

Wie ernst das Datenschutzgcsetz wirklich genommen wird bzw. welche Chancen sich der Private bei einer Klage ausrechnet, zeigt

die Statistik der gerichtlichen Verurteilungen. Ganze vier Prozesse wurden seit 1990 geführt, 1990 und 1993 je einer, 1994 zwei. Alle endeten mit einer Verurteilung.

## Der Zugang zur Intimsphäre

»Das größte Problem beim Datenschutz ist die Einstellung der Menschen«, meint Hans Zeger von der ARGE Daten, der Österreichischen Gesellschaft für Datenschutz. »Viele meinen, sie hätten ohnehin nichts zu verbergen. Aber es geht nicht darum, ob man etwas zu verbergen hat oder nicht. Es geht darum, daß durch die diversen Datensammlungen Behörden und private Institutionen Zugang in unsere Intimsphäre haben. Gegen Datenschutzverstöße muß man deshalb eintreten, weil sie Eingriffe in unsere Privatsphäre sind.«

Was aber ist diese Privatsphäre?

Für viele Bürger sind die Begriffe Rasterfahndung, Lauschangriff etwas völlig Abstraktes, das sie mit der eigenen Privatsphäre gar nicht in Verbindung bringen. Aber wenn gewisse Informationen, Details oder Lebensgewohnheiten in die Öffentlichkeit dringen, kann das mitunter sehr peinlich sein.

»Da immer mehr Daten gesammelt werden, kommt es de facto zu einer systematischen Auflösung der Privatsphäre«, hat Hans Zeger in seinem Buch »Datenschutz in Österreich« geschrieben. Durch das Datenschutzgesetz soll erreicht werden, daß »nur wirklich benötigte Daten der Verwaltung, einem Unternehmen etc. bekanntgegeben werden müssen«. Für Zeger ist »Datenschutz« ein recht diffuser Begriff. »Wer oder was soll geschützt werden? Die Bürger vor den Daten, die Daten vor den Bürgern, der Datenabeiter vor Hackern und lastigen Konkurrenten?«

Grundsätzlich ist der Staat für den Datenschutz verantwortlich, aber der Bürger sollte seine Daten selbst schützen. Der beste Datenschutz ist Datenvermeidung. Das ist in der gegenwärtigen Zeit, in der jeder kleinste Betrieb Informationen auf Computer speichert, leichter gesagt, als getan.

Der Problematik von EDV war man sich bereits Ende der 70er Jahre



bewußt. 1977 wurde ein deutsches Bundesdatenschutzgesetz geschaffen, drei ]ahre später, am 1. Januar 1980, trat das österreichische Datenschutzgesetz in Kraft. Dieses beinhaltete das »Grundrecht auf Datenschutz«, daß »jedermann Anspruch auf Geheimhaltung der ihn betreffenden personenhezogenen Daten [hat], soweit er daran ein schutzwürdiges Interesse, insbesondere im Hinblick auf Achtung seines Privat- und Familienlebens, hat.« Grundsätzlich werden gemäß Datenschutzgesetz, so schreibt Zeger in seinem Buch, vier Bereiche geregelt.

Den höchsten Stellenwert hat das Datengeheimnis. Niemand erhält unbefugt Auskunft.

Gemäß dem österreichischen Beamtencharakter »Vorschrift ist Vorschrift« wurde auch eine Registrierungspflicht eingeführt. Jede Behörde, jeder Betrieb ist verpflichtet, seine Datensammlung dem Datenverarbeitungsregister zu melden.

Vorgeschrieben ist weiters eine Datensicherheit. Der Betreiber von EDV-Anlagen muß gewährleisten, daß kein Unbefugter seine Systeme knackt und personenbezogene Informationen absaugt.

Vorgesehen ist im österreichischen Datenschutzgesetz auch ein Auskunftsrecht. Jeder Bürger muß Auskunft darüber erhalten, wer über ihn Daten sammelt und verarbeitet.

