2006/46 Dossier

https://jungle.world/artikel/2006/46/vergesst-big-brother

Vergesst Big Brother!

Von **Ralf Hutter**

Über Auskunfteien, Spuren im Netz und das so genannte Scoring. Daten und Fakten über staatliche und private Datensammler, gesammelt von Ralf Hutter

Überwachung ist ein großes Thema. Der Präventionsstaat behandelt die in seinem Herrschaftsbereich lebenden Einzelnen wieder offener als Sicherheitsrisiko. Ihre Handlungen sollen, so gut es geht, möglichst oft und möglichst umfassend dokumentiert werden. Die manifeste Staatsgewalt in all ihrer symbolischen, organisatorischen, technischen und auch menschlich-physischen Form täuscht dabei aber leicht darüber hinweg, dass es einen anderen Bereich gibt, in dem die Individuen stärker und subtiler einer ständigen Durchleuchtung ausgesetzt sind.

Diesen Bereich nennt man die Geschäftswelt. In ihr sind wir nicht unbedingt ein potenzielles Risiko, sondern haben manchmal einen hohen materiellen Wert. Nicht nur Vorwissen und Vorbeugung spielen dort eine Rolle, sondern auch Gewinnmaximierung durch die möglichst umfassende Ausbeutung der aus einem Geschäftsvertrag erwachsenden Beziehungen zu einem bestimmten Menschen.

So etwas erfordert eine weiter gehende und genauere Informationsverarbeitung, als sie ein Staat in der Regel leistet. Hier rücken Fakten in den Vordergrund, die für sich genommen nicht unbedingt wichtig und schützens- bzw. überwachenswert erscheinen: Wohnadresse, Anzahl der Kinder, Konten und Kreditkarten, (Hoch-)Schulabschluss oder der Wille, ein Auto zu kaufen oder zu verkaufen.

Diese Daten haben erst mal nichts gemeinsam, außer dass sie sich auf dieselbe Person beziehen und etwas über sie aussagen. So wie auch die Branche und Dauer des Lohnarbeitsverhältnisses, die Anzahl der Wohnungswechsel oder die Konfession. Da all diese Daten irgendwo digitalisiert vorliegen, ergeben sich Möglichkeiten der Verknüpfung und Auswertung.

#

Altbekannte Datensammlungen, aus denen Rückschlüsse auf Privat- oder Geschäftspersonen gezogen werden können, sind Telefonbücher und Branchenverzeichnisse. Aus den darin enthaltenen Informationen darf man sich aber nicht

zu Werbezwecken bedienen. Anders ist das bei Adresslisten privatwirtschaftlicher Stellen. Diese Daten werden schon seit langem für Direktmarketingkampagnen benutzt, d.h. für Postsendungen, in denen die Zielperson direkt angesprochen wird und auch eine Antwortmöglichkeit erhält.

Für ihre Informationsbeschaffung haben die Listenhändler verschiedene Quellen. Daten können im Rahmen von Gewinnspielen, Bonusprogrammen, des Erwerbs von Kundenkarten oder bei ganz normalen Vertragsabschlüssen zu Werbezwecken freigegeben worden sein. Die Versandhäuser Quelle und Otto vermieten alle Profile aus ihren Datenbanken zum einmaligen Gebrauch weiter, man kann die Daten zu Werbezwecken mieten, bekommt sie aber nicht selbst zu sehen. Denn das wäre rechtswidrig.

Postadress, ein Gemeinschaftsunternehmen der Deutschen Post AG und der Bertelsmann AG, beschäftigt 60 Leute, die alle bei der Post eingehenden Adressänderungen und Todesfälle verzeichnen und inte-ressier-ten Firmen zugänglich machen. Dabei werden die Adressen mit weiteren Daten angereichert (z.B. Informationen zur neuen Wohngegend). Auf **www.listbroker.com** werden 1,6 Milliarden »consumer, business and email addresses« angeboten.

#

Um zu verstehen, wie aus vielen Daten viel Geld gemacht wird, müssen wir uns dorthin begeben, wo Begriffe wie »Forderungsmanagement«, »Geomarketing«, »Adressenpotenzial«, »Data Mining«, »Lifestyle-Adressen«, »Kaufkraftklassen«, »Kundenlebenszyklus« und »Know your Customer« eine Rolle spielen.

Die wirtschaftliche Relevanz von Namen und Adressen lässt sich deutlich steigern, wenn sie mit Zusatzinformationen einhergehen. Das sind Informationen, die sich nicht auf bloße objektive Daten beschränken, sondern die zum einen die Bedeutung dieser Daten in einem größeren Zusammenhang veranschaulichen und zum anderen dadurch genauere Rückschlüsse auf die Angepeilten erlauben. Gefragt sind also nicht Datenhändler, sondern Unternehmen, die in großem Ausmaß alle nur möglichen objektiven Merkmale der Lebenslage möglichst vieler Menschen sammeln, sie statistisch auswerten, um dann die Dienstleistung anbieten zu können, jeden Menschen gemäß seiner individuellen Lebensumstände einer Vergleichsgruppe zuzuordnen.

