Im Netz der Späher

Das Internet ist zu einem Paradies für die Datensammler der Werbewirtschaft geworden. Auf Schritt und Tritt stehen die Netzbürger unter Beobachtung – Computer durchleuchten das digitale Ich, um seine Wünsche, Sorgen und Absichten zu ergründen. Ist die Privatsphäre noch zu retten?

In jeder Sekunde, ticketitack, gewinnt Facebook sechs Mitglieder; am Ende jedes Tages sind, grob geschätzt, wieder eine halbe Million hinzugekommen.

Und kaum einer von all den erwartungsfrohen Neubürgern ahnt, dass er bei dem sozialen Netzwerk nun gleichsam Schulden hat. Weil für Facebook jeder Nutzer 100 Dollar wert ist. Weil der Nutzer zum Wirtschaftsgut geworden ist und diese 100 Dollar einspielen muss. Er kann seine Geheimnisse, seine Sehnsüchte, seine Daten herausrücken, er muss sich offenbaren, er sollte nur den naiven Gedanken aufgeben, die Segnungen von Facebook seien kostenlos zu haben; denn er muss eine Menge abwerfen, damit sich das Projekt „Eine Welt voller Freunde“, das Lebenswerk des Mark Zuckerberg, auch rentiert.

Doch wie sollte das möglich sein? Wer interessiert sich schon für einen Neuling, der in Kiel oder Münster oder New York oder San Francisco ein paar Informationen preisgibt, damit er alte Klassenkameraden oder die Jugendliebe wiederfinden kann?

Nun, da wäre zum Beispiel Robert Mueller, Direktor des FBI. Neulich erst war er drüben im kalifornischen Palo Alto, platzte mitten in eine Besprechung bei Facebook hinein, im Schlepp eine Schar von Deputies: Er hatte gerade in der Nähe zu tun, wollte mal eben hallo sagen, pleased to meet you.

Facebook-Gründer Mark Zuckerberg plauderte ein Weilchen mit dem Polizeichef über Nichtigkeiten, dann eilte der Mann auch schon wieder davon – und hinterließ eine leicht verstörte Runde: Was war das eben?

Zuckerberg gewöhnt sich langsam an Besuche der Bundespolizei. Die Beamten schauen öfter bei Facebook vorbei, und meist haben sie einen Gerichtsbeschluss dabei. Denn Facebook weiß nun mal mehr über seine Kunden als jeder Staat über seine Bürger: Facebook kennt ihre Freunde, den Aufenthaltsort, Facebook kennt sexuelle und sonstige Vorlieben, die ganzen, komplexen Lebensumstände.

Und all die Daten und Lebensspuren der Netzbürger sind wertvoll in doppelter Hinsicht. Sie sind Informationen, manchmal Nachrichten, Facebook enthüllt viele Geheimnisse. Und sie sind Waren. Darum sind sie für die Jagd nach Verbrechern so nützlich wie für die Jagd auf Kunden, wie sie die Werbewirtschaft erträumt. Wer herausfindet, wonach den Leuten der

DAS DIGITALE SPIEGELBILD

Freunde, Familie, Urlaub, Konsum, Freizeit, Krankheit, Geld, Liebe, Beruf – alles, was der Nutzer im Internet treibt, schlägt sich auch in seinem digitalen Spiegelbild im Netz nieder und schärft dessen Kontur. Denn viele Anbieter im Internet lassen sich ihre Dienste in einer unsichtbaren Währung bezahlen: Informationen über ihre Nutzer. Dabei bedienen sie sich zum Beispiel unauffälliger Marker auf den Computern ihrer Kunden, den **Cookies.**

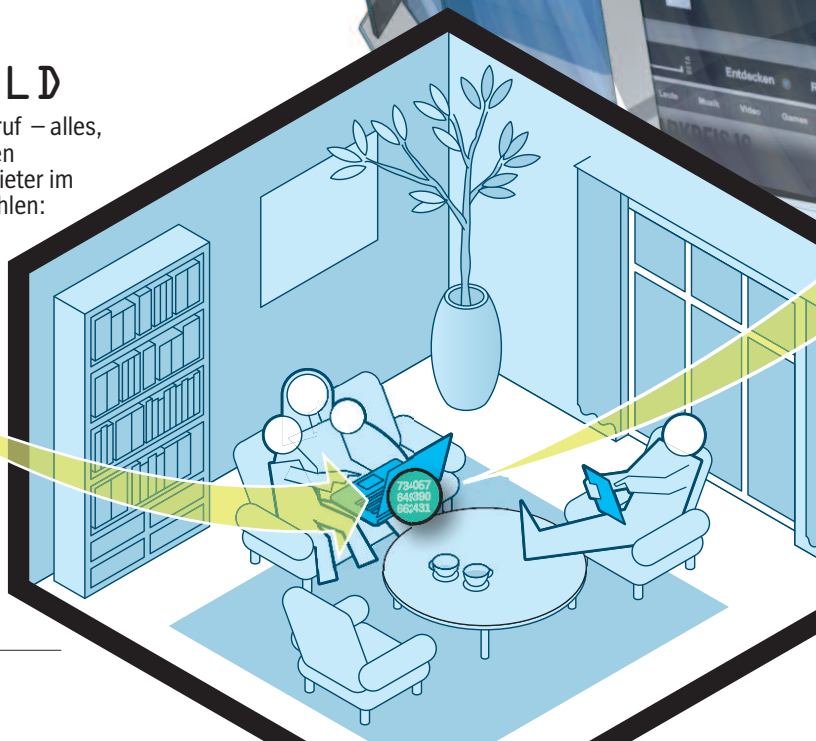
Was ist ein Cookie?

734057 649390 662431

1. Das Cookie ist eine Textdatei mit einer Zeichenfolge. Beim Aufruf einer Web-Seite speichert deren Betreiber sie auf dem Computer des Kunden ab. Dessen Computer ist nun markiert.

2. Beim nächsten Besuch der Web-Seite kann der Betreiber den Kunden identifizieren und kennt dann zum Beispiel dessen frühere Interessen.

3. Er kann die Markierung aber auch, zusammen mit den gesammelten Daten, beliebig oft an andere Interessenten verkaufen, die sie wiederum mit Informationen anderer Betreiber verknüpfen – es entsteht ein digitales Abbild des Nutzers.




amazon.d
Mein Konto
Hilfe
Einkaufswage
FARMVILLE
ebay
zynga
Google
Earth
facebook
Eine neue Twitter Erfahrung! Erfahre
twitter
Der beste Weg herauszufin
weiter
FRIEND
SCOUT24
Wir verlieben Dich!
JETZT KAUFEN?
Zur Kasse gehen
ODER
Jetzt mit 1-Click® kaufen
Lieferung an:
Eine neue Adresse eingeben
Verwalten Sie Ihre 1-Click-Adressen & -Einstellungen
Dies ist ein Geschenk
Erfahren Sie mehr
iTunes
mobile.de
SUCHEN
Auf Neuwagensuch
Jetzt finden
YouTube
Google
Street View
YAHOO! DEUTSCHLAND
NACHRICHTEN
altavista
Bildersuche
Bilder
Nachrichten
flickr
VISA
PayPal
StayFrie
IMMOBILIEN
SCOUT24
DER SPIEGEL

Sinn steht, was ihnen Sorgen oder Lust bereitet, kann mit den Befunden viel Geld verdienen.

Kein Wunder also, dass das gesellige Treiben inzwischen aberwitzige Gewinnphantasien nährt. Sollen sie je in Erfüllung gehen, ist es mit der Gemütlichkeit des guten, alten Internets vorbei: Es beginnt die Zeit des großen Inkassos.

Sagenhafte 450 Millionen Dollar zahlte vor wenigen Tagen die US-Bank Goldman Sachs für einen Anteil von gerade mal 0,8 Prozent an Facebook. Den Wert von Zuckerbergs Firma taxieren die Investmentbanker damit auf 50 Milliarden Dollar; Facebook hat rund 500 Millionen Mitglieder, so errechnen sich die 100 Dollar pro Kopf. Denn gerade bei dieser größten aller Freundeszentralen gewährt die Kundschaft besonders freigebig Einblick in ihr Dasein.