Dieses Recht kann mitunter auch eigenwillig definiert werden, wie der Fall der Stapo-Akten zeigt. Anfang der 90er Jahre wurde bekannt, daß die österreichische Staatspolizei Akten über die Österreicher angelegt hatte. Der Aufregung folgte das Einsehen. Jeder Österreicher durfte ans Innenministerium schreiben und die Herausgabe der Informationen fordern. Die Schreiben, die retour kamen, waren für manche erleichternd - »wir haben keine auskunftspflichtigen Daten über Sie gespeichert«, so der Wortlaut. »Aber erwiesen ist durch dieses Schreiben nichts«, meint ein Betroffener, der aus »berechtigten« Gründen davon überzeugt war, daß »mehr« über ihn gespeichert ist. Seine Frage, auf die er wohl nie eine Antwort erhalten wird: »Was ist mit den >nichtauskunftspflichtigen< Daten?«

## Was die EU-Richtlinie bringt

Das deutsche und das österreichische Datenschutzgesetz sind Auslaufmodelle, denn die bereits im Oktober 1995 von den EU-Gremien beschlossene EU-Richtlinie soll bis 24. Oktober 1998 von den EU-Mitgliedsstaaten in nationales Recht umgewandelt werden. Die EU-Richtlinie ist in manchen Bereichen besser, in manchen Bereichen aber auch schlechter als die beiden Datenschutzgesetze, sind sich deutsche und österreichische Experten einig. Da Deutschland und Österreich die EU-Richtlinie nach eigenen Vorstellungen umsetzen können, bleiben im wesentlichen aber die strengeren nationalen Punkte in der EU-Richtlinie erhalten. »Manche der deutschen Datenschutzvorschriften sind zu wesentlichen Teilen in die europäische Datenschutzrichtlinie eingeflossen«, bestätigt Bundesdatenschützer Joachim Jacob. »Sie haben damit Vorbildcharakter und sind zu einem Exportmodell geworden.« Im Gegensatz dazu hatte Österreich bei der Formulierung der EU-Richtlinie kein Mitspracherecht, da Österreich zum Zeitpunkt der Gestaltung nur einen ßeobachterstatus hatte.

Wie wichtig ein einheitliches europäisches Datenschutzgesetz ist, beweist die Tatsache, daß Griechenland und Italien überhaupt kein diesbezügliches Gesetz hatten, Portugal, Belgien und Spanien haben erst seit Anfang der 90er Jahre Datenschutzgesetze. Mit Inkrafttreten darf der internationale Datenaustausch nur auf Basis der EU-Richtlinie passieren. Das gilt indirekt auch für außereuropäische Länder. In Staaten, in denen es kein vergleichbares Gesetz gibt, dürfen keine Daten von EU-Bürgern verschickt bzw. verarbeitet werden.

Die EU-Richtlinie bringt im groben zwei Änderungen, wobei Deutschland die Punkte bereits seit Jahren in seinem Gesetz erfüllt. In Zukunft gibt es ein sogenanntes aktives Informationsrecht. Bis Oktober 1990 darf sich ein Bürger informieren, wer über ihn Daten verarbeitet. Nach der Umsetzung in nationales Recht muß jedes Unternehmen, aber auch jede Behörde, die eine Datenverarbeitung beginnt, den Betroffenen aktiv informieren, daß seine Daten in dessen Datenverarbeitungssystem gespeichert sind. Eine schwammige Angelegenheit, die in einigen Bereichen wohl kaum in die Realität umgesetzt werden kann. Wenn staatliche Behörden erheben, wird dieses Recht mit hoher Wahrscheinlichkeit beachtet. Wer eine Einkommenserklärung ausfüllt oder einen statistischen Fragebogen beantwortet, macht dies im Bewußtsein, daß seine Daten gespeichert und weiterverarbeitet werden.



