Humanistische Union

RV München
Arbeitskreis
"Gläserner Mensch"

Die alltäglichen Daten-Spuren

Bankautomat, Handy, Payback-Karte: Wo wir an einem ganz normalen Tag überall Spuren hinterlassen

Drei Merkmale genügen meist, um eine Person eindeutig zu identifizieren: Name, Wohnort, Geburtsdatum. Tag für Tag geben wir ahnungs- oder bedenkenlos viele Daten weiter. Jeder Bundesbürger über 18 Jahre ist außer bei den Behörden noch in durchschnittlich 52 kommerziellen Datenbanken erfasst. Seit dem 11. September 2001 verschiebt sich die Balance zwischen Schutz der Privatsphäre einerseits und Sicherheits- und kommerziellen Interessen andererseits. Gesetze zum Datenschutz werden verwässert, Daten zwischen Firmen, Geheimdiensten und Polizei verstärkt ausgetauscht, Lauschangriff und biometrische Verfahren vermehrt eingesetzt.

Welche Spuren hinterlässt ein Durchschnittsbürger täglich? Nennen wir ihn X. und verfolgen seinen Datenschatten. Der Normaldeutsche steht laut Statistik um 6.23Uhr auf. Da seine Wohnung noch nicht über eine medizinische Analysestation verfügt, mit der japanische Forscher Gesundheitswerte etwa aus dem Morgenurin ablesen wollen, bleibt die erste Stunde des Tages datenfrei.

7.30 Uhr: X. verlässt seine Münchner Wohnung und kommt an der Videoüberwachungskamera des Nachbarhauses, sowie bei Betreten des U-Bahnhofes an Kameras vorbei.

In Münchner U-Bahnhöfen hängen 650 Videokameras, an der Station Giselastraße, einem bekannten Drogenumschlagplatz, sind zwei Testmodelle zoom- und schwenkbar. In der Leitstelle am Marienplatz beobachten drei Mitarbeiter die Aufnahmen. Jedes Kamerabild ist etwa sieben Sekunden zu sehen. Bei Straftaten oder zum Schutz der Sicherheit wird ein Videogerät eingeschaltet. Die Bänder können nur von den Vorgesetzten mitgenommen werden, löschen können die Mitarbeiter selbst.

Videokameras suggerieren Sicherheit. In ganz Deutschland gibt es etwa 400000 davon, vor Banken, Versicherungen, Supermärkten, Gerichten, Polizeiwachen. Immer öfter hängen sie auch vor privaten Wohnanlagen. Kommunen überwachen verstärkt öffentliche Plätze und große Straßenkreuzungen in der Hoffnung, Straftaten wie Diebstahl oder Drogenverkauf zu unterbinden. Ob dies gelingt, darüber legen die Behörden aber kaum Rechenschaft ab. Zulässig sind solche personenbezogenen Aufnahmen an Kriminalitätsschwerpunkten. Wieso in München etwa Stachus und Marienplatz überwacht werden, erschließt sich daraus nicht. Dies seien alte Verkehrsüberwachungskameras, sagt Bayerns Datenschutzbeauftragter Reinhard Vetter. Die Speicherzeiten der Bänder variieren nach Bundesland, in Bayern beträgt die Frist zwei Monate, in Baden-Württemberg sind es zwei Tage.

In England haben Wissenschaftler der Universität Hull herausgefunden, dass Überwachungskameras oft unsauber eingesetzt werden, wenn Menschen sie steuern: um Frauen nachzuspionieren etwa oder politische Demonstranten zu überwachen. Zudem können die Bänder in falsche Hände geraten. Im Internet findet sich ein britisches Video mit Namen "Caught in the Act", eine Sammlung von Sexszenen und Straftaten an öffentlichen Orten, aufgenommen von Überwachungskameras.

8.00 Uhr: X. betritt das Firmengebäude, sein Gesicht wird vom Computer mit einer Aufnahme aus der Datenbank verglichen.

Ein solcher "elektronischer Pförtner" soll Sicherheit erzeugen, etwa in sensiblen Rechenzentren oder Druckereien. Daneben wird das Scannen von Fingerabdrücken, Augen oder der Stimme erprobt. Doch besonders die Gesichtserkennung kann auch anders genutzt werden: zur automatischen Fahndung. Manche Flughäfen - in den USA sind es Logan Airport in Boston und Oakland International Airport in Kalifornien - testen Software, die Gesichter scannt, wenn Passagiere durch die Kontrolle gehen. Diese werden mit digitalen Aufnahmen aus Datenbanken der Geheimdienste verglichen. Ziel: Terrorfahndung. Ähnliches wird im

Ferienort Tampa in Florida erprobt. Manche der Systeme können angeblich 15 Gesichter pro Sekunde scannen. Probleme bereiten Sonnenbrillen, Hüte oder ein breites Lachen.

