

Quarks & Co

SCRIPT ZUR WDR-SENDEREIHE „QUARKS & CO“

**BIG BROTHER IS
WATCHING**



Big Brother is watching

Inhalt

Datenspuren	4
Scoring – sind Sie kreditwürdig?	8
Data-Mining – Lesen in der Datenflut	10
Bedrohte Freiheitsrechte in den USA	13
Überwachungskamera	16
RFID – Identifizierung per Funk	19
Biometrie	21
Lesetipp	23
Linktipps	24

Impressum

Text:

Axel Bach,
Tristan Chrytroschek,
Daniel Münter,
Silke Übelstädt

Redaktion und Koordination: Monika Grebe

Copyright: WDR Juli 2004

Weitere Informationen erhalten sie unter: www.quarks.de

Gestaltung: Designbureau Kremer & Mahler, Köln

Diese Broschüre wurde auf 100% chlorfrei gebleichtem Papier gedruckt.

Bildnachweise:

Alle Abbildungen WDR

Datenspuren

Digitale Spuren können deutlicher sein als jeder Fußabdruck. Und um ihnen zu folgen, muss man noch nicht einmal in der Nähe sein. Ob privat oder beruflich: Moderne Kommunikationsmedien gehören zum Alltag. Niemand möchte mehr darauf verzichten. Doch der digitale Fortschritt hat seinen Preis. Fast jeder unserer Schritte und Tätigkeiten wird heute registriert – eine ungeheuerliche Menge von Daten-Spuren. An sechs Beispielen aus dem Alltag möchten wir Ihnen zeigen, was auch über Sie gespeichert werden kann.

In Deutschland sorgt das Bundesdatenschutzgesetz dafür, dass derartige Daten nicht unrechtmäßig genutzt werden. Aus diesem Grund sind auch die Datensätze, die wir Ihnen hier zeigen erfunden, aber realitätsnah.

In der rechten Spalte finden Sie den gespeicherten Datencode, links die Übersetzung in „Klartext“. Die Entsprechungen sind farbig gleich markiert.

1. Surfen im Internet

Beim Surfen im Internet wird die Adresse jeder Seite und jedes Bildes, in so genannten Log-Dateien des Anbieters gespeichert. Würde beispielsweise eine Firma das Surf-Verhalten ihrer Mitarbeiter kontrollieren wollen, könnte sie theoretisch diese Log-Dateien auswerten und herausfinden:

„Unser Mitarbeiter **Wolfgang Schmidt** kommt gerade von unserem **Gesundheitsportal**. Jetzt ruft er **unsere Wetterseite** auf und schaut sich den Wetterbericht für Köln an.“

Gelangt man über einen Hyperlink auf eine andere Seite, wird zusätzlich die **Herkunftsseite** in die Log-Datei geschrieben – in unserem Beispiel steht allerdings nur „ - “, weil die Adresse direkt eingegeben wurde.

```
149.219.195.999 - -  
[15/Jun/2004:13:30:02 +0100] "  
GET /home/gesundheit/  
HTTP/1.1" 200 18158  
" - "
```

"Mozilla/4.0 (compatible;
MSIE 5.5; Windows NT 5.0)"

```
149.219.195.999 - -  
[15/Jun/2004:13:31:19 +0100] "  
GET /home/wetter/  
HTTP/1.1" 200 18158  
" - "
```

"Mozilla/4.0 (compatible;
MSIE 5.5; Windows NT 5.0)"

```
149.219.195.999 - -  
[15/Jun/2004:13:31:19 +0100] "  
GET /images/wetter-koeln.jpg  
HTTP/1.1" 200 4830  
" - "
```

"Mozilla/4.0 (compatible;
MSIE 5.5; Windows NT 5.0)"

2. Mobil telefonieren

Mit jedem Anruf von einem (Mobil-) Telefon hinterlässt man ebenfalls Spuren. So genannte Call Data Records (CDR) erfassen Daten, die zum Beispiel für die Rechnungserstellung benötigt werden. Ein Mobilfunkanbieter könnte theoretisch diese CDRs auswerten und z. B. herausfinden:

„Unser Kunde **Wolfgang Schmidt** ist gerade in der Kölner Innenstadt und ruft **Klaus Lehmann** an. Der ist ebenfalls Kunde bei uns. Das Gespräch dauert **90 Sekunden**. Herr Lehmann ist jetzt in der Nähe von Montabaur und bewegt sich sehr schnell nach Nord-Westen.“

CDR's speichern insgesamt 25 Informationen. Die Firma Ericsson hat uns solch einen Datensatz aus ihrem Testlabor zur Verfügung gestellt und mit nicht existierenden Telefonnummern versehen. Hier können Sie den kompletten Datensatz sehen – einmal hexadezimal codiert und dann in einem lesbaren Format.

```
chargeableDuration  
00 01 30  
dateForStartOfCharge  
04/06/15  
interruptionTime  
0 0 0  
timeForStartOfCharge  
13 32 10  
timeForStopOfCharge  
13 33 40  
calledPartyNumber  
01552186175  
callingPartyNumber  
01551234567  
disconnectingParty  
01
```

3. Einsatz einer Kundenrabattkarte

Kundenrabattkarten sind momentan ein großer Renner in Deutschland. Im Jahr 2002 waren 62 Millionen davon im Umlauf. Wer sich eine zulegt, sollte überlegen, welche Daten er Preis geben möchte. Theoretisch kann der Karten-Anbieter solche Angaben gewinnen:

„**Wolfgang Schmidt** kaufte gestern in unserer **Kölner Filiale** aus der Warengruppe **'Golfzubehör und -schuhe'**. Dafür erhält er **41 Rabatt-Punkte**.“

```
1234567890123456;  
16.06.2004; 15.06.2004;  
234561234; KWQAG;  
Golfzubehör und -schuhe;  
A; 41; 4536
```



4. Einsatz einer Kreditkarte

Zahlen mit der Kreditkarte ist praktisch und recht sicher. Wer ohne Bargeld flüssig sein will, hinterlässt bei jeder Zahlung eine Spur.