Aber auch andere Giganten der Netzwelt, von Google bis Apple, bekommen immer feinere Aufschlüsse über die Lebensumstände ihrer Nutzer. Das halbe Internet hat sich binnen wenigen Jahren in einen Apparat des Erfassens und Protokollierens verwandelt. Eine wachsende Industrie steht bereit, mit raffinierter Technik das Verhalten der Netzbürger auszukundschaften, wo auch immer sie sich aufhalten mögen. Spezialfirmen spionieren aus, was sie lesen, wonach sie suchen und woran sie Interesse zeigen.

All diese Daten sind nur der Rohstoff für komplexe Berechnungen. Sie werden verknüpft, mit bestehenden Datenbanken abgeglichen und in die Zukunft hochgerechnet: Was könnte der Kunde morgen, was übermorgen kaufen wollen? Je feiner gesponnen, je aktueller die Daten, desto teurer lassen sie sich verhökern.

Es ist wie im Goldrausch: Die Skrupellosen probieren, wie weit sie gehen können.

Jüngst erst kam heraus, dass eine kalifornische Firma namens RapLeaf in großem Stil Verhaltensprofile ahnungsloser Netzbürger angelegt hat – mitsamt deren Namen und E-Mail-Adressen. RapLeaf rühmt sich eines Datenschatzes, der bereits eine Milliarde E-Mail-Adressen umfasst. Diese kaufte die Firma großteils von verschiedenen Web-Seiten zusammen, bei denen die Kunden sich mit Namen und E-Mail angemeldet hatten.

Wer Name und E-Mail-Adresse kennt, hat einen Schlüssel, der viele Türen öffnet: Fast alles wird damit zugänglich, was das Internet über die Kundschaft weiß. Vor allem aber erlangt der Datensammler auch noch Zugriff auf das echte Leben diesseits der Netzwelt: auf Wohnanschrift und Telefonnummer.

Eine ganze Reihe sinistrer Firmen hat sich auf das massenhafte Zusammenkratzen (Englisch: Scraping) persönlicher Details aus Diskussionsforen verlegt. Im vergangenen Mai ließ sich sogar die angesehene Marktforschungsfirma Nielsen dabei erwischen, wie sie in dem Selbsthilfeportal PatientsLikeMe automatisch mitlas – dort tauschen sich Ratsuchende über Depressionen und Selbstverletzung aus. Nielsen gelobte flugs Besserung; so etwas werde nicht wieder vorkommen.

Es geht zu wie im Goldrausch. Die Skrupellosen unter den Datenschürfern probieren, wie weit sie gehen können; und das Gesetz ist schwach. Zwar kann der Netzbürger inzwischen etlichen Spähfirmen auf ihren Web-Seiten per Häkchen die Erlaubnis zur weiteren Überwachung verweigern. In der Praxis aber ist ihm die Verfügung über sein digitales Ich bereits weitgehend entglitten.

Im Netz verwandelt sich der Bürger in ein durch und durch maschinenlesbares Wesen – damit wird er zum ohnmächtigen Objekt von Neugierigen jeder Sorte. In den USA lassen Beratungsfirmen bereits massenhaft Beiträge in Web-Foren von schnellen Rechnern analysieren, um zu Wahlkampfzwecken die politische Haltung ihrer Urheber zu ergründen.

Auch den Arbeitsplatz umlauern die Späher. Spezialfirmen durchforsten E-Mails und Telefonverbindungsdaten der Mitarbeiter nach Anzeichen von Korruption, Geheimnisverrat oder auch nur verdächtiger Klüngelbildung.

Besonders entschlossen bahnt die Werbewirtschaft den Weg in die Zukunft der Rundumbeäugung. In ihrem Auftrag wird ein Großteil des Werkzeugs entwickelt und im netzumspannenden Zusammenspiel erprobt.

Echte Schurkereien mögen bislang nur vereinzelt vorkommen; zermürbend wirkt aber vor allem der Normalfall. Unlängst erst prüfte das „Wall Street Journal“ 50 populäre Websites, darunter Yahoo, Ebay und MSN. Ein Testcomputer besuchte dafür der Reihe nach alle Adressen. Danach fanden sich insgesamt 3180 neue Spähdateien, zumeist „Cookies“, in seinem Speicher; so heißen die kleinen Textdateien, mit denen die Computer potentieller Kunden markiert werden.

Zwei Drittel dieser Cookies stammten von Firmen, die darauf spezialisiert sind, die derart gestempelten Nutzer über diverse Adressen durchs Internet zu verfolgen. 131 solche Verfolger wurden im Speicher des Testrechners identifiziert; sie alle sind auf zahllosen Websites zugleich präsent. Nicht selten verlieren deren Betreiber selbst schon den Überblick darüber, mit wem sie alles kooperieren.

Allein das Wörterbuchportal Dictionary.com markiert seine Besucher mit gleich 223 verschiedenen Verfolger-Cookies auf einmal. Nur eine der 50 untersuchten Websites verzichtet ganz auf dieses Mittel: Wikipedia.

Was für das Schaf die Ohrmarke, ist das Cookie für den Menschen. Es macht ihn identifizierbar. Wer ihm über Wochen oder gar Monate hinweg auf der Spur bleibt, erfährt immer mehr über seine Lebenslage, kann immer besser seine Absichten vorausberechnen – stets mit dem Ziel, dem erhofften Kunden die aussichtsreichste Werbung zuzuspielen. Quasi als blinkendes Pünktchen auf den Radarschirmen zahlloser Verfolger bewegt sich der Mensch, beständig beobachtet, markiert und anderswo wiedererkannt.

Ein Cookie könnte nach einer Weile etwa verraten, dass an diesem Computer eine Frau zwischen 35 und 44 Jahren

SAMMLER UND JÄGER

Die zahllosen digitalen Spuren im Internet sind der Rohstoff, auf dessen Verarbeitung sich eine Reihe junger Unternehmen spezialisiert haben. Sie verfolgen über Cookies die digitalen Wege der Internet-Gemeinde und kaufen Nutzerdaten von Web-Seiten-Betreibern. Aus Unmengen von Informationen entstehen digitale Profile der Internetnutzer. Besonders skrupellose Firmen kratzen auch noch zusammen (Scraping), was Chatrooms, Foren und soziale Netze zu bieten haben.

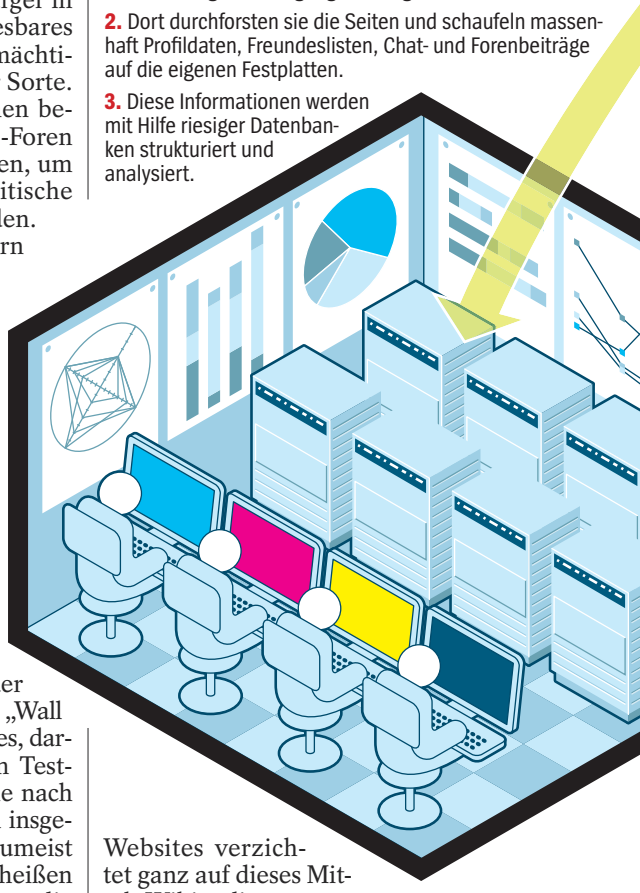
Wie funktioniert Scraping?