8.44 Uhr: An seinem Büro-PC löscht X. einen privaten Brief.

Durch den Befehl verschwindet nicht der Text selbst, sondern nur der Pfad zum Text auf der Festplatte. Die Datei ist nur aus allen Verzeichnissen verschwunden, die Wörter und Sätze liegen noch dort. Ihr Inhalt wird erst gelöscht, wenn an die Stelle des Textes andere Daten kopiert werden. Programme wie EnCase der Firma Guidance Software und PS Smart Cleaner von Pantera Soft können die gelöschten Daten wiederfinden. Diese sind oft in Straf- und Steuerprozessen interessant, wenn Beschuldigte schnell - aber auf untaugliche Weise - Beweismaterial vernichten wollten. Wer wirklich alles endgültig löschen will, muss ein Programm nutzen, das zum Beispiel ständig den freien Platz überschreibt.

11.00 Uhr: X. schreibt eine E-Mail an einen Freund.

Jede gesendete E-Mail läuft über einen Austausch-Server seiner Firma, der mehrere Kopien erstellt: im "X.-gesendet"-Ordner sowie im Backup für X.'s Mail-Verzeichnis, welches automatisch am Ende jedes Tages erstellt und auf Band archiviert wird. Diese Aufzeichnungen können später jederzeit überprüft und bei etwaigen Prozessen als Beweismaterial zugelassen werden. Bei manchen Firmen wird nicht-geschäftliche Post herausgefiltert. Wenn X. versucht, seine Nachricht zu löschen, erzeugt er eine weitere Kopie, die in seinem "Papierkorb" auftaucht.

Jede E-Mail kann auf dem Weg, an jedem einzelnen Knotenpunkt, den sie bis zum Empfänger passiert, abgefangen werden. Sie gleicht dabei eher einer Postkarte als einem Brief. "Hier ist nichts abgesichert", sagt Bernd Radig, Informatikprofessor und Datenschutzbeauftragter an der Technischen Universität München. Viele Experten raten daher zur Verschlüsselung, die einem zugeklebten Umschlag entspricht. Doch gerade in Firmen darf der einzelne Angestellte nötige Programme nur selten installieren.

Über die Knotenpunkte der Service-Provider, die den Internetverkehr ausführen, können sich auch die jeweiligen Regierungen und Polizeibehörden Zugriff verschaffen. Nach dem 11. September 2001 sind in Deutschland und den USA Gesetze für die Überwachung verabschiedet worden. Der USA Patriot Act verpflichtet Internet-Provider, individuelle Daten über das Verhalten ihrer Nutzer an Ermittlungsbehörden weiterzugeben, wenn nur eine polizeiliche Vorladung vorliegt, und nicht erst beim richterlichen Beschluss. Freigegeben werden dann: in Suchmaschinen eingegebene Befehle, besuchte Seiten, Zeit und Verweildauer, im Falle von Kreditkarteneinsatz auch Daten über E-Commerce.

11.40 Uhr : X. telefoniert aus dem Büro mit einem Kollegen.

Wenn der Arbeitgeber einen Einzelverbindungsnachweis erstellt, taucht darin auch dieses Gespräch auf. Die Liste kann elektronisch ausgewertet werden. Im Laufe der Zeit werden sämtliche Telefonnummern aus dem Freundes- und Kollegenkreis bekannt.

12.15 Uhr: X. ruft eine Freundin in Augsburg von seinem Handy an und verabredet sich für den Abend.

Ein Handy arbeitet wie ein Radio-Sender und -Empfänger, der ständig mit festen Sendemasten in Verbindung steht. Bei jeder Bewegung von X. beim Telefonieren, wird das Gespräch von einem Sendemasten zum nächsten übergeben, ohne dass X. es merkt. So ist sein Standort gut zu verfolgen. Wer sein Handy angeschaltet lässt, gibt ein perfektes Bewegungsprofil weiter, selbst wenn er nicht telefoniert.

Das Handy kann auch abgehört werden. Bei normalen Gesprächen muss jemand mithören, um Wichtiges von Unwichtigem zu unterscheiden. SMS-Texte lassen sich automatisch auswerten. Der Fortschritt in der Spracherkennung wird sicherlich bald auch bei der Überwachungstechnik nützlich sein.