Diese Gruppe wird anhand der eingangs erwähnten Merkmale konstruiert. Die Informationen zu den Individuen dieser Gruppe werden mit spezieller Computersoft-ware bearbeitet, um Statistiken für verschiedene Fragestellungen zu bekommen. Daran interessiert sind Kreditinstitute, Versicherungen, Telekommunikationsanbieter, Versandhäuser etc., die gerne im Voraus wüssten, was sie in einer Vertragsbeziehung von einem bestimmten Menschen zu erwarten haben.

Für diese Personen können nun branchenspezifische Scores errechnet werden, Punktzahlen, die die »Attraktivität« eines Subjektes beschreiben sollen. Es geht um Faktoren wie: einen Kredit nicht regelmäßig abzuzahlen, Rechnungen nicht pünktlich zu

begleichen oder Waren zu beanstanden. Die Scores werden wie Wahrscheinlichkeiten behandelt, Wahrscheinlichkeiten, die nichts mit den tatsächlichen Einstellungen und Handlungen der Person zu tun haben müssen.

#

Das Scoring findet in der Regel extern statt, d.h. eine Bank oder Versicherung übergibt die Daten des zu Scorenden samt allen weiteren verfügbaren Daten aus seinen Konsumentenverträgen an einen Dienstleister. Das ist legal, da das Unternehmen angeblich nur anonyme Erfahrungswerte gewinnen will. Unzulässig hingegen ist es, vom Score Vertragsbedingungen oder einen Vertrag selbst abhängig zu machen. Das Bundesdatenschutzgesetz verbietet automatisierte Einzelentscheidungen. Der Score soll nur eine Entscheidungshilfe sein. Es gibt aber Anhaltspunkte dafür, dass sehr wohl Vertragsinhalte von ihm abhängen. Nach Ansicht der Datenschutzbehörden könnte das daran liegen, dass das Bearbeitungspersonal in Banken etc. sich an den Score gebunden fühlt, oder schlicht daran, dass es sich aus Zeitgründen an den Score hält. Nachweisen lässt sich weder die eine noch die andere These.

Unzulässig ist es auch, Daten aus branchenfremden Vertragsverhältnissen einer Person zu verwenden, oder Daten zu Dritten aus der persönlichen Umgebung (Verwandte) wie auch persönliche Daten, die mit dem Vertragsverhältnis nichts zu tun haben.

Wer aber bestimmt, was relevante Daten sind? Thilo Weichert, unabhängiger Landesbeauftragter für den Datenschutz in Schleswig-Holstein, weist darauf hin, dass die Relevanz wissenschaftlich und nach rechtlichen Aspekten beurteilt werden müsse. Die Voraussetzung sei allerdings, dass sowohl die Berechnung eines Score als auch seine Bedeutung für ein bestimmtes Vertragsverhältnis transparent seien, wogegen sich die entsprechenden Scoring-Dienstleister lange gesperrt hätten. Derzeit fänden deswegen Gespräche mit den Aufsichtsbehörden statt.

Weichert bestreitet nicht die Aussagekraft von Statistiken oder das Recht von Unternehmen, ihre wirtschaftlichen Interessen zu wahren. Er hält nur die bisherige Praxis des Scoring für diskriminierend, da z.B. soziodemographische Daten nichts über die »Bonität« aussagten und das Einbeziehen persönlicher Daten schlicht rechtswidrig sei.

#

Nun stellt sich die Frage, inwieweit privatwirtschaftlichen Akteuren in dieser Hinsicht beizukommen ist. Sie behaupteten lange, der Score sei wegen der Vielzahl von allgemeinen Daten gar nicht personenbezogen, eine Ansicht, die mittlerweile auf verlorenem Posten steht. Von der Politik wurde das Thema lange nicht aufgegriffen, mittlerweile prüft die Bundesregierung, ob Gesetzeslücken (insbesondere zu Auskunfteien und Datenhändlern) geschlossen werden können.

Weichert meint, die Gesetze seien ausreichend, es mangele nur an ihrer Anwendung durch die Aufsichtsbehörden, was auch mit deren Ausstattung zusammenhänge. Er stellt sich einen Datenschutz mit den Mitteln der Technik vor. Alle Institutionen, die Scorings

durchführen, müssten zur besseren Nachvollziehbar- und Überprüfbarkeit durch die Datenschutzbehörde offen legen und protokollieren, welche Daten mit welcher Wertigkeit in die Berechnung eingehen. Die verwendete Technik müsste darüber hinaus veränderbar sein.

#

Sehen wir uns einige dieser Institutionen, die eine Grauzone als Freiraum nutzen, genauer an.