Wer etwa in einem Restaurant sein Mittagessen mit einer Kreditkarte bezahlt, hinterlässt zunächst nur eine relativ undeutliche Datenspur: Der Betrag wird lediglich autorisiert; d. h. es wird mit einer Anfrage (0200) überprüft, ob die Karte gültig ist und die Summe im Kreditrahmen liegt. Die entsprechende Autorisierungsstelle gibt in ihrer Antwort (0210) nur ein OK und könnte aus den Daten theoretisch Folgendes lesen:

```
„Um 15 Uhr 24 wird heute (am 15.06.) mit einer
Kreditkarte mit der Nummer 5000123456789012,
die bis Oktober 2007 gültig ist, eine Rechnung
über 140 Euro 50 zur Bezahlung akzeptiert. Der
Vorgang erhält die Autorisierungsnummer
883191.“

0200
5000123456789012
14050
152422
0615
0710
978

-----

0210
5000123456789012
14050
152422
0615
0710
00
978
883191
```

Erst am Abend leitet das Restaurant alle Zahlungsvorgänge gesammelt weiter. Jetzt kann der Zahlvorgang mit dem Restaurant in Verbindung gebracht werden.

5. Online-Einkauf

Wer im Internet surft, hinterlässt häufig nicht nur Spuren in Log-Dateien, sondern auch Spuren, die er selbst verursacht. Wer etwa bei einem Online-Buchhändler Kunde ist, der findet auf seinem eigenen Computer mit hoher Wahrscheinlichkeit ein oder mehrere so genannter Cookies. Das sind kleine Text-Dateien, die verschiedene Anbieter nutzen, um z. B. die darin gespeicherte Kundennummer mit dem Datensatz der Kundendaten abzugleichen. Bei einem erneuten Besuch der Seiten, übermittelt der Browser automatisch alle relevanten Cookies an den Buchhändler. So kann man dann z. B. persönlich begrüßt werden und muss bei einer Bestellung nicht erneut seine Adresse eingeben. Diese Informationen könnten in einem Cookie stecken:

- Domäne, die den Cookie gesetzt hat (und ihn lesen darf)
- Hinweis, ob alle Rechner der Domäne buecher-ueber-nacht.de Zugriff haben
- Pfad innerhalb der Domäne
- Hinweis, ob der Cookie nur über sichere Verbindungen gelesen werden darf
- Gültigkeit des Cookies („Timestamp“ = Sekunden seit 01.01.1970, 00:00 Uhr); in diesem Fall z.B. bis zum 31.12.2030
- Name des Cookies
- „Wert“ des Cookies – z. B. die Kundennummer oder der Zeitpunkt des letzten Besuchs der Seite

```
buecher-ueber-nacht.de
TRUE / FALSE 1924949532
z-abcde POT123-ABCDE
```

6. Computer ausschalten

Wer in einer Firma an einem Netzwerk-Computer arbeitet, hinterlässt beim An- und Abmelden ebenfalls kleine Dateien auf dem Server. Die betreffende Firma könnte diese Dateien theoretisch auswerten und herausfinden:

„Unser Mitarbeiter Wolfgang Schmidt hat heute um 16 Uhr und 4 Sekunden den Computer heruntergefahren.“

```
farnsworth (149.219.195.999)
closed connection to
service WWW-Server
[2004/06/15 16:00:04, 1]
smbd/service.c:close_cnum(677)
```

```
farnsworth (149.219.195.999)
closed connection to
service Redaktion
[2004/06/15 16:00:04, 0]
passdb/pdb_ldap.c:
ldap_connect_system(316)
```



Scoring – sind Sie kreditwürdig?

Nehmen wir an, jemand braucht ein neues Auto oder möchte mal wieder Urlaub machen. Oder er hat genug davon, monatlich Miete zu zahlen, und träumt statt dessen von einer Eigentumswohnung. Oft fehlt dazu das nötige „Kleingeld“. Hier helfen die Banken weiter. Sie bieten „rasche“ Kredite – für das Auto, den Urlaub oder die Eigentumswohnung.



Sofortkredite erfüllen Wünsche, glaubt man den Banken

Doch wie entscheidet eine Bank, wem sie einen Kredit gibt und wem nicht? Hier kommt die Schufa, die „Schutzgemeinschaft für allgemeine Kreditsicherung“ ins Spiel. Im Schufa-Verbund sind nicht nur fast alle deutschen Kreditinstitute, sondern auch rund 2000 Händler und andere Dienstleister, über 60 Telekommunikationsfirmen, fast 50 Versicherungen, 75 Versorgungs-, fast 90 Inkassounternehmen und über 350 gewerbliche Wohnungsgesellschaften. Die Schufa hat Daten von rund 59 Millionen Bürgern in ihrem Speicher, das ist der Großteil der geschäftsfähigen Bevölkerung.

Sie weiß alles über laufende Kredite und Konten, Kreditkarten, über Alter und Wohnort. Allein aus diesen Merkmalen kann die Schufa die Kreditwürdigkeit eines jeden berechnen. Das interessiert vor allem Banken und Sparkassen, Versandhäuser oder Telekommunikationsunternehmen. Denn jeder Kredit ist mit einem Risiko behaftet. Riskant sind auch Dienstleistungen oder Waren, die auf Rechnung geliefert und erst später beglichen werden.

Die Suche nach dem erhöhten Risiko



Mit welcher Formel die Schufa das Kreditrisiko berechnet, ist Firmengeheimnis. Doch das Verfahren ist bekannt: das so genannte „Scoring“.

Um einen Score zu ermitteln, durchkämmen Hochleistungsrechner die Datensätze der rund 59 Millionen bei der Schufa registrierten Bürger. Heraus kommen diejenigen, die in den letzten 15 Monaten einen Kredit platzen ließen. In einem zweiten Schritt sucht der Computer nach den gemeinsamen Merkmalen dieser „Kreditversager“. Für alle

Was verraten die Daten?

Kreditinteressenten, die ebenfalls diese Merkmale tragen, kann es eng werden. Statistisch gesehen stellen sie ein erhöhtes Risiko dar. Da aber immer nur die letzten 15 Monate in die Berechnungen einfließen, können sich diese Kennzeichen auch ändern. Ein Score ist damit so dynamisch wie das Leben selbst.

Nicht nur Banken profitieren

Das Verfahren ist anerkannt und standardisiert. Dank des Scores kann jeder Bankangestellte rechnerunterstützt in nur wenigen Sekunden erfahren, ob ein Kunde kreditwürdig ist oder leer ausgehen muss. Denn: Wer einen zu niedrigen Score besitzt, stellt ein zu hohes Risiko dar – und hat damit keine Chance auf einen Kredit. Das schützt aber auch den Bankkunden vor finanziellen Überforderungen. Denn die Gefahr, sich zu übernehmen, ist groß. Schätzungsweise drei Millionen Deutsche sind bereits nicht mehr in der Lage, ihre Schulden aus eigener Kraft zu tilgen.