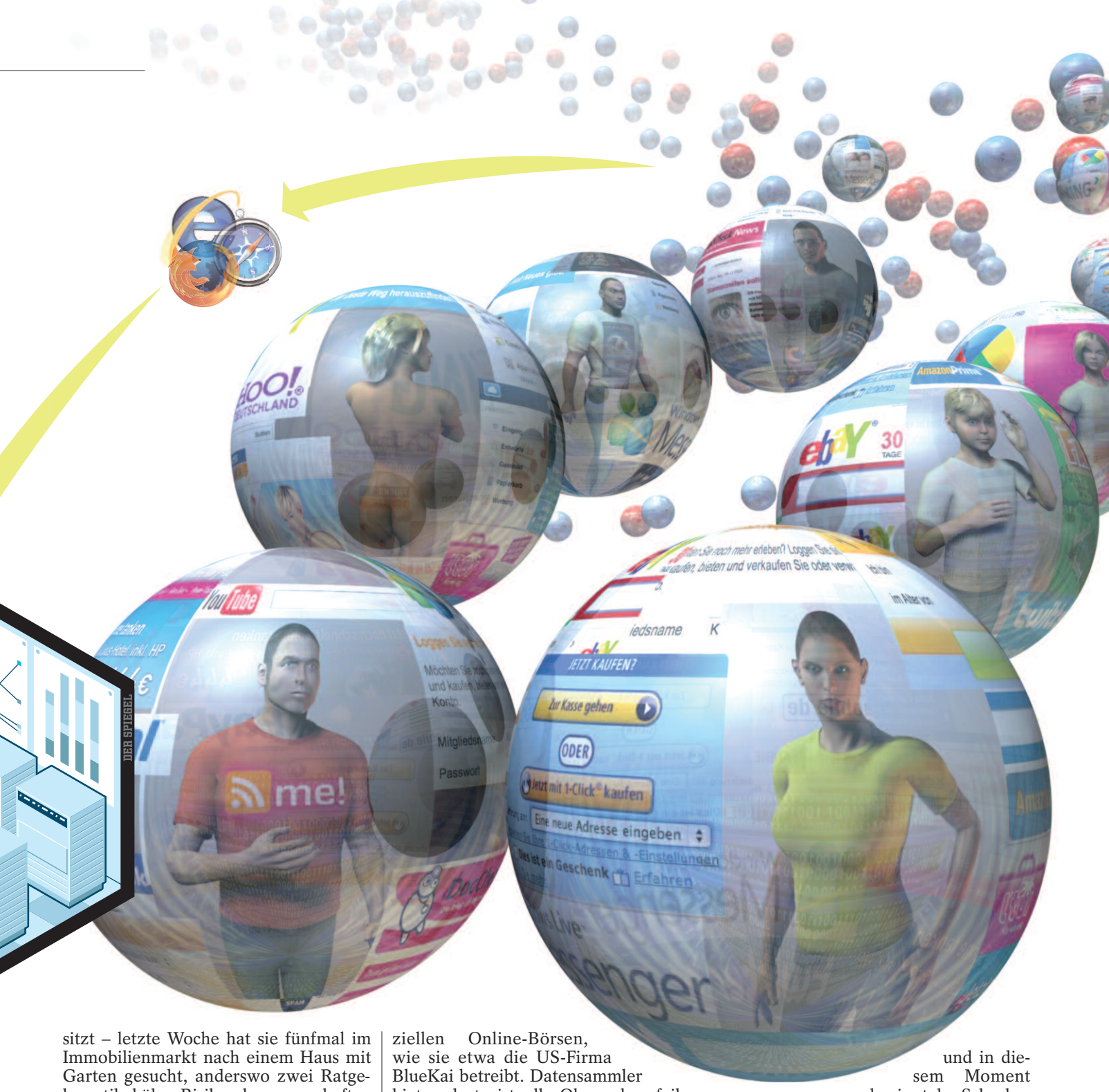
Beim Web-Scraping werden systematisch private Informationen über Einzelpersonen oft mit Hilfe präparierter Browser abgerufen und gesammelt.

1. Computer von Spezialfirmen melden sich automatisch unter Scheinnamen z. B. bei sozialen Netzen oder Foren an. So erlangen sie Zugang zu den geschützten Bereichen.

2. Dort durchforsten sie die Seiten und schaufeln massenhaft Profildaten, Freundeslisten, Chat- und Forenbeiträge auf die eigenen Festplatten.

3. Diese Informationen werden mit Hilfe riesiger Datenbanken strukturiert und analysiert.





sitzt – letzte Woche hat sie fünfmal im Immobilienmarkt nach einem Haus mit Garten gesucht, anderswo zwei Ratgeberartikel über Risikoschwangerschaften gelesen, beim Autoportal drei Stunden lang penibel geräumige Karossen verglichen und bei diversen Finanzdienstleistern Kreditrechner mit sechsstelligen Summen gefüttert.

Damit lässt sich eine Menge anfangen. Ohne es zu wissen, hat die Unbekannte sich in ein lukratives Gut verwandelt, das wochenlang immer wieder verkauft wird – wer ihre Ohrmarke erwirbt, kann ihr Werbung für Windeln, Baudarlehen oder Jahreswagen zuspielen, wo auch immer sie sich im Netz gerade bewegt.

Mittlerweile ersteigert die Werbewirtschaft interessante Kunden auch an speziellen Online-Börsen, wie sie etwa die US-Firma BlueKai betreibt. Datensammler bieten dort virtuelle Ohrmarken feil, automatisch gruppiert nach beobachtetem Verhalten und vermuteten Absichten: Das können 200 000 Gutverdiener sein, die Anzeichen von Nestbauverhalten zeigten. Oder 30 000 Reiselustige, die seit vorgestern nach Flügen ab Chicago fahndeten – bei Bedarf auch sortiert nach Reiseziel oder Abflugdatum. Solche Profile gibt es schon für umgerechnet einen halben Cent das Stück; ein guter Datensatz kann aber auch einen halben Euro oder mehr einbringen.

Die jüngste Errungenschaft: Augenblicks-Auktionen. Der Mensch klickt irgendwo im Internet auf einen Link – und in diesem Moment beginnt der Schacher darum, welche Anzeige er sogleich sehen wird. Das alles geschieht in Millisekunden: Rasend schnell taxieren die Rechner von BlueKai (Leitspruch: „Ihr Kunde ist ein bewegliches Ziel“) den Besucher: Gehört er zu einer der Zielgruppen, für die Gebote vorliegen? Und welcher Werber zahlt gerade den höchsten Preis?

In diesem Tempo können nur Maschinen entscheiden – hier dealen Computer mit Computern. Auch die Rechner des Käufers, der an die Börse angeschlossen ist, müssen im Augenblick der Auktion eine Menge kalkulieren: Hat dieser Anzeigenplatz bereits gute Resultate gebracht? Hat

der Besucher in der letzten Viertelstunde schon 30 Anzeigen gesehen, so dass er abzustumpfen droht? Je nachdem variieren die Computer der Agenturen ihre Gebote.

Doch was ist eigentlich so verwerflich daran, wenn die Werbung immer besser zu den eigenen Bedürfnissen passt?

Das Problem ist die Raffinesse der Technik. Einmal ausgereift, lässt sie sich ebenso gut für ungemütliche Zwecke einsetzen. „Als Nächstes könnte dann aus Ihrem Online-Verhalten zum Beispiel Ihre Kreditwürdigkeit herausgelesen werden“, sagt Thilo Weichert vom Unabhängigen Landeszentrum für Datenschutz in Kiel.

Das Werkzeug der Verhaltensanalyse ist vielseitig wie das Leben selbst. Wer will, kann damit auch netzübergreifend Signale sinkender Zufriedenheit mit dem Beruf registrieren oder einen Hang zu politischer Widerborstigkeit. Es muss ja nicht gleich so weit kommen wie in Steven Spielbergs Zukunftsthriller „Minority Report“, in dem eine Spezialeinheit Verbrechen vorausahnt und unterbindet, bevor sie begangen werden.