Die wohl bekannteste ist die Schufa (früher e.V., seit 2000 Holding AG), eine Mischung aus Auskunftei und Scoring-Anbieter, die von der Kredit gebenden Wirtschaft getragen wird. Die an die Schufa durch eine Art Mitgliedsbeitrag angeschlossenen Unternehmen liefern ihr Daten über Dritte (die vorher eingewilligt haben müssen) aus ihrer Geschäftstätigkeit und erhalten dafür gegen Gebühren Daten über Einzelpersonen oder gewerbliche Geschäftspartner.

Im Jahr 2005 verfügte die Schufa über 384 Millionen Daten von 63 Millionen Menschen und erteilte 77 Millionen Auskünfte, von denen 53 Prozent mit der Berechnung eines Score verbunden waren.

Einerseits wirkt die Schufa moderat angesichts der Tatsache, dass sie für ihre Auskünfte weder mikrogeografische Daten (Lebenshaltungskosten, Sozialstruktur, Scheidungsrate, Erwerbslosenrate) verarbeitet noch das Einwohnermeldeamt heranzieht. Sie darf auch weder Angaben über Beschäftigungs- noch über Vermögensverhältnisse sammeln.

Andererseits speichert sie drei Jahre lang so genannte Negativmerkmale (ohne dass es sie interessieren würde, ob der zu Grunde liegende Tatbestand noch erfüllt ist), titulierte Forderungen wie Urteile und Vollstreckungsbescheide sogar 30 Jahre lang. Sie hat Einblick in die Schuldnerverzeichnisse der Amtsgerichte, was das Bundesdatenschutzgesetz erlaubt. Darüber hinaus macht sie sich daran, auch jenseits des Kreditgewerbes ihre Geschäftstätigkeit zu erhöhen. Sie arbeitet eng mit der Wohnungs- , der Versicherungswirtschaft und mit Inkassounternehmen zusammen – an diese verkauft sie Adressdaten.

#

Mehr zu bieten hat die Schober Informa-tion Group aus Ditzingen bei Stuttgart, die auch Scorings durchführt und nach ihrer Selbstdarstellung »Europas führender Provider von Adressen, Daten und Database-Systemen« ist. Sie bietet 5,5 Millionen Firmenadressen mit 100 Millionen Zusatzinformationen aus Deutschland, Österreich und der Schweiz; 50 Millionen Privatadressen aus Deutschland mit zehn Milliarden Zusatzinformationen; 960 Millionen »Consumer«- und 45 Millionen »Business«-Adressen aus Europa und den USA. Das ergibt nach eigenen Angaben 5 000 Direktmarketingaktionen jährlich, die Firma wirbt außerdem damit, das »Adresspotenzial« bestimmter Länder angeben zu können.

Was aber sind das für Zusatzinformationen? Schober verschickt zweimal jährlich Millionen

von Fragebögen an deutsche Haus-halte, um Konsumgewohnheiten (»Lifestyledaten«) möglichst genau zu ergründen. In diesen Fragebögen können Dritte auch selbst formulierte Fragen platzieren lassen, um mit den daraus gewonnenen Erkenntnissen ihre Warenproben gezielt zu verschicken. So etwas wird »Selective Sampling« genannt. In Schobers »Lifestyle MarketBase« werden »fünf Millionen Konsumenten mit konkreten Interessen und Kaufabsichten, verknüpft mit hochwertigen Adressen«, geführt; Informationen über 3,5 Millionen Haushalte – das entspricht fast zehn Prozent aller deutschen Haushalte – liegen vor; eine Aufteilung in 5 000 Zielgruppen ist möglich.

Daneben gibt es noch die »eMarketBase« mit »über sieben Millionen privaten E-Mail-Adressen mit Einwilligung für E-Mail-Werbung« und die »Geo MarketBase«. Sie enthält soziodemographische Daten, Informationen zu regionalen Haushaltsstrukturen (u.a. den »Ausländeranteil«) und Gebäudeinformationen, denn Schober hat fast alle Häuser Deutschlands selbst bewertet. Dabei stützt sich die Firma vor allem auf die Arbeit des Tochterunternehmens Infas Geodaten GmbH, das »geographische Informations- und Managementlösungen« anbietet.

Kunden können die Dienstleistung des Geomarketing in Anspruch nehmen, bei der Marktinformationen, geografische Daten und unternehmenseigene Zahlen zu aussagekräftigen Karten zusammengeführt werden. Räumliche Zusammenhänge und Zeitreihenanalysen können bis auf Wahlbezirksebene bestimmt werden, teilweise sogar bis auf einzelne Häuser.