Drei Millionen Deutsche sind nicht mehr in der Lage, sich aus eigener Kraft von ihren Miesen zu befreien

Vergleichbar mit der ADAC-Pannenstatistik

Das Score-Verfahren ist trotz weniger Angaben erstaunlich genau. So liefert es Banken, Versandhäusern und Handy Providern gute Einschätzungen selbst über Neukunden. Die Kreditrisiken für beide Seiten sind dadurch deutlich minimiert.

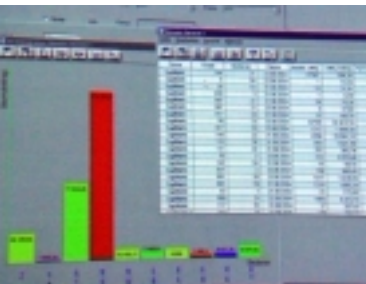
Ähnlich funktioniert auch die ADAC-Pannenstatistik. Bestimmte Auto-Modelle haben aufgrund zurückliegender Erfahrungswerte ein höheres Pannenrisiko als andere. Doch die Statistik kann im nächsten Jahr schon wieder anders aussehen und die Rangfolge der Modelle eine andere sein.



Data-Mining – Lesen in der Datenflut

In allen Bereichen unserer Gesellschaft türmen sich Berge von Daten. Unternehmen horten die Produktions-, Lager- und Verkaufsdaten ihrer Produkte. Wissenschaftler sammeln große Mengen von Rohdaten in ihren Experimenten. Regierung und Verwaltung speichern statistische Daten über Wirtschafts- und Verbrechenentwicklung. Alle stehen vor dem gleichen Problem: Daten sind nicht gleich Informationen. Ohne zielgerichtete Auswertung sind sie wertlos. Intelligente Computerprogramme mit Techniken des „Data-Mining“ helfen wichtige Zusammenhänge im Datenschwungel zu entdecken.

Data-Warehouse und Mustersuche



Eine große Hürde des „Datenschürfens“ steht ganz am Anfang des Prozesses: Alle Datensätze müssen in einem einheitlichen Format vorliegen. Das gilt vor allem für Daten aus verschiedenen Unternehmensbereichen. Sollen diese zusammengeführt werden, ist eine Übersetzung in eine einheitliche Form unumgänglich. Diese so genannte Datenintegration ist oft der schwierigste Teil der Aufgabe. Viele Unternehmen sind dazu übergegangen, alle Unternehmensdaten vorsorglich in eine große einheitliche Datenbank, das Data-Warehouse, aufzunehmen.

Firmendaten enthalten verborgene Informationen

Sind die Daten vorbereitet, kann die Data-Mining-Software ihre Arbeit beginnen. Ganz ohne menschliche Hilfe geht es allerdings nicht. Ein Administrator füttert das System zum Beispiel mit den Profilen besonders kreditwürdiger und besonders unzuverlässiger Kunden. Mit mathematisch-statistischen Verfahren und Methoden der künstlichen Intelligenz durchforstet das Programm dann den Datenberg und versucht Gemeinsamkeiten und Zusammenhänge zu entdecken. Oft findet es dabei Muster, die dem Menschen bis dahin verborgen geblieben waren. Möglicherweise sind Kunden, die oft umziehen, aber keine Kinder haben, besonders kreditwürdig – oder gerade nicht. Meistens ist diese Suche nach Mustern ein mehrstufiger Prozess. Der Computer liefert erste Resultate, der Mensch verfeinert die Suche und der Rechner analysiert die Daten in der neuen Richtung.

Die Anwendung

Data-Mining kommt in den verschiedensten Bereichen zum Einsatz: von der wissenschaftlichen Genanalyse bis zum Kundenmanagement. Denn in all diesen Bereichen gibt es Grundtypen von Fragestellungen:

- **Klassifikation:** Ist dieser Kunde kreditwürdig oder nicht?
- **Konzeptbeschreibung:** Welche Eigenschaften haben reparaturanfällige Fahrzeuge?
- **Segmentierung:** Wie lassen sich meine Kunden in aussagekräftiger Weise in Untergruppen einteilen?
- **Prognose:** Wie wird sich der Dollarkurs entwickeln?
- **Abhängigkeitsanalyse:** Welche Produkte werden häufig zusammen gekauft?
- **Abweichungsanalyse:** Gibt es jahreszeitliche Umsatzschwankungen?

Versicherungsgesellschaften finden betrügerische Kunden, Fabriken Fehler in der Produktion und Versandhäuser Kunden, denen man besser keinen Kauf per Rechnung anbietet.

Das Praxisbeispiel: Data-Mining an der Ladenkasse

Jeder Einzelhändler kennt das Problem: Am Ende des Jahres stimmt die Abrechnung nicht. Das Europäische Institut für Einzelhandel schätzt, dass die Inventurdifferenzen in Lebensmittelsupermärkten zu rund einem Drittel auf das Konto der Angestellten gehen. Doch die Kassierer lassen sich mit Data-Mining überprüfen. Moderne Kassen erzeugen jeden Tag große Mengen von Daten: Sie zeichnen jede Aktion auf. Jeden Artikel, jedes Storno, jede Pause, jedes Öffnen der Kasse.



Diese Daten werden abends auf den Zentralcomputer übertragen und am nächsten Tag vom Revisor analysiert. Mit Data-Mining hilft ihm eine Software die wichtigen Informationen von den unwichtigen zu unterscheiden. Ein Beispiel ist Leergut: Ein Kunde lässt an der Kasse einen Leergutbon mit den Einkäufen verrechnen. Doch jeder Leergutbon ist eine Gelddrückzahlung. Mit etwas krimineller Energie könnte sich ein Kassierer bereichern und sich selbst Geld auszahlen.

Moderne Kassen speichern alle Aktionen des Kassierers



Doch der Revisor erkennt, wenn eine Filiale häufiger als der Durchschnitt Geld für Leergut herausgibt. Dann vergleicht er alle Kassierer der Filiale miteinander. Dabei fällt ihm möglicherweise einer auf, der ungewöhnlich häufig Leergutbons annimmt. Mit wenigen Mausklicks durchforstet er dann die Kassenbons der vorhergehenden Wochen.