Die Werbewirtschaft müht sich bereits nach Kräften, in die Zukunft des Kunden zu spähen. Aus Daten wie Haushaltseinkommen, Wohngegend und Schulbildung erstellt sie ein Verhaltensmodell, eine Art digitale Simulation der Zielperson – der Rest ist mathematische Knobelei: Wie hoch ist die Wahrscheinlichkeit, dass dieser Mensch demnächst ein teures Fahrrad kauft? Wo könnte er seinen Urlaub verbringen wollen? Ist sein Verhalten typisch für jemanden, der Schwierigkeiten hat, ein Darlehen zurückzuzahlen? All diese Schlussfolgerungen gilt es dann zu verkaufen, solange sie heiß sind.

Die Verhaltensprognose steckt noch in den Anfängen. „Bislang sind die Ergebnisse nicht besser als bei den anderen Methoden“, sagt Christoph Schäfer von der Hamburger Werbeagentur Performance Media. „Das braucht noch ein paar Jahre.“ Bei dem Tempo, mit dem die datengetriebene Werbung voranschreitet, beruhigt das wenig. „Allein in Deutschland“, sagt Schäfer, „werden schon jetzt Tag für Tag Dutzende Milliarden Cookies gesetzt.“

Das Goldfieber brach aus, weil derzeit zwei Dinge zusammentreffen: Zum einen ist die Infrastruktur des Erfassens inzwischen eingespielt und im Internet so gut wie überall verbreitet. Zum anderen lohnt es sich erst jetzt so richtig, sie auch einzusetzen: Das Publikum verbringt inzwischen sein halbes Leben mit Anschluss ans Netz. Es hinterlässt dort Tag für Tag Privatfotos und Kommentare, sucht Rat bei Blasenschwäche oder ein Hotel für den Seitensprung, tut seine politische Meinung in diversen Foren kund und versorgt den Bekanntenkreis mit Nachrichten über seinen Tageslauf.

Ergiebig sind vor allem die sozialen Netzwerke, wo es auf Mitteilsamkeit geradezu ankommt. Die gut 500 Millionen Mitglieder von Facebook bringen mehr als 30 Milliarden Kommentare, Fotos und sonstige Bekundungen ihrer Existenz im Monat hervor – pro Nutzer 60 Stück.

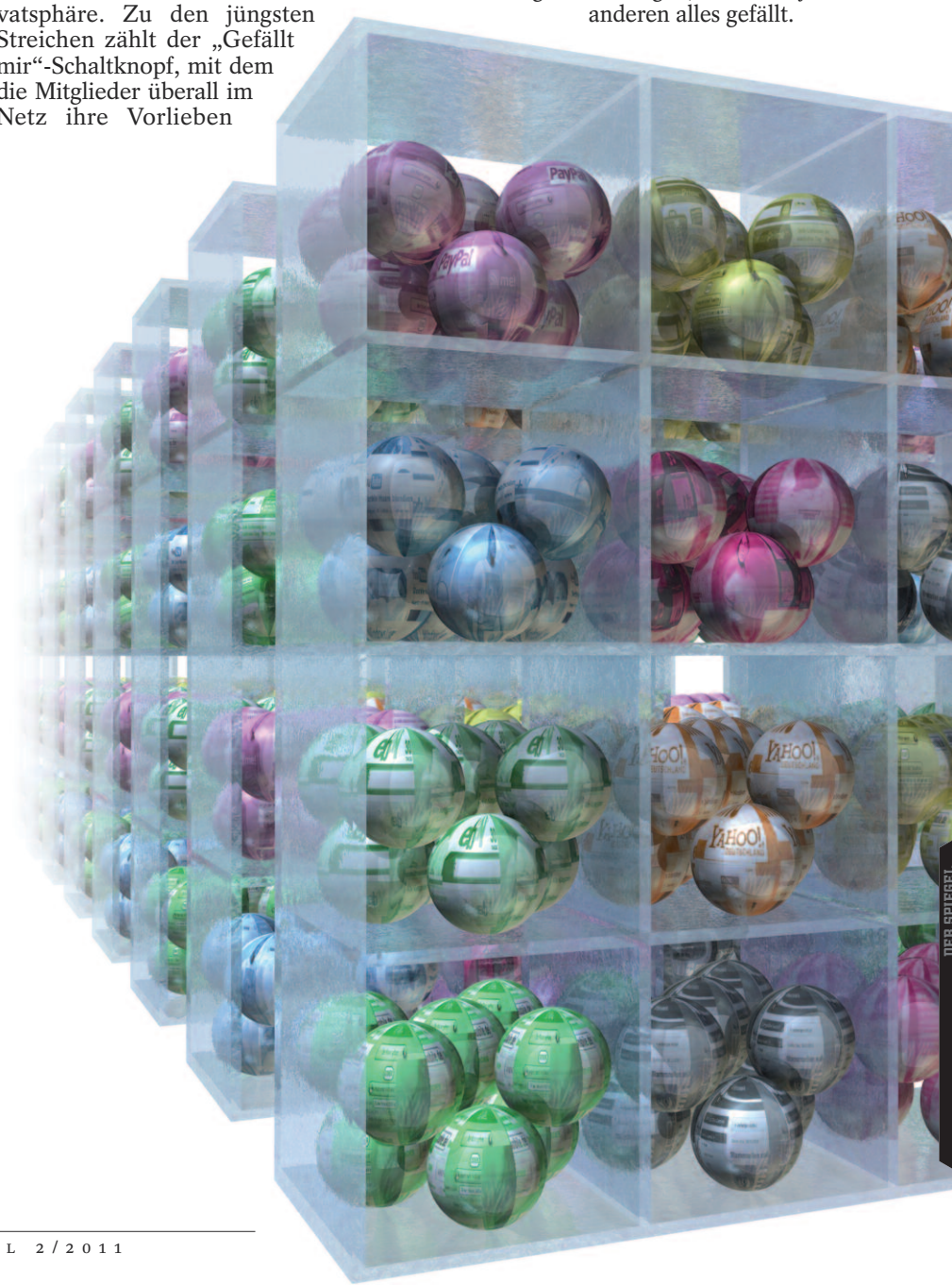
Auch überall sonst, wo die Leute nach Austausch und Gemeinschaft streben, steigt der Output. Allein die Nutzer des Dienstes Twitter veröffentlichen derzeit jeden Tag 95 Millionen Kurzmeldungen, genannt „Tweets“. All diese Neckereien und Fundsachen, Kurzweisheiten und launigen Sprüche bilden zusammen ein stets aktuelles Zentralregister der Stimmungen, Trends und Befindlichkeiten.

Was auch immer der Mensch tagein, tagaus hinterlässt an Lebensspuren und anderen digitalen Abriebseln – es lagert sich in irgendwelchen Datenspeichern ab.

Vor allem Facebook macht den Datenschützern Sorge. Die Firma erfindet immer neue Schikanen für die Privatsphäre. Zu den jüngsten Streichen zählt der „Gefällt mir“-Schaltknopf, mit dem die Mitglieder überall im Netz ihre Vorlieben kundtun können: den politischen Kommentar im Diskussionsforum, die tolle Stichsäge im Online-Baumarkt, das Handyfilmchen der Freundin beim Portal MyVideo. Jeder Klick erscheint auf der Profilseite des Nutzers – und wird zumeist auch dem Freundeskreis mitgeteilt.

Erst im April 2010 wurde die kleine blaue Klickfläche eingeführt, und schon ist das Internet damit gepflastert: Mehrere hunderttausend Adressen bieten ihren Besuchern dieses bequeme Mittel, ihren Beifall zu äußern. Deren Betreiber hoffen auf Zutrieb durch die automatisierte Mundpropaganda per Mausklick.

Den größeren Nutzen hat aber Facebook: Damit ist bald die halbe Netzwelt auf dem Radarschirm der Firma. Sie kann nun auch außerhalb des Dienstes intime Kenntnisse über die Vorlieben ihrer Mitglieder erlangen – oft genug wüssten selbst Ehegatten nicht so genau zu sagen, was dem jeweils anderen alles gefällt.



Für den Netzbürger wird es immer schwerer zu überblicken, wem er wo was genau verrät. „Es ist ein großes Problem, wenn Anbieter mit massiver Marktmacht auf Web-Seiten zugreifen, die gar nichts mit ihnen zu tun haben“, sagt Datenschützer Weichert.