#

Wer sich nun fragt, wie es möglich ist, die über 19 Millionen in Deutschland stehenden Gebäude einzeln zu bewerten, sei an CityServer erinnert. Der Verlag Tele-Info stellte Ende der neunziger Jahre unter diesem Namen eine Datenbank zusammen, die digitalisierte Karten mit Bildmaterial verknüpfen sollte. Dafür fuhren mit spezieller Technik ausgerüstete Kleintransporter durch die Straßen aller größeren oder touristisch interessanten deutschen Städte, machten digitale Aufnahmen der Straßenzüge und verknüpften diese durch GPS-Ortung mit den dazugehörigen Werten von Meereshöhe, Längen- und Breitengraden.

Trotz eines separat vertriebenen Telefonnummernverzeichnisses, das die ungefähre Lage des zu einer gesuchten Nummer gehörenden Anschlusses auf einem Stadtplan anzeigte (und für einige Städte sogar Bilder der Straßenansicht lieferte), ist das alles legal, weil Bilder keiner konkreten Anschrift zuzuordnen sind. Als Zweck wurde u.a. die Nützlichkeit für Verkehrs- und Rettungsleitsysteme und für (Stadt-)Planungs-systeme angegeben.

In letzter Zeit ist es still geworden um CityServer, der Verlag tritt mittlerweile nicht mehr in Erscheinung. Unklar ist, ob das Ziel erreicht wurde, jede deutsche Stadt mit einer Bevölkerung von über 20 000 Menschen zu erfassen. Fakt ist jedenfalls, dass die Technik erfolgreich exportiert wurde. So bietet das Tochterunternehmen Imageos die CityServer-Dienste in den USA und Kanada an.

Das kostenlose Programm Google Earth zeigt ebenfalls Straßenansichten aus allen Ecken

des Planeten bei der Suchanfrage für die entsprechende Adresse. Gegen eine Jahresgebühr von 400 US-Dollar werden weitere Dienstleistungen ergänzt, darunter auch die Anreicherung der Karten mit externen (z.B. demografischen, geologischen und Gebäude-)Daten. Nicht nur die Bau-, Immobilien-, Architektur- und Überwachungsbranchen haben etwas von den virtuellen Flügen über Straßen, Dächer und Brachland, bei denen genaue Abmessungen ersichtlich sind. Versicherungen werden mit der Erstellung »der Risikomuster eines geografischen Gebiets« gelockt, und gegenüber Militär und Geheimdiensten werden offen die Vorzüge der hochwertigen und schnellen Luftbilder für Übung wie Ernstfall angepriesen.

Fairerweise wird sogar die Gegenseite angesprochen: NGO helfe die kostenpflichtige Variante u.a. bei der »Visualisierung der Armutsrate« und der »Linderung von Kriegen/Konflikten«.

#

Noch einmal zum Scoring: Ein weiteres Unternehmen in diesem Bereich ist CEG, ein Tochterunternehmen der Creditreform AG. Dort warten 49 Millionen Daten zu einem Fünftel aller Deutschen (inkl. 18 Millionen personenbezogener Negativmerkmale) und eine eigene Umzugsdatenbank auf Kundschaft. Neben Scoring ist auch Monitoring möglich. CEG-Alert bietet Unternehmen die Möglichkeit, über »neue Ereignisse« bei der Kundschaft sofort informiert zu werden.

Verborgene Potenziale in der bestehenden Kundschaft zu entdecken, behauptet die Informa GmbH, ein Joint-Venture-Unternehmen von Schober und InFoScore. Die Firma führt ebenfalls nicht nur Scorings durch, sondern vetreibt auch Software, die den Zugriff auf Datenbanken verbessert, verbunden mit der Einbeziehung externer Daten (die bei Schober reichlich vorhanden sind). Ähnlich arbeitet Bürgel, das neben Informationen zu 36 Millionen Privatpersonen in Deutschland nicht nur zwölf Millionen Privat- und 3,6 Millionen Un-ter-neh-mens-adressen anbietet (jeweils »bonitätsgeprüft«), sondern auch Datenrationalisierung und -anreicherung. 15 Millionen »europäische Business-Adressen« stehen dort ebenfalls zur Verfügung.

Weitere Anbieter sind Dun & Bradstreet, Deltavista, Coface, das Telekomtochterunternehmen SolvenTec und ein Joint Venture des Bertelsmannablegers Arvato mit der bereits erwähnten Firma InFoScore. Das Internet-Angebot ABIT e.POS führt die Services mehrerer dieser Unternehmen zusammen. Die ABIT AG ist ansonsten auf Forderungsmanagement spezialisiert. Sie versucht z.B., den Überblick über laufende Insolvenzverfahren zu haben.