Das Data-Mining-Programm liefert also Indizien. Überführt ist der Angestellte noch nicht – er steht lediglich unter verschärfter Bobachtung.

Mit dieser Technik arbeitet der Revisor sehr effektiv. Er kann jederzeit die gängigen Betrugsmaschen überprüfen. Das Programm weist ihn aber auch auf mögliche Methoden der Betrüger hin, die er noch nicht kennt.

Data-Mining zur Leistungskontrolle?



Revisor am Computer

Eine Handelskette in der Schweiz berichtet, dass sie mit einem solchen Programm innerhalb von zwei Monaten 200 000 Franken eingespart habe. Daraufhin entließ sie über 50 Kassiererinnen und Kassierer. Die Software wird seit wenigen Jahren aber auch in etlichen großen Supermarkt- und Kaufhausketten in Deutschland eingesetzt. Die betreffenden Firmen gehen mit diesen Informationen aber nicht gerne an die Öffentlichkeit.

Die Überprüfung der Angestellten durch Data-Mining hat nämlich einen unangenehmen Beigeschmack.

Für den Computer ist zunächst jeder verdächtig und viele Kassierer fürchten, dass auch ihre Fehler und Schwächen ausgewertet und gegen sie verwandt werden. Für sie ist es unangenehmer, bei der Arbeit das Gefühl zu haben, dass jemand hinter ihnen steht und jede Schwäche registriert. Gewerkschafter und Datenschützer fordern deshalb, dass Angestellte und Arbeitgeber in einer Betriebsvereinbarung festhalten, dass das Data-Mining-Programm nicht zur Leistungskontrolle eingesetzt werden darf.

Bedrohte Freiheitsrechte in den USA

In den USA hat der Datenschutz von jeher einen geringeren Stellenwert als in Deutschland. Es gibt kein „Bundesdatenschutzgesetz“ und keinen „Bundesdatenschutzbeauftragten“. Seit den Anschlägen des 11. September 2001 hat die Regierung im Namen der Terrorbekämpfung die Rechte der Bürger weiter beschnitten.

11. September und "Patriot Act"

Nach dem Terrorakt zögerte die Regierung von George Bush nicht lange. Bereits vier Wochen später unterzeichnete der Präsident ein Gesetzespaket mit dem Namen „USA Patriot Act“ (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism). Einstimmig nahmen beide Kammern des Parlaments die Vorlage an. Der „Patriot Act“ erweitert die Befugnisse der Bundespolizei FBI und der Geheimdienste. Ihre Kontrolle durch Richter und Gerichte wurde hingegen geschwächt. Ohne konkreten Tatverdacht kann jetzt zum Beispiel das FBI Telefone abhören und Emails kontrollieren. Viele Kritiker sehen die Bürgerrechte in Gefahr.



Das World Trade Center
am 11.9.2001

Die Behörden erhielten sogar Vollmachten, pauschal gegen unschuldige Bürger zu ermitteln. Bei allgemeinen Nachforschungen kann das FBI auf fast alle privaten und öffentlichen Datenbestände zugreifen. Dazu zählen Versicherungen, Reisebüros, Banken, Versandhändler, Telefongesellschaften und viele mehr. Besonders pikant: Auch Buchhandlungen und Büchereien müssen ihre Kundendateien und Verkaufsunterlagen herausrücken. Auch hier muss kein konkreter Verdacht vorliegen. Die betroffenen Einrichtungen, Firmen und Geschäfte dürfen ihre Kunden noch nicht einmal von diesen Überprüfungen unterrichten. Niemand weiß, welche Bücher als verdächtig gelten. Selbst der Besuch einer Tauchschule ist mittlerweile Anlass zu einer Sicherheitsüberprüfung. Wegen der Möglichkeit terroristischer Anschläge von See sollen alle Tauchschulen ihre Mitglieder melden.





Logo des Information Awareness Office im Pentagonon

Total Information Awareness und MATRIX

Mit den neuen Gesetzen scheint der Hunger des amerikanischen Staates nach den Daten seiner Bürger unersättlich geworden zu sein. Anfang 2002 kündigte das Pentagon ein ganz besonderes Forschungsprojekt an: das Programm „Total Information Awareness“ (TIA), was so viel heißt wie „Totales Informationsbewusstsein“. Das Programm setzte sich zum Ziel, sämtliche verfügbaren öffentlichen Datenquellen in einer gigantischen Datenbank zu vereinen. Data-Mining-Programme sollten dann in diesem Datenberg nach auffälligen Personen suchen. Doch das Parlament nahm Anstoß an den umfassenden Überwachungsplänen. Daraufhin wurde das Programm in „Terrorist Information Awareness“ umbenannt. Die Befürworter versicherten, dass es nicht zur Überprüfung amerikanischer Bürger eingesetzt werden sollte. Ende 2003 stoppte der amerikanische Kongress schließlich TIA.

Ein ähnliches Programm läuft aber auf Ebene der Bundestaaten weiter. Ursprünglich hatten sich 14 Bundesstaaten unter der Führung von Florida auf eine zentrale Datenbank mit dem Namen MATRIX (Multistate Anti-Terrorism Information Exchange) geeinigt. Ziel ist es, mit Data-Mining nach Mustern und Verbindungen zwischen Personen und Ereignissen zu suchen. Die Datenbank enthält Informationen der Strafverfolgungsbehörden sowie persönliche Informationen von Amerikanern, die in käuflichen Datensammlungen verfügbar sind.

Kontrolle im Luftverkehr: CAPPS II und No-Fly-Listen

Ähnlichen Fleiß beim Sammeln von Daten legen die Behörden in der Luftfahrt an den Tag. Sie sind dabei, die Daten aller Flugpassagiere zu speichern und zu analysieren. Auf den Druck der amerikanischen Regierung mussten sich auch europäische Airlines verpflichten, vor dem Abflug Informationen über ihre Fluggäste zu übertragen. Verschiedene amerikanische Fluggesellschaften haben schon komplette Datensätze von einigen Millionen Passagieren an die Behörden übergeben, um damit das Computerprogramm des CAPPS II (Computer Assisted Passenger Pre-screening System) zu trainieren.