Anders hingegen ist es bei privaten Organisationen wie etwa Adreßhändlern. Jeder Adreßhändler müßte, bevor er Name und Adressen an Dritte weitergibt, den Betroffenen anschreiben und ihn darüber informieren.

»Das kann bestenfalls als Theorie bezeichnet werden«, ist auch die Leiterin der Datenschutzkommission im Bundeskanzleramt in Wien, Ministerialrätin Waltraut Kotschy, überzeugt- »Der Adreßverlag kann leicht behaupten, einen Brief an den Betroffenen abgeschickt zu haben. Der Bürger hat keine Möglichkeit zu beweisen, daß er keinen erhalten hat.« Hinzu kommt auch noch das Kostenproblcm. Wenn man davon ausgeht, daß ein Unternehmen bei einem Adressenhändler etwa 100000 Adressen bestellt, so müßten 100000 Bürger informiert werden. Welcher Adreßhändler zahlt freiwillig das Porto für 100000 Briefe?

In der EU-Richtlinie gibt es zudem unzählige Ausnahmen. In zahlreichen Fällen dürfen die Daten weitergegeben werden, ohne Betroffene zu informieren. Etwa wenn Unternehmer den Finanzämtern Daten über Kunden übermitteln müssen etc.

Freilich gibt es auch für einige staatliche Stellen eine Ausnahme in der EU-Richtlinie. Wenn die innere Sicherheit eines Landes betroffen ist, gilt die EU-Richtlinie nicht. Terrorfahnder und Kriminalisten dürfen dann agieren, ohne die EU-Richtlinie einhalten zu müssen.

Die zweite Neuerung betrifft das Klagsrecht von Privaten. Wer künftig eine Klage gegen jemanden einbringt, der seiner Meinung nach illegal Daten verarbeitet oder personenbezogene Daten mißbraucht, hat künftig bessere Chancen. Laut EU-Richtlinie muß es in jedem EU-Staat eine oder sogar mehrere Stellen geben, die das Recht haben, private Datenverarbeitungen zu kontrollieren, sprich: eine Art Datenverarbeitungspolizei. In Deutschland wird diese Funktion ohnehin schon seit Jahren vom Bundesbeauftragten und den Landesbeauftragten für den Datenschutz bzw. von den jeweiligen obersten Aufsichtsbehörden wie etwa den Innenministerien erfüllt. In Österreich ist dafür künftig eine Abteilung im

Bundeskanzleramt oder eine Institution wie etwa die Österreichische Gesellschaft für Datenschutz zuständig.

Für den deutschen Bundesdatenschützer Jacob sind derartige Änderungen aber zu wenig, er fordert gleichzeitig mit der Umsetzung der EU-Richtlinie eine umfassende Novellierung des Bundesdatenschutzgesetzes. »Es muß einer von Multimedia, Internet und Chipkarten geprägten Zukunft gerecht werden«, so Jacob.

# Der Autor

## Datenbank-Register Gerald Reischl

Krankenhaus Neunkirchen/Ceburtenregister
Pfarre Neunkirchen/Taufregister
Neunkirchen/Geburtenbuch
Neunkirchen/Meldeamt
Neunkirchen/Kindergartenregister
Neunkirchen/Volksschuldatei
Schuldatenbank Seminar Sachsenbrunn
Musikhochschule Wien
Universität Wicn/Immatrikulationsdatei
Universität Wien/Publizistikinstitut
Universität Wien/Institut für Theaterwissenschaft
Universität Wien/Sponsionsdatei
Ministerium für Justiz/Personalinformationssystem
»Niederösterreichische Nachrichten«/Freie-Mitarbeiter-Datei
ORF/Freie-Mitarbeiter-Dalenbank
»Presse«/Mitarbeiterdatei
»Kurier«/Mitarbeiterdatei
Ergänzungsabteilung Militärkommando Niederösterreich
Wehrdienstdatei Landwehrstammregiment 37 Wiener Neustadt
Bezirkshauptmannschaft/Reiscpaßregister
Bezirkshauptmannschaft/Verwaltungsstrafregister
Bezirkshauptmannschaft/Kfz-Zulassungsstelle
Rotes Kreuz/Blutspende-Datenbank
PADI-Taucherlizenz
Brockhaus/Kundendatei
Mobilkom Austria/Kundendatei
Post und Telekom Austria/Kundendatei
Telefonbuch, Herold Telefon-CD
Zentralmeldeamt Wien
Finanzkammer der Erzdiözese Wien