Auf eine Ruhepause ist nicht zu hoffen. Kaum war der „Gefällt mir“-Schalter etabliert, schickte Facebook sich an, die Mitglieder auch übers Netz hinaus ins echte Leben zu begleiten: Der neue Dienst „Facebook Orte“ erlaubt es dem Nutzer, jederzeit mitzuteilen, wo er sich gerade aufhält. Das sind heikle Daten. Werden die Leute lernen, damit sparsam umzugehen? Oder gewöhnen sie sich mit der Zeit daran, einer notorisch unberechenbaren Firma anzuvertrauen, wo sie arbeiten, leben und Urlaub machen?

Bewegungsmuster gehören zu den sehr persönlichen Dingen; im mobilen Internet kommt dieser verlockende Schatz nun in die Reichweite der Datensammler. Jeder, der Zugang hat, könnte unschwer auf Namen und Adressen schließen.

Heutige Mobiltelefone wissen immer, wo sie sind; entweder haben sie die GPS-Satellitenortung eingebaut, oder sie prüfen ihre Lage anhand der WLAN-Funknetze in der Umgebung, deren Kenndaten sie empfangen. Der Besitzer aber kann kaum kontrollieren, wer alles von seinem Aufenthaltsort erfährt, sobald er sein Handy einschaltet.

Denn jedermann kann sich leicht Zugang zu solchen Ortsdaten erschleichen:

Die Hälfte der beliebtesten Apps auf dem iPhone verraten die Ortsdaten der Besitzer an Spähfirmen.

Ein gutes Dutzend Firmen bieten in Deutschland beispielsweise die Ortung von Handys an – etwa für Eltern, die ihre Kinder im Blick behalten wollen. Die gleiche Technik erlaubt jedoch auch dem gewalttätigen Ehemann, unbemerkt seiner Frau nachzustellen. Zwar schicken die Dienste eine SMS mit einer Anfrage an das Gerät, denn das Gesetz verlangt die Einwilligung des Überwachten. Wer aber Zugang zu dem Telefon hat, kann die Nachricht umstandslos abfangen und beantworten.

„Wir wissen, dass die Überwachung leicht zu aktivieren ist“, sagt Sabine Ungeheuer vom Frauenhaus in Limburg an der Lahn. „Wir raten deshalb den Frauen, sich eine neue Sim-Karte zu besorgen.“

Die Werbewirtschaft ist gewiss nicht auf Stalking aus, aber die Wege der Kundschaft sind auch für sie von hohem Wert. Das „Wall Street Journal“ überprüfte jüngst 101 beliebte Programme („Apps“) für das iPhone von Apple und andere Smartphones. Das Ergebnis: 47 Apps verrieten die Ortsdaten des Besitzers an Spähfirmen. Und ist sein Aufenthalt erst bekannt, fällt es oft nicht schwer, auch sein Ziel zu erahnen. Versuche mit anonymen Bewegungsdaten von Mobilfunkanbietern haben gezeigt: Die meisten Menschen pflegen im Alltag doch einen recht vorhersagbaren Trott.

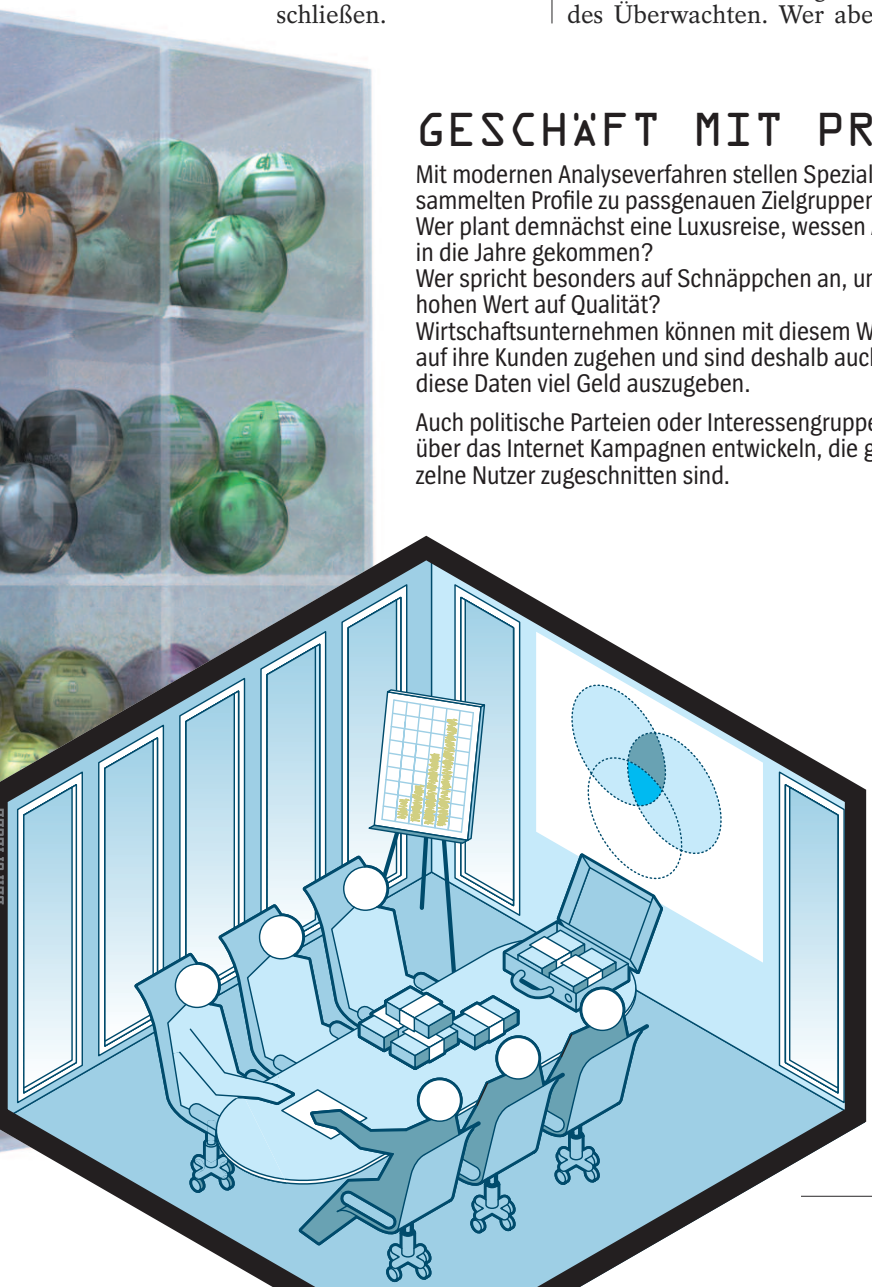
Es liegt in der Natur der Sache, dass die Datensammler immer noch mehr erfahren wollen. Google-Chef Eric Schmidt stellt sich die Suchmaschine der Zukunft, wie er unlängst bekundete, als ein „allwissendes System“ vor: „Ich glaube, die meisten Leute wollen nicht, dass Google ihre Fragen beantwortet“, sagte er. „Sie wollen, dass Google ihnen sagt, was sie als Nächstes tun sollen.“

Dies ist nicht einfach nur die ulkige Vision eines zahlenvernarrten Technokraten. Es ist die Vision eines Managers, der maßgeblich mitbestimmt, in welche Richtung der Datenriese Google strebt. Und selbst wenn das Ziel abwegig klingen mag: Die Firma kann ihm nur näher kommen, indem sie mittels ihrer Algorithmen immer mehr in den Alltag und möglichst auch in die Gehirnwindungen ihrer Nutzer hineinzukriechen versucht.