12.15 Uhr: X. bezahlt in der Kantine mit der Firmenchipkarte.

Alles, was er isst oder trinkt, kann erfasst, auffällige Konsum- oder Trinkgewohnheiten beobachtet werden.

12.43 Uhr: X. geht zum Geldautomaten am Marienplatz.

Seine Anfrage geht an einen Zentralrechner, der in Frankfurt bei der Gesellschaft für Zahlungssysteme GZS steht. Dort werden der Ort des Automaten, der abgehobenen Betrag, Tag und Uhrzeit protokolliert. Das Abheben wird online autorisiert, die PIN-Nummer überprüft. Aus Haftungsgründen, wie man bei den Banken sagt, werden viele Terminals zusätzlich videoüberwacht, um nachweisen zu können, dass ein Kunde Geld aus diesem Automaten erhalten hat, falls es später Beschwerden gibt. Es gibt Geräte mit integrierten Kameras, aber auch solche, die den ganzen Raum erfassen. Auch die beiden New-York-Attentäter Mohammed Atta und Abdulaziz Alomari wurden gefilmt, als sie an Bankautomaten in Portland, Maine am Abend vor dem Anschlag Geld abhoben.

13:00 Uhr: X. kauft sich ein Hemd und zahlt mit Kreditkarte.

Beim Einsatz des Plastikgeldes werden außer der Warengruppe auch Unregelmäßigkeiten beim Gebrauch von Kreditkarten erfasst. Wenn zum Beispiel ein Kunde, der immer nur Bekleidung oder Benzin mit Karte bezahlt hat, plötzlich teuren Schmuck damit kauft, schlägt das System Alarm. Wenn fast gleichzeitig Beträge in Berlin und New York abgebucht werden, kann man davon ausgehen, dass jemand den Sicherheitscode geknackt hat.

Das Kreditunternehmen erhält so Informationen zur Person, über Arbeitgeber, Konsumausgaben, Reisen, Geschäftsbeziehungen und Vermögensverhältnisse des Herrn X. Das Bundesdatenschutzgesetz wie auch das Bankgeheimnis erlauben diese Daten nur für Zahlungstransaktionen zu speichern und zu übermitteln sowie intern zu nutzen.

13.10 Uhr: X. holt sich im Kaufhaus noch Lebensmittel und lässt sich dabei Rabattpunkte gutschreiben.

In Deutschland gibt es bereits 50 Millionen Kundenkarten wie Payback oder Happy Digits. Die elektronische Rabattmarke sammelt Daten über Kaufgewohnheiten, welche die Kaufhäuser mit Name, Adresse, Telefonnummer und Personalausweisnummer verbinden können. Manche Konzerne behaupten, das System sei dazu da, gefragte Produkte

stets vorrätig zu haben. Die Daten würden nicht verkauft oder sonstwie weitergegeben.

Tatsächlich erfassen moderne High-Tech-Kassen, welche Waren zu welchen Uhrzeiten häufig gekauft werden. Die Regale werden entsprechend befüllt. Was Herr X. gern kauft, verrät aber erst die Kundenkarte. Sollte er etwa mehrfach Windeln erworben haben, darf man davon ausgehen, dass er ein kleines Kind hat. Also schickt man ihm schon mal Werbung für alle möglichen Babyartikel zu. Wenn Herr X. nicht dagegen widersprochen hat, dass seine Daten anonym ausgewertet werden dürfen, ist dies mit dem Datenschutz vereinbar. "Alles, was der Käufer an Spuren hinterlässt, wird im gesetzlich erlaubten Rahmen gnadenlos ausgenutzt", sagt der Datenschützer Bernd Radig. "Illegalität können sich Konzerne nicht leisten, der Imageverlust wäre zu groß."

Seit dem 11. September häufen sich vorwiegend in den USA Anfragen von Behörden an Handelskonzerne. Dem amerikanischen Magazin Popular Science sagte Larry Ponemon vom Privacy Council, er sei von einer großen Supermarktkette beauftragt worden, die Übergabe von Kauflisten von Kunden mit spezifischem ethnischen Hintergrund an die Behörden zu überwachen. Sie wollten, so Ponemon, ein Profil der "Essgewohnheiten von Terroristen" erstellen.

16.15 Uhr: Das ständige Arbeiten am PC verursacht bei X. Rückenschmerzen. Er hat einen Termin beim Orthopäden.

Bei Mitgliedern gesetzlicher Krankenversicherungen rechnet der Arzt seine Leistungen über die Versichertenkarte ab. Dort sind nur Verwaltungsdaten, aber keine medizinische Angaben gespeichert. Diese gehen vom Arzt nur an die zuständige Kassenärztliche Vereinigung.