Magistrat der Stadt Wicn/Organstrafverfügung-Datenbank (Kurzparkzonen-Abgabe)
Gemeinde N.-L/Grundsteuer-Datenbank
EVN/Kundendatei (Wohnung Neunkirchen)
EVN/Kundendatei (Grundstück N.-L.)
Wiener Stadtwerke/Kundendatei
Grundbuch
Finanzamt/Datenbank für Gebühren und Verkehrsteuern
Finanzamt Neunkirchen/Einkommensteuernummer
Öffentlicher Notar Dr. Richard Grubmayr Neunkirchen/Kundendatei
Interunfall/Kundendatei Haushaltversicherung
Interunfall/Kfz-Versicherung
Hausverwaltung Friedrich & Padelek GesrnbH/Mieterdatei
Sport Eybl/Kundendatei
Porsche Oberlaa/Kundendatei
Porsche Bank AG - Versicherungs AG/Kundendatei
Anker/Datei Ex-Versicherungskunden Kfz
Anker/Unfallversicherungsdatei
Anker/Krankenversicherungsregister
ÖAMTC/Mitglieder-Datenbank
ÖAMTC/Schutzbrief-Datenbank
Elektro-Köck/Kundendatei
Institut für Markt- und Sozialanalysen IMAS
AUA/Vielfliegerprogramm Qualiflyer
Lufthansa/Vielfliegerprogramm Miles&More
Press-Club Hertz International
Zeitungsherausgeberverband/Journalisten-Datenbank
Verkehrsamt Wien/Führerscheinregister
Die Erste Bank/Kundenkartei
Eurocard/Kundendatenbank
Visa/Kundendatenbank
Eurocheque-Card/Abrechungsregister Europay Austria
Kurtheater Reichenau/Mitgliederdatei
Bundestheater/Programmregister
Baumarkt Schilowsky/Kundendatei
Ikea/Family-Card
Michelfeil/Kundendatci



Elite-Möbel/Kundendatei
Möbel Lechncr Gloggnitz/Kundendatei
Nico/Kundenkartei
Kika/Kundendatei
Wein & Co. /Kundendatei
Actual-Fenster/Kundendatei
Packard Bell/Kundenrcgister
Netway-Provider/Internetuser-Datei
Genios-Datenbank/Kundenregisler
Hauptverband der Sozialversichcrungsträger
Wiener Gebietskrankenkasse
Niederösterreichische Gebietskrankenkasse
Stadibauamt Neunkirchen/Einreichplan-Register
S-Bausparkasse/ßausparer-Rcgister
Österreichische Beamtenversicherung/Kundendatei
Krankenhaus der Barmherzigen Brüder/Patienteninformationssystem
Krankenhaus der Stadt Neunkirchen/Patienteninformationssystem
Unfallkrankcnhaus Meidling/Patienteninformationssystem
Krankenhaus Wiener Neustadt/Patienteninformationssystem
Institut für Sonnen- und Tropenmedizin/Patientendatei
Zahnarzt Dr. Graf-Müller/Patientendatei
Hausarzt Dr. Nertit/Patientendatei

Nicht näher aufgeschlüsselt:
Diverse journalisten-Vertei(erlisten
Divejse Visa-Datenbanken (Auslandsreisen)