Die Beteuerung der Späher, es würden ja nur anonyme Daten verarbeitet, ist im Zweifelsfall wenig wert. „Von anonymisierten Daten sprechen wir schon lange nicht mehr“, sagt Datenschützer Weichert. „Es ist meist nur eine Frage des Aufwands, sie wieder zu personalisieren.“

Forscher haben mehrfach vorgeführt, wie man aus verstreuten Bruchstücken ganze Identitäten rekonstruiert. Die Informatiker Arvind Narayanan und Vitaly Shmatikov etwa zeigten, dass dafür oft schon die Kenntnis der Vorlieben bei Kinofilmen genügt. Sie nahmen 100 Millionen Filmbewertungen von 500 000 anonymen Kunden des Online-Filmverleihers Netflix – und in zwei Dritteln der Fälle bekamen sie die Urheber heraus, sofern diese Kunden sich schon anderswo im Netz namentlich zu ein paar Filmen geäußert hatten. Das Muster einiger Vorlieben ergibt bereits ein unverwechselbares Profil, das den Nutzer ziemlich zuverlässig auffindbar macht.

Vielen entspannten Zeitgenossen bereitet all das wenig Sorgen. Sie warnen



GESCHÄFT MIT PROFIL

Mit modernen Analyseverfahren stellen Spezialisten die gesammelten Profile zu passgenauen Zielgruppen zusammen. Wer plant demnächst eine Luxusreise, wessen Auto ist schon in die Jahre gekommen?
Wer spricht besonders auf Schnäppchen an, und wer legt hohen Wert auf Qualität?
Wirtschaftsunternehmen können mit diesem Wissen gezielt auf ihre Kunden zugehen und sind deshalb auch bereit, für diese Daten viel Geld auszugeben.

Auch politische Parteien oder Interessengruppen können über das Internet Kampagnen entwickeln, die genau auf einzelne Nutzer zugeschnitten sind.

vor Hysterie in der laufenden Debatte um die Privatsphäre. Ihr Hauptargument: Was erfahren die schon? Warum soll nicht jeder wissen, dass ich morgen nach München fliege und gestern nach einem Leberknödelrezept gesucht habe? Mit einem Satz: Ich habe nichts zu verbergen.

Dieser Standpunkt verkenne, was auf dem Spiel steht, meint der US-Jurist Daniel Solove. Es sei ein fundamentales Missverständnis, dass eine Privatsphäre nur brauche, wer etwas ausgefressen hat. Den Schutz vor dem Sammeln, Ausspähen und Überwachen aller Aktivitäten hält Solove auch gar nicht für entscheidend – tatsächlich wird ja zumeist nur Banales entdeckt. In seinem Buch „The Digital Person“ erläutert Solove, wo für ihn die echte Bedrohung beginnt: wenn das verstreute Sammelgut von unzugänglichen Instanzen verarbeitet wird, die niemandem Rechenschaft geben.

Solove zieht zum Vergleich Franz Kafkas „Prozess“ heran. Ein Josef K. wird in diesem Roman eines Morgens verhaftet, ohne zu wissen, warum. Eine namenlose Behörde hat offenbar gegen ihn ermittelt, hat Daten ausgewertet und Anklage erhoben – nie aber erfährt K. auch nur, was gegen ihn vorliegt; folglich ist ihm auch keinerlei Verteidigung möglich. K. darf übrigens, während der Prozess läuft, sein normales Leben unbehelligt fortsetzen. Am Ende aber wird er von zwei Männern abgeholt und erstochen „wie ein Hund“.

Dem Netzbürger ergeht es, vom Ausgang abgesehen, nicht ganz unähnlich: Winzige Details, die für sich nichts bedeuten mögen, werden verknüpft und verglichen, Schlüsse werden gezogen, Voraussagen hochgerechnet und Entscheidungen gefällt. Falsch oder richtig – der Bürger, Objekt unbekannter Analyseapparate, hat bei der fremdgesteuerten Biopsie seines Verhaltens nicht das Geringste mitzureden.

Dieser Entzug der Verfügungsgewalt über die eigene Person verändert die Machtbalance zwischen Menschen und Unternehmen. Er könnte ein Gemeinwesen nachhaltiger entkräften, als es die grobschlächtige Gedankenpolizei aus George Orwells „1984“ vermocht hätte.

Mit dem Staat ist zwar ebenfalls stets zu rechnen, wenn es um Überwachung geht – Stichwort Vorratsdatenspeicherung. Aber im Vergleich geht es da übersichtlich und nicht halb so verstörend zu: Man kennt die Akteure, und wenn sie ihr Spiel zu weit treiben, rafft man sich auf und geht demonstrieren oder zieht vor Gericht.

Im chaotischen Ökotop der kommerziellen Datensammelei dagegen finden sich schon Fachleute nur mit Mühe zurecht. Dabei steht ein Medium auf dem Spiel, das inzwischen für viele lebenswichtig ist. Wer hat heute noch die Wahl, sich dem Internet konsequent zu entziehen? Nicht einmal die verräterischen Cookies wird man so leicht los, denn dummerweise dienen sie zum Teil auch nützlichen Zwecken, etwa dem Speichern von Warenkörben in den Online-Shops. Wer sie pauschal aussperrt, kann viele Websites gar nicht mehr richtig nutzen.

Weitaus stärker noch treibt sozialer Druck das Publikum in die Selbstentäußerung – auch der Nachbar ist neugierig. Wer sich nicht in einem sozialen Netzwerk präsentiert, ist fast schon der Eigenbrötelei verdächtig. Überall erwartet die Mitwelt, dass der Netzbürger offenherzig mittut; alle wollen einander finden, erreichen und bei Gelegenheit auch gern ein wenig ausspähen können.

Das stundenlange Stöbern in anderer Leute Facebook-Profilen gehört zu den Tätigkeiten mit dem größten Suchtpotential. Und zwischendrin wird mal eben ein neuer Bekannter gegoogelt oder eine der speziellen Personensuchmaschinen wie Yasni.de angeworfen, die aus Hunderten Quellen zusammentragen, was das Internet über die Zielperson weiß. Auch „Street View“ gibt es nur, weil jeder gern in fremde Straßen guckt.

Das Internet ist ein Paradies für die Neugier. Mark Zuckerberg, der Chef von Facebook, glaubt gar, im Rausch der neuen Möglichkeiten habe sich unser Bedürfnis nach Privatsphäre weitgehend verflüchtigt. Als er das neulich in einem Interview etwas verquast auszudrücken versuchte, war die Aufregung groß – es hieß, er habe (was nicht ganz stimmt) vom „Ende der Privatheit“ gesprochen.

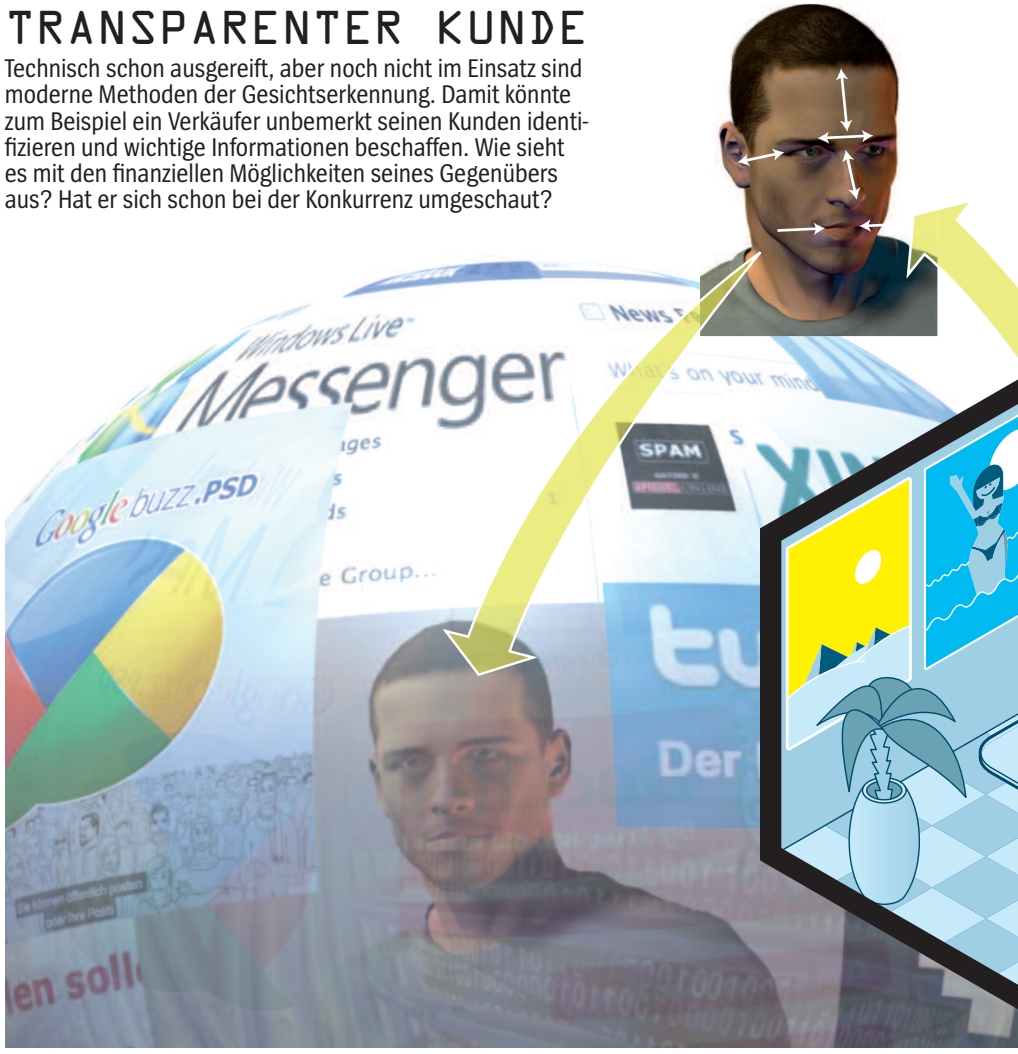
Ist es tatsächlich schon so weit? Ist ein Mindestmaß unbehelligten Daseins nicht länger nötig – oder, wenn doch, leider nicht mehr zu retten?