Diese darf sie den Kassen nur so übermitteln, dass keinem Versicherten seine Leiden zugeordnet werden können. Hospitäler rechnen direkt mit den Kassen ab. Hätte Herr X. eine chronische und damit behandlungsintensive Erkrankung wie Diabetes, die im Rahmen des neuen Disease-Management-Programms erfasst wird, könnte seine Krankenkasse ein vollständiges Gesundheitsprofil über ihn erstellen. Der Datenschutz wird auch Thema, wenn die derzeit diskutierte Online-Krankenakte kommt. Dann nämlich werden medizinische Daten einer Person auf ihrer Karte gespeichert.

16.50 Uhr: X. reicht das Salbenrezept vom Orthopäden in der Apotheke ein.

Die meisten Apotheken rechnen heute mit den Krankenkassen nicht mehr selbst ab, sondern nutzen die Angebote von Apothekenrechenzentren. Dort werden teilweise die Patientendaten einzelner Apotheken ausgewertet, auf CD gebrannt und an die Apotheken zurück verkauft. X. kann so im Apothekenrechner als Kunde katalogisiert werden. Sein Apotheker kann auch nach Krankheiten in seinem Stadtviertel fahnden.

17.10 Uhr: X. 's Bahncard ist abgelaufen, er besorgt sich eine neue und erkundigt sich nach dem neuen Bonusprogramm BahnComfort.

Seit 2002 versucht die Bahn, an den Erfolg der Meilenprogramme der Fluglinien anzuknüpfen. Wer sich bei BahnComfort qualifiziert, darf etwa in die DB-Lounges an großen Bahnhöfen, die Bahn erfährt seine Reisedaten schon beim Versuch, diesen Sonderstatus zu erwerben.

Ähnlich funktioniert das Miles&More-Programm der Lufthansa, bei dem X. auch eine Gutschrift für Bahn-Fahrten auf ICE-Sprinter-Strecken und dem Metropolitan zwischen Hamburg und Köln bekäme, ebenso wie für Mietwagen- und Hotelbuchungen. Sein Bewegungsprofil oder seine Urlaubsvorlieben verrät er nebenbei. Und wie man bei der Flugaffäre mancher Bundestagsabgeordneten kürzlich gesehen hat, scheitert Datenschutz oft nicht an technischen Hürden, sondern an menschlichen Fehlern. Selbst verschlüsselte Daten müssen irgendwo gelesen werden.

17.30 Uhr: X. fährt mit seinem Auto Richtung Augsburg los. Da er das Restaurant, in dem seine Freundin ihn erwartet, nicht kennt, gibt er die Zieladresse in sein Navigationssystem ein.

Es nutzt ein System von 24 Satelliten, um den aktuellen Standort zu ermitteln und die Route zu überwachen. Technisch ist es kein Problem, den Standort über einen Sender oder ein Handy zu übermitteln. In den USA nutzen das manche Autofahrer, um Informationen über Staus oder Restaurants am Wegesrand abzurufen. Autovermieter versuchen so auch den Diebstahl von Luxuskarossen zu verhindern, deren Motor dann kurz vor der Grenze einfach ausgeht. Beim zu schnellen Fahren erheben andere auch eigene Strafen. Das dafür benutzte Programm AirIQ kann zudem ein Online-Profil der Fahrten erstellen.

Wird die Gebühr für Mautstellen auf Autobahnen elektronisch beim Vorbeifahren eingezogen, wie etwa in den USA möglich, fallen personenbezogene Daten an. In Deutschland wird es konkret bei der geplanten Lkw-Maut. Dazu soll das System mit GPS und einer Einheit betrieben werden, die über Mobilfunk die Maut abrechnet. Die zum Ende des Jahres 2003 für den Einsatz vorgesehene Technik ermöglicht es, exakte Bewegungsprofile zu erstellen. Damit könnten Systembetreiber und andere nachvollziehen, wer wann wohin gefahren ist. Natürlich auch, wie schnell. Datenschützer fordern deshalb, weiterhin Barzahlung zu ermöglichen.

Statistisch gesehen geht X. um 22.47 Uhr ins Bett. Falls keine Videokamera im Schlafzimmer installiert ist, bleibt zumindest dieser Bereich privat.

Dieser Text basiert auf einer Arbeit von Hubert Filser.

München im Juli 2003

HUMANISTISCHE UNION e.V.
Regionalverband München-Südbayern
Paul-Hey-Straße 18, D -82131 Gauting
Tel. 089/ 850 33 63
Fax 089/89 30 50 56
humanistische-union@Link-M.de
www.humanistische-union.de/suedbayern