# Quellen und Literatur

## Zeitungen/Magazine


ADAC motorweit
AUSTRIA PRESSE AGENTUR
AUTOTOURING
BASLERZEITUNG
BUNTE
COMPUTER UND RECHT. Köln 1995
COMPUTERWELT
DEUTSCHE GERICHTSVOLLZIEHER ZEITUNG
DIE PRESSE
DER SPIEGEL
DER STANDARD
DIE WELT
FOCUS
FRANKFURTER ALLGEMEINE ZEITUNG (FAZ)
GEOGRAPHIE UND SCHULE
GIM International Geomatic Info Magazine
IT-SICHERHEIT
KRIMINALISTIK
KURIER
NATUR E
NEUE JURISTISCHE WOCHENSCHAU
NEWS
NEW YORK TIMES
OBERÖSTERREICHISCHE NACHRICHTEN
ÖFFENTLICHE SICHERHEIT
**PC INTERN**
PRAKTIKER
PROFIL
RECHT DER DATENVERARBEITUNG
SALZBURGER NACHRICHTEN
STERN
THE SAS SYSTEM IOURNAL
TIME

TORONTO STAR
TRAFFIC TECHNOLOGY INTERNATIONAL
VERKEHRSNACHRICHTEN
WIRTSCHAFTSBLATT
WIRTSCHAFTSWOCHE

### TV

ARD »Ratgeber Technik«
ARD »Wiso«
ORF »ZiB 2«

## Literatur

ARGE DATEN: Datenschutz & Informalionsrecht (Nr. 4/95), Richtlinien 95/46/EG des europäischen Parlaments und des Rates, kommentiert.

BÖTTGER, ANDRFAS/PFEIFFER, CHRISTIAN: Der Lauschansriff in den USA und in Deutschland. In: ZRP 1994, Heft 1 .

BERUFSVERBAND GEPRÜFTER GRAPHOLOGEN/PSYCHOLOGEN: Schriftpsychologie, die unbekannte Wissenschaft. München 1997.

BONDER, MICHAEL/STUDENT, THOMAS: Wem gehört was in Europa? Die 100 größten Konzerne. Düsseldorf/München 1996.

BUNDESMINISTERIUM FÜR JUSTIZ (Ö): Organisierte Kriminalität - Professionelle Ermittlungsarbeit- Neue Herausforderung. Wien 1996.

BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: IT-Sicherheit: Heute und in der Zukunft - Der Beitrag des BSI.

BUNDESKRIMINALAMTGESETZ (BKAG): Juli 1997.

BUNDESMINISTERIUM FÜR GESUNDHEIT: Das Transplantationsgesetz. Bonn 1997.

BUNDESMINISTFRIUM FÜR GESUNDHEIT UND KONSUMENTEN-SCHUTZ: Verbraucher im Netz. Wien 1997.

BUNDESMINISTERIUM FÜR JUSTIZ: Bundcsgesetz über »besondere Ermittlungsmaßnahmen«, Text, Materialien. Wien 1997.

BUNDESMINISTERIUM FÜR VERKEHR: Der neue EU-Führerschein und die neue Punkteregelung. Bonn 1997.



BUNDESMINISTERIUM FÜR VFRKEHR: Verkehrstelematik, Fragen und Antworten. Bonn 1996.

DAS BUNDESKRIMINALAMT: Wiesbaden 1995.

DATENSCHUTZBERICHT 1995: Wien 1996.

DATENSCHUTZGESETZ ÖSTERREICH: Wien 1993.

DER BUNDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ: Tätigkeits-bericht 1995-1996. Bonn 1997.

DER BUNDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ: Bundesdaten-schutzgesetz -Text und Erläuterung. Bonn 1996.

DER FISCHER WELTALMANACH 1997. Frankfurt 1997.

DEUTSCHE AKADEMIE FÜR VERKEHRSWISSENSCHAFT: 33. Deutscher Verkehrsgerichtstag 1995.

DIRECT MARKETING VERBAND ÖSTERREICH: Adressen und Direkt-Marketing. Ein Leitfaden. Wien 1997.