Die Software teilt die Reisenden in Risikogruppen ein. Wer von der Norm abweicht, wird kontrolliert. Wer zu verdächtig ist, darf gar nicht erst an Bord. Doch nach welchen Kriterien Personen auf diesen No-Fly-Listen landen, offenbart die Transportbehörde nicht.

Kriegsgegner im Visier

Dass diese Aktivitäten nur zum Teil dazu dienen Terroristen aufzuspüren, zeigt der Fall der Dominikanernonne Virgine Lawinger. Sie wollte an einer Antikriegsdemonstration in Washington teilnehmen. Doch die Sicherheitsbehörden verweigerten ihr den Zugang zum Flugzeug. Die 75-Jährige steht auf der No-Fly-Liste. Schwester Lawinger ist also eine der Personen, die als potentiell gefährlich gelten. Möglicherweise deshalb, weil sie in der Anti-Kriegs-Bewegung aktiv ist. Eine offizielle Erklärung geben ihr die Behörden allerdings nicht. Fälle wie ihrer werden immer häufiger bekannt.



Dominikanernonne Virgine Lawinger

Im Land formiert sich jetzt Widerstand. Bürgerrechtsorganisationen und einige Politiker beider Parteien wollen die Macht des Staates wieder einschränken.

So hat das amerikanische Parlament eine Idee des US-Justizministers Ashcroft immer wieder abgelehnt. Ashcroft wollte eine Datenbank einrichten, in der unüberprüfte Hinweise und Beobachtungen von Bürgern gespeichert werden sollten. Eine Datenbank für Denunzianten also.



Überwachungskamera

Überwachungskameras und Gesichtserkennung

In Bahnhöfen und auf Flughäfen, in Kaufhäusern und auf öffentlichen Plätzen – überall sind Kameras auf uns gerichtet. Kaum eine Form der Überwachung ist allgegenwärtiger als die der Videoüberwachung. Rechtlich gesehen ist die Aufnahme von Videobildern eine Form der Datenerhebung. Das Problem: Der Gefilmte weiß oft nicht, dass Bilder von ihm gemacht werden, also Daten erhoben werden. Dabei haben wir alle seit dem Volkszählungsurteil aus dem Jahre 1985 das Recht auf „informationelle Selbstbestimmung“. In Deutschland hat jeder das Recht, über die Erhebung, Preisgabe und Nutzung seiner persönlichen Daten zu bestimmen. Die Videoüberwachung ist ein gutes Beispiel für den Konflikt zwischen einer Überwachungstechnologie und dem Recht auf informationelle Selbstbestimmung.



Großbritannien

Verglichen mit Großbritannien steckt die Videoüberwachung in Deutschland noch in den Kinderschuhen. Pro Einwohner gibt es dort dreiundzwanzigmal so viele Kameras wie in Deutschland. Kein anderes Land setzt mehr Kameras pro Kopf ein, um seine Bürger zu beobachten. Die Briten haben dabei viel geringere datenschutzrechtliche Bedenken als die Deutschen. Im Gegenteil: Sie sehen Kameras als Wunderwaffe der öffentlichen Sicherheit, besonders seit der Ermordung des kleinen Jamie Bulger im Februar 1993. In einem Einkaufszentrum in Liverpool filmte eine Kamera, wie zwei Zehnjährige Jamie entführten. Kurze Zeit später brachten die Teenager den Zweijährigen um. Die Videobilder führten zu ihrer Festnahme. Spätestens seitdem sind die Briten vom Nutzen der Überwachungskameras überzeugt. Über die nächsten zehn Jahre gaben sie mehr als fünf Milliarden Euro für vier Millionen Kameras aus. Überwachung wurde als Allheilmittel der Verbrechensbekämpfung gepriesen. Dennoch gibt es bis heute keine stichhaltigen Beweise, dass Kameras tatsächlich Verbrechenszahlen verringern.



Jamie Bulger wird entführt

Automatische Gesichtserkennung

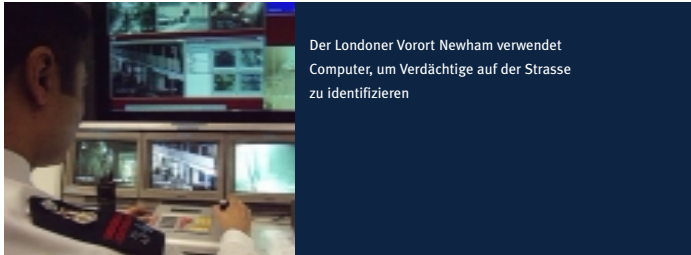
Überwachung ist teuer. Der Fall Copeland ist ein Paradebeispiel: 1999 terrorisierte David Copeland London mit Nagelbomben. Nach 13 Tagen wurde er mithilfe von Überwachungskameras gefasst. Doch der Aufwand der Ermittlungen war hoch. Die Polizei musste 26.000 Stunden Videomaterial durchforsten, um ihn zu identifizieren. Darum sucht man in England nach neuen Methoden, um die Überwachung per Kamera effektiver zu gestalten. Der Londoner Vorort Newham glaubt eine Lösung gefunden zu haben: Computer sollen helfen, Straftäter zu identifizieren. Ein Rechner isoliert Gesichter aus laufenden Videobildern und vergleicht sie mit einer Verdächtigen-Datenbank. Wenn der Computer glaubt, ein verdächtiges Gesicht in der Menge gefunden zu haben, alarmiert er einen menschlichen Überwacher. Dieser kann dann entsprechend reagieren. Newhams Behörden behaupten, das System hätte die Verbrechenszahlen verringert. Doch der Erfolg liegt wohl eher in der Abschreckung, denn selbst nach Jahren des Einsatzes hat es noch zu keiner einzigen Festnahme geführt.

Menschen sehen besser als Computer

Trotz der Fortschritte auf dem Gebiet der automatischen Gesichtserkennung: Menschen erkennen Gesichter immer noch viel besser als Computer. Vor zwei Jahren führte die amerikanische Regierung einen Test von Gesichtserkennungssystemen durch. Der so genannte „Face Recognition Vendor Test“ kam zu ernüchternden Ergebnissen: Selbst unter besten Bedingungen erkennen die Systeme nur neun von zehn Personen. Die Ergebnisse sind noch schlechter, wenn mehr als



drei Jahre zwischen den aktuellen Aufnahmen und den Bildern der Datenbank liegen. Markante Gesichtszüge erleichtern dem Computer die Identifikation. Deshalb sind Männer in der Regel leichter zu erkennen als Frauen, und alte Menschen einfacher als junge. Zudem haben die Lichtverhältnisse und der jeweilige Kamerawinkel großen Einfluss auf die Qualität der Auswertung. Bilder einer Überwachungskamera automatisch vom Computer auswerten, geschweige denn Menschen von einem Rechner erkennen zu lassen, ist also noch Zukunftsmusik.