In Wahrheit ist das Problem eher, dass darüber im Moment ein paar Großunternehmen zu entscheiden scheinen, für die Fatalismus in dieser Sache von großem Vorteil wäre. Die Frage lautet also: Warum kann nicht jeder selbst bestimmen, wer wie viel Einblick in sein digitales Dasein bekommt? Warum erfahren die Ausgespähten zumeist noch nicht einmal, wo ihre Daten überall herumvagabundieren?

Es geht nicht mehr nur um ein paar Spuren hie und da. Die eifrigsten Netzbürger werfen bereits einen sehr deutlichen digitalen Schatten – durchs Netz begleitet sie ein Doppelgänger, der seinem Urbild in vielen Details immer ähnlicher wird. Und dieses digitale Abbild beginnt

TRANSPARENTER KUNDE

Technisch schon ausgereift, aber noch nicht im Einsatz sind moderne Methoden der Gesichtserkennung. Damit könnte zum Beispiel ein Verkäufer unbemerkt seinen Kunden identifizieren und wichtige Informationen beschaffen. Wie sieht es mit den finanziellen Möglichkeiten seines Gegenübers aus? Hat er sich schon bei der Konkurrenz umgeschaut?



mit der Zeit ein beunruhigendes Eigenleben im Netz.

Das digitale Ich hat heute zumeist bei Facebook oder einem anderen Sozialnetz seinen Hauptwohnsitz. Dort findet es eine Bühne vor, die bespielt werden will. Zum ersten Mal in der Geschichte hat der Privatmensch eine Ständige Vertretung in der Öffentlichkeit.

Überraschend ehrlich geht es bei der Pflege der Profile in diesen Sozialnetzen zu, wie mehrere Studien gezeigt haben. Von kleineren Retuschen abgesehen, präsentieren die Leute sich weitgehend so, wie sie sind. Der Traum vom Internet als Maskenball der Identitäten begeistert nur noch die kleine Minderheit der Rollenspieler. Die „virtuelle Identität“ als pixeliger Avatar hat sich als der Flop des Jahrzehnts erwiesen. Ihr einst vielbestaunter Hauptschauplatz, die Online-Welt von „Second Life“, ist heute weithin verödet. Die Betreiberfirma entließ im Sommer ein Drittel der Angestellten.

Das Internet ist längst nicht mehr das ganz andere, sondern ein Teil der Realität. Die Leute wollen sich nicht verstecken, sie wollen gefunden werden. Und wer etwas gelten will, tritt wie im echten Leben meist mit Namen auf. Sogar die Rezensionen bei Amazon werden zunehmend namentlich gezeichnet; der Online-Versender ermuntert ausdrücklich dazu. Der echte Name beglaubigt das Urteil – schlechte Zeiten für „katercarlo0815“ oder „nadelhexchen“.

Dumm ist nur, dass dem Einzelnen leicht die Kontrolle darüber entgleitet, was die Netzwelt sich für ein Bild von ihm macht. Das kommt, weil an diesem Bild jeder mitmalen darf: Scherzbolde, Neider und der böse Nachbar – jeder Pinselstrich, Geschmier inklusive, bleibt haften.

„Nun ist das Schlimmste, was du getan hast, oft das Erste, das jeder von dir erfährt.“

Das Internet ist ein Zerrspiegel, es betont und vergrößert das Negative. Denn alles, was im Netz auf Widerspruch gestoßen ist, peinlich war oder einfach nur irgendjemandem nicht gepasst hat, wandert in den Trefferlisten der Suchmaschinen eher nach oben. Solche Sachen werden nun einmal, so sind die Menschen, häufiger verlinkt. „Nun ist das Schlimmste, was du getan hast, oft das Erste, das jeder von dir erfährt“, schreibt der US-Rechtswissenschaftler Jeffrey Rosen.

Günther Oettinger ist einer von vielen, die das bestätigen können: Wer bei Google nach ihm sucht, bekommt schon auf der ersten Seite in gleich vier Fundstellen präsentiert, wie gründlich sich der gelernte CDU-Regionalfürst mit einem Auftritt als designierter EU-Kommissar auf Englisch blamierte – Video inklusive.

Der Ökonom Alessandro Acquisti an der Carnegie Mellon University in Pittsburgh erforscht gerade, wie sich die Verfallszeit von guten und schlechten Informationen unterscheiden. Seine ersten Ergebnisse sind ernüchternd: Das Gerücht, jemand habe einen Preis errungen, verflüchtigt sich schnell. Wird dagegen gemunkelt, er sei betrunken am Steuer erwischt worden, bleibt das hartnäckig in Umlauf.

Das digitale Ich ist viel stärker ein soziales Produkt, als die Menschheit das bisher kannte. Was einer im Netz für eine Figur macht, unterliegt einem stetigen Plebiszit und gelegentlich auch den Launen des Mobs – wohl dem, der da gar nicht erst auffällt.

Fatalerweise erweist sich das Publikum auch noch als erstaunlich leichtgläubig: Dem neuen Medium nimmt es fast alles unbesehen ab.

Wer will, kann sich das zunutze machen. Michael Arrington zum Beispiel, Gründer des angesehenen Technik-Blogs „TechCrunch“, meldete sich spaßeshalber bei Facebook als Google-Chef Eric Schmidt an. Binnen 24 Stunden gewann er dort zahlreiche „Freunde“; unter den ersten waren der Vizepräsident von Facebook und der Gründer des Videoportals YouTube.

Der Kölner Journalist Boris Kartheuser betreibt das Identitäten-Hopping berufsmäßig. Er ist spezialisiert auf verdeckte Recherchen; dafür schlüpft er häufig in fiktive Rollen. Mal gibt er sich als PR-Mann aus, der sich auf eine dubiose Stellenanzeige bewirbt, mal als FDP-Funktionär mit Verbindungen zu Pharmakreisen. So eine Scheinidentität ist im Internet schnell gegründet: Eine schlichte Website, ein Profil beim Berufenetzwerk Xing, vielleicht noch eine Wohnungsanzeige bei ImmoScout.de – das genügt schon, um eine falsche Existenz zu beglaubigen. „Es ist erstaunlich, wie leicht das geht“, sagt Kartheuser.