ESA: Bulletin Nummer 91 , Noordwijk 1997.

EUROPÄISCHE KOMMISSION: Schutz der finanziellen Interessen der Gemeinschaft, Betrugsbckämpfung, Jahresbericht 1996.

FINK, MANFRED: Lauschziel Wirtschaft. Berlin 1995.

GEOSPACE: Österreich - ein Porträt in Luft- und Satellitenbildern, Salz-burg 1996.

GESELLSCHAFT FÜR ZAHLUNGSSYSTEME MBH: Geschäftsbericht 1996.

GRABAU, RUDOLF: Technische Aulklärung. Stuttgart 1989.

HAUPTVFRBAND DER ÖSTERREICHISCHEN SOZIALVERSICHERUNGS-TRÄGER: Handbuch der österreichischen Sozialversicherung 1997.

HERLES, WOLFGANG: Die Machtspieler. Düsseldorf/München 1998.

INTERNATIONAL ACADEMY OF ASTRONAUTS (IAA): Position Paper on Orbital Debris. Paris 1995.

JAMES SPACE DIRECTORY 1996.

LEIBERICl l, PETER (Hg.): Business Mapping im Marketing. Heidelberg 1997.

LEUTHARDT, BEAT: Leben Online. Hamburg 1996.

NENTWICH/PEISSL/PISJAK: Konsumentenkartcn. Verbraucherrecht, Ver-braucherpolitik. Wien 1993.

ORWELL, GEORGE: 1984. Frankfurt/Berlin 1996.

ÜAMTC AKADEMIE: Der Steinzeitjäger im Straßenkreuzer. Auszüge aus der Dissertation von Dr. Klaus Atzwanger zum Thema »Aggression auf der Autobahn«. Wien 1995.

ÖSTERREICHISCHE AKADEMIE DER WISSENSCHAFTEN: Das digitale Krankenhaus. Wien 1997.

PICHLER, WOLFGANG: Certification Authority im Internet, Diplomarbeit an der TU-Wien. Wien 1997.

PRESSE- UND INFORMATIONSAMT DER BUNDESREGIERUNG: Polizeiliche Kriminalstatistik für das Jahr 1996.

RELIN, AXEL: Kontrolle flächengestützter Beihilfen in der Landwirtschaft durch Satellitenfernerkundung. In: Schriftenreihe der Zentralstelle für Agrardokumentation und -information (ZADI), Band 8, Bonn 1996.

SAS INSTITUTE INC. ANNUAL REPORT 1996.

SCHOBER, KLAUS: Die neue Dimension im Direktmarketing, Market-Universe-Database. Düsseldorf/München 1997.

SIEBRECHT, MICHAEL: Rasterfahndung. Berlin 1997.

TELEKOMMUNIKATIONSGESETZ TKG (D): Juli 1996.

TELEKOMMUNIKATIONSGESETZ (Ü): August 1997.

THEORIE UND PRAXIS DER WIRTSCHAFTSINFORMATIK: Data Warehouse (Heft 195). Heidelberg 1997.

THEORIE UND PRAXIS DER WIRTSCHAFTSINFORMATIK: Database Marketing (Heft 193). Heidelberg 1997.

TÜV RHEINLAND: Feldversuch »Autobahntechnologien A 555« - Ergebnisse und Vorschläge. 1995.

ULFKOTTE, Udo: Verschlußsache BND. München/Berlin 1997.

UNIVERSITÄTSKLINIK FÜR ANÄSTHESIE UND ALLGEMEINE INTENSIVMEDIZIN AKH: Leistungsbericht.

VEREIN FÜR KONSUMENTENINFORMATION: Projektbericht: Erhebung zum Mißbrauchsrisiko bei Telebanking im Einzugsermächligungsverfahren. Wien 1996.

WANNER, STEPHAN: Die negative Raslerfahndung. München 1985.