Der Londoner Vorort Newham verwendet Computer, um Verdächtige auf der Strasse zu identifizieren

VideoObjectTracker

Trotzdem können Computer heute schon einiges leisten. Das Fraunhofer Institut in Karlsruhe hat den „VideoObjectTracker“ entwickelt, ein Programm, das außergewöhnliches Verhalten erkennen kann. So ist der Computer zum Beispiel in der Lage, einen Fußweg vor einem Gebäude zu überwachen. Bewegt sich dort ein Mensch, registriert ihn das Programm. Sobald der Passant den erlaubten Weg verlässt, erkennt dies die Software und gibt Alarm. Solche Computerprogramme werden bereits zur Ausbruchüberwachung von Gefängnissen eingesetzt. Das Programm ist zum Beispiel auch imstande, ein ungewöhnliches Objekt im überwachten Bereich zu erkennen. Nach einer kurzen Toleranzzeit benachrichtigt das System den Wachdienst. Die Sicherheitsleute prüfen dann das Objekt, so zum Beispiel eine abgestellte Tasche.



RFID – Identifizierung per Funk

RFID

Auf Joghurtbechern, an T-Shirts und Kundenkarten bahnt sich eine Revolution an: RFID könnte schon bald das neue Zauberwort sein: Es steht für Radio Frequenz Identifikation, eine Art der drahtlosen Datenübertragung. RFID-Etiketten sollen in naher Zukunft die Strichcodes ablösen. Die neuen Etiketten tragen winzige Mikrochips und Radioantennen, die per Funk Daten mit Computern in der Lagerhaltung austauschen können. So muss man die Strichcodes nicht mehr mühsam von Hand mit einem Scanner einlesen. Das spart Zeit beim Transport und Geld bei der Lagerhaltung. Logistiker erhoffen sich damit Einsparungen in Millionenhöhe. Doch die neue Technik ist nicht ohne Tücken. Datenschützer befürchten, dass die Daten auf den Chips nicht nur zur Vereinfachung der Logistik dienen, sondern auch zur Ermittlung von Einkaufsgewohnheiten. Kundenkarten könnten zum Beispiel selbständig Signale senden, anhand derer Marktforscher die Einkaufsgewohnheiten der Kundschaft auf Schritt und Tritt überwachen könnten.



RFID-Chip, wie er schon heute in Pilotprojekten verwendet wird

Wie funktioniert's?

RFID-Etiketten funktionieren ähnlich wie die Etiketten, die Geschäfte an Kleidungsstücken zur Diebstahlsicherung anbringen. Bei Diebstahl-Warnanlagen stehen an den Ausgängen des Geschäfts Antennen, die gleichzeitig senden und empfangen. Die Antenne sendet schwache elektromagnetische Wellen aus, die von einem Chip im Etikett aufgenommen werden. Der Chip sendet nun seinerseits ein Signal aus, das die Antenne erkennt und daraufhin einen Alarm auslöst.



Diebstahlsicherungsanlagen regen mit elektromagnetischen Wellen Chips in Transpondern an

RFID-Etiketten funktionieren nach demselben Prinzip. Ihre Funksignale sollen jedoch nicht den Diebstahl verhindern, sondern Daten an Computer im Lager und an der Kasse übertragen. Auch hier sendet ein Lesegerät schwache elektromagnetische Wellen aus, die mithilfe einer Spule im Etikett einen geringen Strom erzeugen. Dieser Strom sorgt dafür, dass der Mikrochip seine Informationen wie Artikelnummer, Preis, Gewicht und Herstellungsdatum an einen Zentralcomputer sendet. Manche Etiketten können bis zu 100 Kilobyte an Daten speichern. Das entspricht etwa 30 beschriebenen DIN A4-Seiten. Diese Daten können beliebig oft gelesen, verändert, gelöscht und neu geschrieben werden. Damit lässt sich der Warenfluss automatisch verfolgen. Wird eine Ware knapp, bestellt der Computer nach. Das einzige, was der massenhaften Verbreitung



von RFID-Chips noch entgegensteht, ist ihr Preis. Im Moment sind die Etiketten noch zu teuer, um sie auf ein Kaugummipapier zu kleben, aber bei wertvollen Einzelstücken lohnt sich ihr Einsatz schon heute.

Logistikers Traum, Datenschützers Alptraum

Datenschützer befürchten, dass die Daten auf den Chips zur Bespitzelung von Kunden genutzt werden könnten. Per Funk könnte man somit ihre Position im Supermarkt, ihre Verweildauer vor einzelnen Regalen und die Produkte in ihrem Einkaufswagen registrieren. Doch auch nach Verlassen des Geschäftes hören die Chips nicht auf zu senden. Auch das nächste besuchte Geschäft könnte innerhalb von Sekunden erfahren, welche Produkte die Kunden mit sich führen. Schon beim Betreten eines Kleidungsgeschäfts könnten so zum Beispiel Marke, Preis und Alter der getragenen Kleidung über die eingenahten RFID-Etiketten ermittelt werden.

RFID führt Hund und Herrchen zusammen

Doch RFID kommt nicht nur bei Logistikaufgaben zum Einsatz. Wenn Haustiere verloren gehen, kann die RFID-Technologie wertvolle Dienste leisten. So genannte RFID-Transponder können mit einer Spritze einem Haustier leicht unter die Haut gesetzt werden. Der Mikrochip speichert eine 15-stellige Erkennungsnummer. Wenn der tierische Freund verloren geht und sich bei einem Tierarzt oder einem Tierheim wieder findet, kann die Zahl mit einem solchen Gerät gelesen werden. Über ein Haustierregister kann das Tier dann identifiziert werden und zu seinem Besitzer zurückgebracht werden.