#

Die Sammelwut hat nicht nur diese Art von Unternehmen gepackt. Bis hin zum Einzelhandel werden immer häufiger Daten »einfach so« gesammelt – sie sind eben Geld wert. Selbst bei Wohnungsmietverträgen, wo zur Absicherung sowieso eine Kaution vereinbart wird, soll es bereits zu umfassenderen Datengesuchen gekommen sein. Die Vermieterschutzgemeinschaft Vpaz führt eine Datenbank über Mieter, die einmal

Zahlungsprobleme hatten, verbunden mit Erkenntnissen aus der »allgemeinen Schuldnerliste«. Die Versicherungswirtschaft betreibt die Datenbank »HIS«, in die Leute kommen, die aus irgendwelchen Gründen eine bestimmte Anzahl von Negativpunkten erhalten haben, und die den Kontakt zwischen den Versicherungen vermittelt, wenn eine Informationen zu den Negativpunkten einer bestimmten Person von der anderen braucht. Selbst in der gesetzlichen Krankenversicherung ist die Einführung von Scoring-Methoden geplant.

#

Die allerorts digitalisiert anfallenden Daten, das Internet, spezielle Computerprogramme etc. machen es allen, die damit umgehen können, möglich, ein Höchstmaß an Informationen auszuwerten. Das geht mitunter schnell. So wird von langen Wartezeiten in Hotline-Warteschleifen berichtet und von ungünstigen Zahlungsbedingungen nach Eingabe einer Lieferadresse in ein Onlinebestellformular – vermutlich, weil die Telefonnummer bzw. Adresse softwaregesteuert einer Gegend zugeordnet wurde, in der ein finanziell nicht gut gestelltes Klientel vermutet wird.

Außerdem ist die Unachtsamkeit groß. Wie wichtig es ist, einen sparsamen und kritischen Umgang mit den eigenen Daten zu praktizieren, ist vielen Menschen nicht bewusst. So rückt man im Austausch für kleine (oder unnötige) Annehmlichkeiten wie Gewinnspiele und Bonusprogramme mit persönlichen Angaben heraus. Der Bundesbeauftragte für den Datenschutz, Peter Schaar, monierte bereits im April 2005, dass aus der Angabe, die erhobenen Daten würden »zu Marketingzwecken« weiterverarbeitet, kaum ersichtlich werde, dass das Datenmaterial sowohl im Ausland als auch zu Kredit- und Personalbeurteilungen verwendet werden könnte.

#

Aus all dem wird ersichtlich, dass gerade ein zentrales Prinzip des Datenschutzes verloren zu gehen droht: das der Datenvermeidung. Schaar sieht die »eigentliche Gefahr« in der »Vernetzung und Verknüpfung« der Datenbestände, also in der Profil-er-stel-lung. Auch wenn der Datenschutz in der jüngeren Vergangenheit einige Gesetze »entschärfen« konnte, ist diese Aussage hilflos, denn nicht die Unterscheidung zwischen der Erhebung von Daten und deren Verknüpfung ist das Problem, sondern die immer umfassendere Erhebung selbst sowie die Frage, ob sie dauerhaft kontrolliert oder gar verhindert werden kann.

Der weltweit führende Internetsuchmaschinenanbieter Google protokolliert beispielsweise alle Suchanfragen (inklusive der evtl. dazugehörigen Google-Accounts) und speichert sie, wenn die entsprechenden Cookies aktiviert sind. Als das US-Justizministerium im Januar die Herausgabe von zufällig ausgewählten Verbindungsdaten verlangte – nach eigenen Angaben, um Internetfilter für Minderjährige zu testen – , konnte Google den Rechtsstreit noch gewinnen.

Das berüchtigte Gesetz »Patriot Act« erlaubt allerdings zur »Terrorabwehr« die Herausgabe solcher Daten, der Vorgang muss dann weder richterlich abgesegnet sein

noch darf er öffentlich gemacht werden. Von daher ließe sich die fadenscheinige Aktion als Einschüchterungsversuch interpretieren. Auch deutsche Strafverfolgungsbehörden bedauern sicherlich nicht die Tatsache, dass von manchen Internetprovidern unerlaubt bestimmte Daten gespeichert werden, wenn sie dann einen Zugriff darauf bekommen.

#

Vor diesem Hintergrund erscheint das immense und stetig wachsende Angebot an elektronischen Dienstleistungen gerade von Google problematisch. Verfügbar sind derzeit: eine PC-Desktop-Suchmaschine, die den kompletten Festplatteninhalt indiziert und auf einem Server speichert, damit auf die Daten von anderen Rechnern mit dem gleichen Google-Account zugegriffen werden kann; der Foto-Organizer Picasa; die webbasierte Textverarbeitung Writely; der Instant Messenger Google Talk; die Werkzeug-leiste Google Toolbar, die in Internetbrowsern benutzt werden kann und alle besuchten Webadressen an Google sendet.