ZEGER, HANS: Datenschulz in Österreich. Wien 1991.

# Dank

Generaldirektor für öffentliche Sicherheit Mag. Michael Sika, Bundesbeauftragter für den Datenschutz Dr. Joachim Jacob, Trend- uncl Zukunftsforscher Matthias Horx, Ing. Dieter Göschler vom Institut für Datenschutz und Informationssicherheit, BSI-Pressesprccher Michael Dickopf, Dr. Dirk Hager vom Referat Technische Risiko-Analyse und Abwehr im BSI, Dr. Manfred Hochmeister vom Institut für Rechtsmedizin der Universität Bern, Mag. Dr. Walter Peissl vom Institut für Technikfolgen-Abschätzung in der Akademie der Wissenschaften, Leiter der Abteilung VII/B/7 im Bundeskanzleramt Dr. Hans Peter Lehofer, Universitätsprofessor Dr. Reinhard Posch, Leiter der Abteilung Verkehr und Konsumentenschutz im ÖAMTC Dr. Karl Obermair, ÖAMTC-Experte Harald Dirnbacher, Ministerialrat Dr. Werner Schmidt vom Büro des Bundesbeauftragten für den Datenschutz (BfD), BfD-Pressesprecherin Helga Schumacher, Oberst Franz Kößler vom Büro für EKF in Wien, Arthur-D.-Little-Geschäftsführer Dr. Manfred J. Kunze, Prof. Dr. Dipl.-Ing. Manfred Rausch, DeTeMobil-Presscsprecher Stefan Wichmann, Dipl.-Ing. Hanns H. Schubert, ARGE-Daten-Chef Dr. Hans Zeger, Bundesamt für Eich- und Vermessungswesen Dipl.-Ing. Michael Franzen, SAS-Institutc-Geschäflsführer Mag. Gerhard Graf, Klaus Pokorny, leitender Staatsanwalt Mag. Christian Pilnacek, meine Kollegin Birgit Braunrath-Tarta'rolti, Kurier-Herausgeber und Chefredakteur Peter Rabl, Kuräer-Sonntag-Chefredakteur Herbert Gärtner, Fotograf Franco Garzarolli, »Computerdoktor« Fritz Hilbert, Formel-1-Pilot Alexander Würz, meine Mutter Christine Reischl und alle Informanten und Gesprächspartner, die ungenannt bleiben wollen.

Der Autor freut sich über Anregungen, persönliche Erfahrungen mit »Datenjägern« und Hinweise. Bitte entweder schriftlich an Mag. Gerald Reischl, Postfach 19, A-2620 Neunkirchen oder E-Mail greischl@netway.at. Alle Briefe und elektronischen Postkarten werden vertraulich behandelt.

»Alle reden vom ›global village‹. Dieses globale Dorf ist aber keine Idylle, sondern ein kompliziertes und teilweise auch riskantes Netzwerk für Menschen, Unternehmen und Staaten. Dieses Buch hilft, es zu verstehen.«

Joachim Jacob, Bundesbeauftragter
für den Datenschutz in Deutschland

»Dieses Buch führt dem Leser eindrucksvoll vor Augen, wie ›durchsichtig‹ der Mensch geworden ist. In welchem Maß und mit welchen Techniken seine Intimsphäre offengelegt werden kann. Der Autor zeichnet ein beklemmendes Szenario, das nachdenklich stimmt. Ein wichtiges Buch an der Schwelle zum nächsten Jahrtausend!«

Mag. Michael Sika, Generaldirektor für die
öffentliche Sicherheit in Österreich

»Es besteht kein Zweifel, daß der Einsatz modernster Technologien der Schlüssel zur Bewältigung unserer unmittelbaren Zukunft ist. Der Autor liefert jedoch einen wichtigen Hinweis, daß der Preis dafür nicht die totale Aufgabe des Persönlichkeitsschutzes sein darf.«

Matthias Horx, Trendforscher