RFID im Reisepass

Auch Menschen könnten bald mit RFID-Technologie leichter zu identifizieren sein. Es gibt Pläne, in wenigen Jahren sollen unsere Reisepässe RFID-Chips tragen. Die Chips könnten dann das digitalisierte Bild des Inhabers, seine persönlichen Daten und Fingerabdrücke speichern. Bei einer Kontrolle liest ein Beamter diese Informationen einfach per Funk aus. Auch hier befürchten Datenschützer einen Missbrauch der Informationen, denn wer kann schon genau feststellen, wann und wo die Daten des Chips im Ausweis gelesen werden?

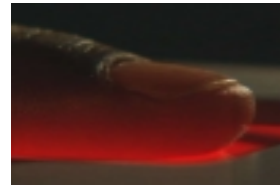
Biometrie

Biometrische Verfahren sind seit einigen Jahren auf dem Vormarsch. Mithilfe von moderner Technologie gelingt es inzwischen immer besser, Menschen anhand von Körpermerkmalen zu erkennen. Die Bandbreite biometrisch messbarer und damit unterscheidbarer Merkmale ist riesig. Am bekanntesten sind Fingerabdrücke, das Muster der Iris (Regenbogenhaut) und natürlich das Gesicht. Aber auch andere Merkmale können genutzt werden: die Hand- oder Fingergeometrie, das Venenmuster, die Stimme, das Tippverhalten an der Computertastatur, die Unterschriftendynamik und sogar die Art zu gehen. Biometrische Daten sind extrem personenbezogen und deshalb hochsensibel. Deswegen stehen sie unter besonderem Schutz.

„Von Minutien und Templates“

Biometrische Systeme vergleichen die gespeicherten Daten mit aktuell erhobenen Messdaten und berechnen daraus die Wahrscheinlichkeit der Übereinstimmung. 100-prozentige Sicherheit gibt es dabei nicht. Da Kameras (z. B. für Gesichts- oder Irisbilder) und Sensoren (z. B. für Fingerabdrücke) immer geringfügig andere Aufnahmen liefern, muss jedes System Abweichungen tolerieren. Die Festlegung dieser Toleranzschwelle ist eine große Herausforderung. Ist sie zu niedrig, werden Personen beispielsweise bei einer Zugangskontrolle trotz Berechtigung abgelehnt. Ist sie zu hoch, werden Unberechtigte akzeptiert.

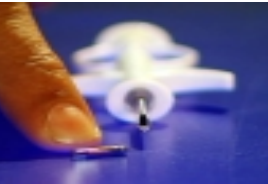
Wie funktioniert so eine Messung? Die Linien eines Fingerabdrucks zum Beispiel sind in Form und Lage zueinander einmalig. Die Erkennungssoftware sucht in der Aufnahme eines Fingerabdrucks individuelle Merkmale wie z. B. kurze Linien, Gabelungen und Kreuzungen, so genannte Minutien. Das Programm vergleicht entstehende Muster mit der gespeicherten Vorlage. Datenbanken oder Zugangs-Chipkarten speichern in der Regel keine Rohdaten der vermessenen Körperteile, sondern nur Referenzmuster, so genannte Templates. Gerade Datenschützer halten das für unbedingt notwendig, denn aus biometrischen Daten lassen sich weitergehende Informationen über eine Person herauslesen, z. B. über Krankheiten.



Jeder Fingerabdruck ist einzigartig



Charakteristische Merkmale ergeben ein Minutienmuster



RFID-Transponder werden zur leichteren Identifizierung in Tiere implantiert





ICAO setzt auf Gesichtserkennung

„Biometrie im Pass der Zukunft“

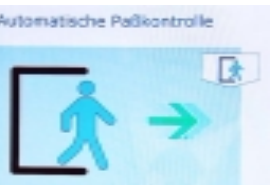
Nach dem 11. September 2001 haben die USA die Diskussion um biometrische Daten im Reisepass verstärkt und auch die Europäer unter Zeitdruck gesetzt. Schon 2006 sollen alle Pässe biometrisch aufgerüstet sein. Als internationalen Standard empfiehlt die internationale zivile Luftfahrtbehörde ICAO (International Civil Aviation Organization) das digitale Gesichtsbild, also die Gesichtserkennung. Die biometrischen Daten sollen auf einem RFID-chip gespeichert werden. Bei einer Kontrolle liest der Grenzbeamte die Daten auf dem Chip einfach per Funk aus.

Gigantisches Laborexperiment?

Ob biometrisch aufgerüstete Reisepässe tatsächlich die Sicherheit erhöhen, weiß niemand. Das Büro für Technikfolgenabschätzung des Deutschen Bundestags hat kürzlich einen Sachstandsbericht zum Thema „Biometrie und Ausweisdokumente“ veröffentlicht. Er basiert auf mehreren Gutachten und soll eine Hilfestellung für die Arbeit der Fachausschüsse des Bundestages sein. Der Bericht kommt zu dem Ergebnis, dass die bisherigen Erkennungstechniken noch zahlreiche Tücken aufweisen. Zusätzlich gibt er zu bedenken, dass trotz geringer Fehlerraten bei größeren Feldstudien immer noch eine große Anzahl von Menschen nicht erkannt werden. Dies würde in der Realität den Reiseverkehr erheblich stören. Außerdem wird die Einführung der neuen Passgeneration mit Sicherheit ein teures Vorhaben. Fazit der Verfasser: „Die Frage, ob die erwartbare Erkennungsleistung bei der Verifikation eine hinreichende Sicherheit gewährleistet und ob die erhofften Verbesserungen bei der Grenzkontrolle den hierzu erforderlichen Aufwand rechtfertigen, muss politisch entschieden und begründet werden.“



Zukunftsvision: Kontrolle von Biometriepässen



Schneller über die Grenze dank Biometrie?