Das tun auch die Softwares, die Google für beschleunigtes Surfen (Web Accelerator) oder für das Surfen und Suchen per Handy anbietet; Google News und die im Google Newsreader abonnierten Feeds versorgen mit Informationen zu den individuellen Interessensgebieten; im Calendar werden Termine gespeichert; Google Finance hilft bei der Verwaltung von Aktien; mit dem Google Page Creator werden Home-pages erstellt, mit Google AdSense die dazugehörigen Werbeanzeigen geschaltet; im Kleinanzeigenmarkt Google Base und im ebenfalls Google gehörenden »Online Community«-Portal Orkut wird das Privatleben ausgebreitet; beim Benutzen der Produktsuchmaschine Froogle, der Suchmaschine für erscheinende oder eingescannte alte Bücher, Google Print, dem Routenplaner Google Maps und dem bereits erwähnten Google Earth sammelt sich auch so einiges an Daten zu persönlichen Interessen und Aktivitäten an. Die Liste lässt sich fortsetzen.

Neueste Errungenschaften sind der On-line-Bezahldienst Gbuy und die Videoplattform YouTube; am argwöhnischsten von allen wird aber seit langem der kostenlose E-Mail-Dienst Gmail beobachtet. Der Welterfolg von Google beruht auf dem Suchalgorithmus, der effektiver als die Konkurrenz arbeitet, d.h. riesige Datenmengen werden in einzigartiger Weise geordnet und analysiert. Diese Kunst wird bei Gmail auch auf die Inhalte der ein- und ausgehenden E-Mails angewandt, die mit dem patentierten Verfahren »Content Extraction« gescannt werden. Das Patent beinhaltet übrigens auch das Erstellen von Profilen. Google wirbt damit, dass im Gmail-Postfach nur individuell zugeschnittene Werbung erscheint. Aber nicht genug damit: Google erlaubt sich, alle Daten auch nach Löschung des E-Mail-Kontos zu speichern, was in den USA nicht verboten ist.

#

Das öffentlich geäußerte Ansinnen, möglichst viel Wissen dieser Welt zusammenzutragen und auch mehr über »Sie« zu wissen (natürlich nur zu »Ihrem« Vorteil), stimmt nachdenklich. Wenn wir dann noch beachten, dass die Datenschutzbestimmungen des Unternehmens es ausdrücklich erlauben, Informationen aus den verschiedenen Diensten zusammenführen zu dürfen, ist Misstrauen angebracht.

Nicht nur, weil Google damit etwas Unliebsames anstellen könnte – das Unternehmen ist börsennotiert und persönliche Daten sind einen Haufen Geld wert –, sondern weil solche Daten einfach für staatliche, privatwirtschaftliche und kriminelle Akteure Leckerbissen sind. Kooperationen mit Elektronikherstellern und Softwarefirmen wie Hewlett-Packard, IBM, Intel, Motorola und Sun sorgen dafür, dass uns Google bald in vielen Produkten begegnen wird.

Es geht dabei nicht nur ums Ausspionieren, sondern um die Gewöhnung an bestimmte Produkte. Während gespeicherte Datenbestände (nicht nur bei Google – die Konkurrenz hat Ähnliches im Angebot, nur nicht in dem Ausmaß) ansteigen, sinkt das Datensicherheitsbewusstsein in der Bevölkerung. Denn diese Produkte und die damit verbundene Datenpreisgabe können sehr praktisch sein.

San Francisco will ein kostenloses, stadtweites Funknetzwerk für den Internetzugang (Wireless-LAN) einrichten, so wie andere US-Städte es schon haben. Als Sponsor bot sich Google an, mit folgenden Bedingungen: Alle Surfer müssten sich regis-trie-ren, was bei einem kostenlosen Angebot eigentlich nicht notwendig ist, und das Surfverhalten dürfe ein halbes Jahr lang gespeichert werden.

Lukrativ wäre für den Konzern vor allem, dass die Standorte der (evtl. mobil) Surfenden ermittelbar sind, da dabei Möglichkeiten einer individuellen, punktgenauen Werbeanzeige (also z.B. für einen Laden um die Ecke) entstehen. Entschieden ist bisher noch nichts, was auch an der Anwesenheit einer kritischen Gegenöffentlichkeit liegen dürfte. Dennoch haben solche Vorhaben Zukunft, denn die Anzahl der mobilen und internetfähigen kleinen oder großen Elektronik- und Kommunikationsgeräte wird weiter ansteigen.

#

Da in den USA seit Jahrzehnten Scorings durchgeführt werden, hat sich auch die Kritik daran etabliert und zu gesetzlichen Schutzmaßnahmen geführt. Es gibt dort sogar die Möglichkeit, die eigenen Daten selbst auf einer Homepage anzugeben und sich probehalber einen Score errechnen zu lassen. Das kann vor bösen Überraschungen schützen. Negativer sieht es in anderen Bereichen aus. Datenschutzbestimmungen sind in den USA im Geschäftsbereich kaum vorhanden. So ist es möglich, dass die Allgemeinen Geschäftsbedingungen von Gmail Dinge vorsehen, die derzeit in der EU verboten wären. Während hierzulande Daten aus aufgelösten Vertragsverhältnissen nicht gespeichert werden dürfen, kann das Unternehmen Google damit machen, was es will.

Strittig ist auch der Umgang mit einem Google-Produkt, das ein europäisches Unternehmen gar nicht erst anbieten dürfte: Google Analytics ist ein Programm, das zur

Analyse der Besuche der eigenen Homepage kostenlos heruntergeladen werden kann. Wer dort vorbeisurft, dessen IP-Adresse wird erfasst und gespeichert, was in der EU nicht erlaubt ist, da die IP-Adresse zu den persönlichen Daten gezählt wird.

Ulrich Kühn von der Hamburger Datenschutzbehörde weist darauf hin, dass Goo-gle zwar solche Konflikte interessiert zur Kenntnis nehme, aber nie bereit sei, seine Produkte einem anderen Rechtsraum anzupassen. Schleswig-Holsteins Datenschützer Weichert betont, dass US-Provider, was den Datenschutz betrifft, generell »auf abschüssiges Gelände« führten. Es könne davon ausgegangen werden, dass Daten an Geheimdienste und Polizeibehörden weitergegeben werden. Erst kürzlich sei einer Person die Einreise in die USA verweigert worden, weil sie vorher bei einem Internetbuchversand ein missliebiges Buch gekauft habe.

Auf gerichtliche Anordnungen hin fallen alle Datenschutzgrenzen. Und je mehr Daten bei Unternehmen wie Google vorliegen, desto öfter werden staatliche Behörden zugreifen. Die US-Bürgerrechtsgruppe Epic betont, in den USA wirke sich die schleichende Gewöhnung an die geringe Sicherheit oder gar Offenlegung persönlicher Daten besonders aus, da die Durchsetzung des verfassungsmäßigen Rechts auf Privatsphäre auch davon abhänge, inwieweit sie tatsächlich erwartet werden kann.

#

Wo wie in den USA die Datenerfassung groß ist, sollte es nicht verwundern, dass der Datenhandel riesige Ausmaße hat. Auch im außerlegalen Bereich. Im Januar wurde bekannt, dass es Hunderttausende von Anrufen beim Mobilfunkanbieter Verizon gab, bei denen sich Betrüger als Angehörige der nicht existierenden Verizon-Abteilung »special need group« ausgaben und behaupteten, im Namen von Sprachgeschädigten anzurufen, um deren Daten zu ermitteln.

Als treibende Kräfte hinter dem Geschäft mit Telefonnummern werden Privatdetektive und Anwälte gesehen, die sie für ihre Recherchen gebrauchen können. Bis 1999 konnten Unternehmen Kundendaten in Massen verkaufen, was zu vielen Fällen von Missbrauch bis hin zum Identitätsdiebstahl führte. Der größte Datenhändler ChoicePoint musste noch im Februar 2005 zugeben, Daten über 145 000 Menschen »versehentlich« verkauft zu haben – an eine Verbrecherbande, die auf Identitätsdiebstahl spezialisiert war. Um welche Daten es ging, wurde den Opfern nicht gesagt. Seither verkauft der Marktführer sicherheitshalber zumindest die sensibelsten Daten wie Sozialversicherungs- und Führerscheinnummern nicht mehr an Kleinunternehmen, sondern nur noch an große Konzerne und staatliche Stellen.

ChoicePoint kann sich das leisten, hat die Firma doch mehrere millionenschwere Verträge mit staatlichen Stellen, nach eigenen Angaben mit 7 000 Strafverfolgungsbehörden. In den USA ist es üblich, dass so genannte Profiler massenhaft Daten aus öffentlichen Verzeichnissen sammeln und individuelle Dossiers anlegen, die sie oft an solche Stellen verkaufen.

Die Gefahr von Identitätsdiebstahl und -schwindel lauert allerdings nicht nur in der

Umgebung von digitalisierten Daten, sie geht nicht nur von Hackern, betrügerischen Rechercheuren oder großen Konzernen mit hochkomplexen Algorithmen zur Datenauswertung aus. Zu Millionenschäden führt selbst die denkbar einfachste Form des Datenklaus: das Durchsuchen von Altpapiertonnen. Dort finden sich gut erhaltene Dokumente mit verwertbarem Zahlenmaterial. Jüngst wurden in England solche Fälle publik.

#

Es wäre praktisch, Kommunikationswege zu entwickeln, die es erlaubten, dass das Kommunizierte nach der Übermittlung nicht mehr zugänglich ist. Wie etwa bei den aus einschlägigen Filmen bekannten sich selbst zerstörenden Tonbändern. Nur eben digital. Das klingt lächerlich? Das US-Unternehmen Void Communications sorgt mit genau dieser Idee derzeit für Wirbel. Es ist gerade dabei, das Produkt VaporStream auf den Markt zu bringen, das alle Spuren von elektronischer Kommunikation unwiderruflich löscht. Beiträge in Internetforen und E-Mails oder andere Kurznachrichten sollen sofort nach dem Lesen/Abrufen vom VaporStream-Internetserver verschwinden. Auf der eigenen Festplatte werden sie gar nicht erst gespeichert.