Lesetipps

„Biometrische Identifikation. Grundlagen, Verfahren, Perspektiven“

Autor: Michael Behrens
Verlagsangaben: Vieweg Verlag, November 2001
ISBN: 3528057866
Sonstiges: 243 Seiten, Preis EUR 46,90

„Biometrische Verfahren“

Autoren: Veronika Nolde, Lothar Leger
Verlagsangaben: Deutscher Wirtschaftsdienst, 2002
ISBN: 3871564648
Sonstiges: 477 Seiten, Preis EUR 49,-



Linktipps

SCHUFA UND SCORING

Mehr Infos zur SCHUFA und zum Thema SCHUFA-Auskunft und Scoring:
www.schufa.de/downloads/EB_D.pdf

Mehr Infos zum Auskunftsanspruch über den persönlichen Score-Wert:
www.bfd.bund.de/buergerfragen/fra24.html

DATA-MINING

Data Warehouse und Data-Mining im öffentlichen Bereich – Datenschutzrechtliche und -technische Aspekte. Eine Beurteilung des Landesbeauftragten für den Datenschutz Mecklenburg-Vorpommern. Mit einer kurzen technischen Einführung
http://www.lfd.m-v.de/informat/dwh/index_dw.html

Gutachten des Unabhängigen Zentrums für Datenschutz Schleswig-Holstein zur Data-Mining-Software Loss Prevention der Firma Fujitsu
<http://www.datenschutzzentrum.de/material/themen/wirtscha/lossprev.htm>

Ein Hersteller von Data-Mining-Software zur Untersuchung von Betrug an der Ladenkasse stellt sein Produkt vor.
http://www.logware.de/datamining_lossprevention.htm

Online-Version eines Artikels von Prof. D. A. Keim von der Universität Konstanz: Datenvisualisierung und Data-Mining, Datenbank Spektrum, Vol. 2, No. 1, pp. 30-39, 2002. Sehr fachlicher aber interessanter Überblick über die Techniken des Visuellen Data-Minings.
<http://fusion.cs.uni-magdeburg.de/pubs/spektrum.pdf>

BIOMETRIE

Das Büro für Technikfolgenabschätzung beim Deutschen Bundestag berät die Parlamentarier in Fragen des wissenschaftlich-technischen Wandels.
<http://www.tab.fzk.de/>

Hier findet man auch den aktuellen Sachstandsbericht zum Thema "Biometrie und Ausweisdokumente"
<http://www.tab.fzk.de/de/arbeitsberichte.htm>

Die Homepage der International Civil Aviation Organization, die maßgeblich für die Form und die Sicherheit (gegen Fälschung und Missbrauch) von Reisedokumenten verantwortlich ist (englisch)
<http://www.icao.int/>

Hier schreiben die Biometrieexperten des Chaos Computer-Clubs über Schwachstellen biometrischer Systeme.
<http://www.biometrische-systeme.org/>

FREIHEITSRECHTE IN DEN USA

Die Internetzeitschrift des Heise-Verlages (c't) verfolgt die Entwicklung in den USA kritisch und seriös. Im Archiv finden sich zahlreiche Artikel zum Thema Einschränkung der Freiheitsrechte.
www.telepolis.de

Exemplarisch einige Links:

Totale Überwachung:
<http://www.heise.de/tp/deutsch/inhalt/te/13580/1.html>
Überwachungsmonster USA:
<http://www.heise.de/tp/deutsch/inhalt/te/13982/1.html>
Das Terrorist Screening Center der USA:
<http://www.heise.de/tp/deutsch/inhalt/te/17489/1.html>
Kriegsgegner auf CAPPS-Überwachungsliste:
<http://www.heise.de/tp/deutsch/inhalt/te/15375/1.html>

Informationen der Bürgerrechtsorganisationen "Electronic Privacy Information Center" und "American Civil Liberties Union" zum Patriot Act (Englisch)
<http://www.epic.org/privacy/terrorism/usapatriot/>
<http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=13255&c=207>

RFID

EAN, der Weltstandard für Identifikationsverfahren im Einzelhandel, setzt sich für RFID ein:
<http://www.ean.de/ean/Inhalt/e4/e64>

Datenschützer haben Bedenken gegenüber der RFID-Technologie:
<http://www.spychip.de/>

Registrierung von Haustieren:
<http://www.tierschutzbund.de/service/>

Die Bundesdruckerei wird den neuen Reisepass mit RFID-Technologie produzieren:
<http://www.bundesdruckerei.de/de/border/index.html>



Quarks & Co Scripte

KAMERAÜBERWACHUNG

„Urban Eye“, ein europäisches Forschungsprojekt zur Videoüberwachung:
<http://www.urbaneye.net/>

Die Website des Londoner Stadtteils Newham Council (englisch):
<http://www.newham.gov.uk/>

Die Studie zur Gesichtserkennung aus den USA
Face Recognition Vendor Tests (englisch):
<http://www.frvt.org/>

Mehr zum VideoObjectTracker des Fraunhofer Instituts in Karlsruhe
http://www.vision.fraunhofer.de/vision_neu/de/projekte/65.html

In der Reihe QuarksScript sind folgenden Themen als Broschüren erhältlich:

Lebenskünstler Baum
Die fantastische Welt des Unsichtbaren
Leben ohne Schmerz?
Lebensquell Wasser
Das Geheimnis der Neandertaler
Volksdroge Alkohol
Der Kampf gegen die Kilos
Abenteuer Fliegen
Spurensuche auf dem Mars
Das ABC der Vitamine
Gute Hexen - böse Hexen
Das geheime Leben der Frösche
Lernen mit Köpfchen
Wunder Ei
Wunderdroge Tee
Was Knochen erzählen
Blut - Der ganz besondere Saft
Milch unter der Lupe
Die Welt der Düfte
Risiko Elektromog?
Diagnose „zuckerkrank“
Wie wir lernen
Diäten unter der Lupe
Energie der Zukunft
Die Börse - einfach erklärt
(2. überarbeitete Auflage)
Die Biochemie der Liebe
Die Kunst des Klebens
Der Traum vom langen Leben
Mindestens haltbar bis ...
Kampf dem Schmutz
Schokolade - die süße Last
Abenteuer Fahrrad
Unser Schweiß
Unsere Haut

(Diese und weitere Themen können Sie es online unter www.quarks.de als PDF beziehen)

So bestellen Sie ein QuarksScript:

Beschriften Sie einen C5-Umschlag mit Ihrer Adresse und mit dem Vermerk „Lebenskünstler Baum“.
Frankieren Sie ihn mit 0,77 € und schicken Sie ihn in einem normalen Briefkuvert an:

WDR Fernsehen

Quarks & Co

Stichwort: Titel der Sendung, z. B. „Lebenskünstler Baum“

50612 Köln

Wenn Sie mehrere Scripts gleichzeitig bestellen wollen, geben Sie als Stichwort „Sammelbestellung“ an und legen einen Zettel bei, der die gewünschten Hefte auflistet. Je C5-Umschlag und 0,77 € Porto können bis zu 10 Scripts verschickt werden.