Mehr noch, beim Schreiben einer Nachricht wird sofort die Zieladresse unkenntlich gemacht, und von wem eine Nachricht kommt, soll nur im Posteingang, nicht aber beim Lesen zu sehen sein. Diese Technik kann vielleicht für ausgewählte Korrespondenzen sinnvoll sein, nicht aber für den Normalfall. Nachrichten können so weder weitergleitet noch gespeichert werden. Schade, dass Diskretion und Sicherheit manchmal so wenig zueinander passen.

#

Die Datenflut ist nicht zu überblicken, geschweige denn zu kontrollieren. Wie sich ihr also entgegenstellen? Und wie den damit verbundenen Annehmlichkeiten begegnen? Viele technische Neuerungen finden durch die freiwillige Übernahme Verbreitung. Ein ungeahnter positiver Aspekt offenbarte sich, als im März die Chicago Tribune berichtete, mit legaler Recherche an tausende Daten über CIA-Angestellte, -Institutionen und -Aktivitäten gekommen zu sein. Eine Sprecherin des Geheimdienstes musste einräumen, dass wegen der gegenwärtigen Möglichkeiten der Datenverarbeitung selbst Tarnidentitäten nicht mehr sicher seien.

In Schweden mussten Mitte Oktober innerhalb von zehn Tagen gleich zwei Ministerinnen zurücktreten, weil bekannt wurde, dass sie schon seit langem keine Rundfunkgebühren zahlten und auch den Lohn für ihre Kindermädchen nicht versteuerten. Dort sind, wie in den USA, viele amtliche Register öffentlich.

#

Es wäre idiotisch, angesichts dieser Fälle die neuen Möglichkeiten für die Zivilgesellschaft zu feiern, die es erlauben, staatlichen Akteuren besser auf die Finger zu schauen. Zu offensichtlich ist der Aspekt, dass die Überwachungs- und Disziplinargesellschaft schon

immer davon lebte, dass alle aufeinander aufpassen. Die Datenflut bewirkt nicht, dass das zwischen allen Beteiligten auf Augenhöhe geschieht, die neuen Technologien verstärken die bestehenden Asymmetrien.

CIA-Spione und Ministerinnen haben durch die potenzielle Sichtbarmachung aller möglichen Daten weitaus weniger zu verlieren als die große Masse an Menschen, deren Wohl und Wehe von den Konditionen lebenswichtiger Verträge abhängt. Dass in diese Verträge möglichst alle zur Verfügung stehenden Informationen eingehen, ist in einer an Vertragsverhältnissen ausgerichteten Welt kein Wunder.

#

Wer Risiken minimieren möchte, kann verschiedene Dinge tun. Informationen finden sich in dem von den Verbraucherzentralen herausgegebenen Ratgeber »Datenschutz für Verbraucher«.

Generell empfiehlt es sich, nicht bei Marktforschungsaktionen, Bonusprogrammen und Gewinnspielen mitzumachen, bei denen persönliche Daten abgefragt werden. In Fällen, bei denen Verträge nur abgeschlos-sen werden können, wenn persönliche Daten angegeben werden, die nicht erforderlich sind (wie z.B. bei einigen Internetprovidern), empfiehlt Roland Schäfer von der Deutschen Vereinigung für Datenschutz, falsche Angaben zu machen, solange es sich nicht auf den Ablauf des Vertragsverhältnisses negativ auswirkt.

Adresshändlern und anderen Unternehmen kann ein Text wie z.B. »Ich widerspreche der Nutzung und/oder Übermittlung meiner Daten für Werbezwecke oder für die Markt- oder Meinungsforschung (§ 28 Abs. 3 Bundesdatenschutzgesetz)!« geschickt werden. Zu den meisten Google-Diensten gibt es Alternativen anderer Anbieter.

Und was das Scoring betrifft: Jeder Mensch hat das Recht, entsprechenden Dienstleistern prinzipiell eine Score-Berechnung zu untersagen oder zumindest eine kostenlose und verständliche Übersicht über die bei der Erstellung verarbeiteten Daten und ihre jeweilige Gewichtung zu erhalten. Wurden falsche Daten verwendet, besteht ein Korrekturanspruch.

Es ist also eine Überlegung wert, vorsichtshalber ein formloses Schreiben z.B. an die Schufa zu senden, um die Unterlassung der Score-Berechnung zu erwirken. Die Adresse lautet: Schufa Holding AG, Verbraucherservicezentrum Hannover, Postfach 56 40, 30056 Hannover.