Mit seiner echten Identität geht der Mann umso vorsichtiger um: Er tritt auch außerhalb des Berufs unter wechselnden Pseudonymen auf, und für seine E-Mails bevorzugt er Wegwerfadressen. Im Internet bewegt er sich wie in Feindesland: von Deckung zu Deckung. „Allein schon über ein Pseudonym, das man aus Bequemlichkeit immer wieder nutzt, lässt sich ja schon sehr viel verknüpfen.“

In der Tat ist die Verknüpfbarkeit scheinbar weit verstreuter Details eines der größten Probleme: Früher konnte man kontrolliert kleinste Teile seiner Identität preisgeben: dem Kollegen die Handy-Nummer, der Freundin die Erzählung eines peinlichen Missgeschicks, einem Dritten die Urlaubspläne. Das alles war kein Problem, denn das Wissen befand sich in Streubesitz. Jeder wusste nur ein bisschen.

Heute lassen sich Linien ziehen von Punkt zu Punkt. Computer verknüpfen alle maschinenlesbaren Spuren zu einem Bild, das einem Porträt immer ähnlicher wird. Es kann sogar Züge enthalten, von denen sonst niemand weiß – zum Beispiel, dass dieser Mensch zu Online-Glücksspielen neigt oder dass er sehr leicht auf vermeintliche Schnäppchenangebote hereinfällt.

Eine Online-Börse wie BlueKai etwa, die im Hauptgeschäft mit Nutzerdaten handelt, erfährt von Tausenden Web-Seiten, was die Besucher dort treiben – von Expedia.com zum Beispiel auch Reiseziele und gewünschte Flugdaten. BlueKai gibt an, jederzeit an die 200 Millionen Menschen mit genauer bestimmten Kaufabsichten im Angebot zu haben, unterscheidbar nach mehr als 30 000 Merkmalen. Über die Börse, heißt es, würden täglich mehr als 75 Millionen Anzeigenplätze versteigert.

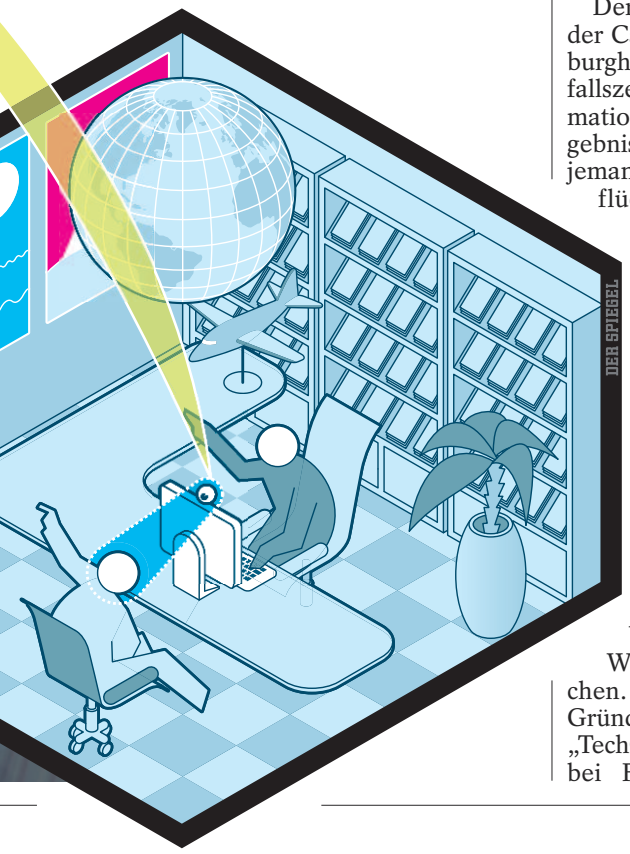
Nicht minder imposant sind die Zahlen der US-Firma AudienceScience: Sie registriert rund 270 Milliarden Aktionen von über 380 Millionen Internetnutzern

Wie funktioniert Gesichtserkennung?

1. Eine Kamera nimmt das Gesicht des Kunden auf. Der Computer erstellt anhand von Merkmalen wie der Gesichtsgeometrie oder dem Haaransatz ein digitales Profil.

2. Dieses wird dann mit den Profilen verglichen, die in großen Datenbanken gespeichert sind.

3. Ist der Kunde einmal identifiziert, kann der Verkäufer wichtige Hintergrundinformationen abrufen.



täglich, von Seitenaufrufen bis hin zu Suchanfragen. Aus diesem Input lassen sich jederzeit für die Werbekunden Zielgruppen nach Maß zuschneiden – stets streng anonym, wie die Firma versichert.

In New York sitzt ein Konkurrent namens Lotame, der ebenfalls eine reichhaltige „Taxonomie menschlichen Verhaltens“ bietet, aber noch einen Schritt weiter geht: Im Auftrag von Targeted Victory, einer Beratungsfirma, half Lotame jüngst den beiden republikanischen Senatskandidaten Dino Rossi und Marco Rubio im Wahlkampf. Die Firma analysierte etwa die Kommentare, die potentielle Wähler im Internet hinterließen, um deren Stimmungslage zu erkunden. Das versetzte die Wahlkämpfer in die Lage, Wechselwähler gezielt zu umgarnen oder überzeugte Multiplikatoren als Unterstützer zu mobilisieren.

Das allgemeine Schlüsseziehen, so scheint es, hat begonnen. Einen Blick in die Zukunft der automatischen Verhaltensanalyse erlaubt das Beispiel der kleinen aufstrebenden Firma Cataphora aus Kalifornien, die für andere Unternehmen das Treiben der Mitarbeiter untersucht.

Cataphora kann dafür alle erdenklichen digitalen Hinterlassenschaften auswerten: Telefonverbindungsdaten, Einträge in elektronischen Kalendern, vor allem aber gespeicherte E-Mails, deren Anzahl bei Großkunden leicht in die Millionen gehen kann.

Diese Datenmassen durchpflügen die Rechner von Cataphora nach Mustern verdächtigen Verhaltens. Manchmal argwöhnt ein Unternehmen etwa, Mitarbeiter könnten Geschäftsgeheimnisse verkauft haben. Die Rasteranalyse könnte dann beispielsweise einen Klüngel von Kollegen zutage fördern, die häufig E-Mails austauschen, obwohl sie keineswegs eng zusammenarbeiten.

Auffällig auch, wenn sie plötzlich häufiger zu Telefonaten überwechseln („Lasst uns das lieber am Telefon besprechen“). Und dann fliegt vielleicht auch noch ein Kollege aus dem E-Mail-Verteiler des Schattennetzwerks, die anderen verkehren nun hinter seinem Rücken. Wollen sie ihm nur eine Geburtstagsüberraschung bereiten? Oder fürchten sie einen potentiellen Verräter?

„Was bei dieser Analyse auffällt, beweist noch nichts, aber es empfiehlt sich dann, genauer hinzusehen“, sagt Markus Morgenroth, bei Cataphora für den europäischen Markt zuständig.

Die Rechner der Firma suchen dabei vor allem nach Schlüsselwörtern, Floskeln oder linguistischen Mustern. Damit lassen sich auch Sozialgefüge und Stimmungslagen innerhalb der Firma ergründen. Zum Beispiel: Wer verteilt Aufgaben immer nur weiter, übernimmt aber selbst wenig? Wer hat öfter mal Redewendungen gebraucht, die auf Frustration, Besorgnis oder Geheimniskrämerei hindeuten? Wann, mit wem und worüber?

Cataphora, seit acht Jahren im Geschäft, war ursprünglich spezialisiert auf Gerichtsverfahren gegen Unternehmen. In den USA müssen dabei oft Millionen E-Mails nach Indizien durchforstet werden. Der Jurist William Herr, lange Jahre als Spezialist für Schadensersatzklagen beim Chemieriesen Dow Chemical beschäftigt, hat öfter mit Cataphora zusammengearbeitet. „Die Firma ist in einem wachsenden Markt ganz vorn dabei“, sagt er. „Als ich zum ersten Mal sah, was die mit unseren alten E-Mails anstellen können, dachte ich mir, ich schreibe im Leben keine E-Mail mehr.“

Nach deutschem Recht ginge so ein Vorgehen nicht so einfach. Doch hiesige Firmen, die mit US-Unternehmen zusammenarbeiten, sind heute schon verpflichtet, ihre E-Mails aufzubewahren für den Fall, dass ihr Geschäftspartner einst vor einem US-Gericht angeklagt wird.

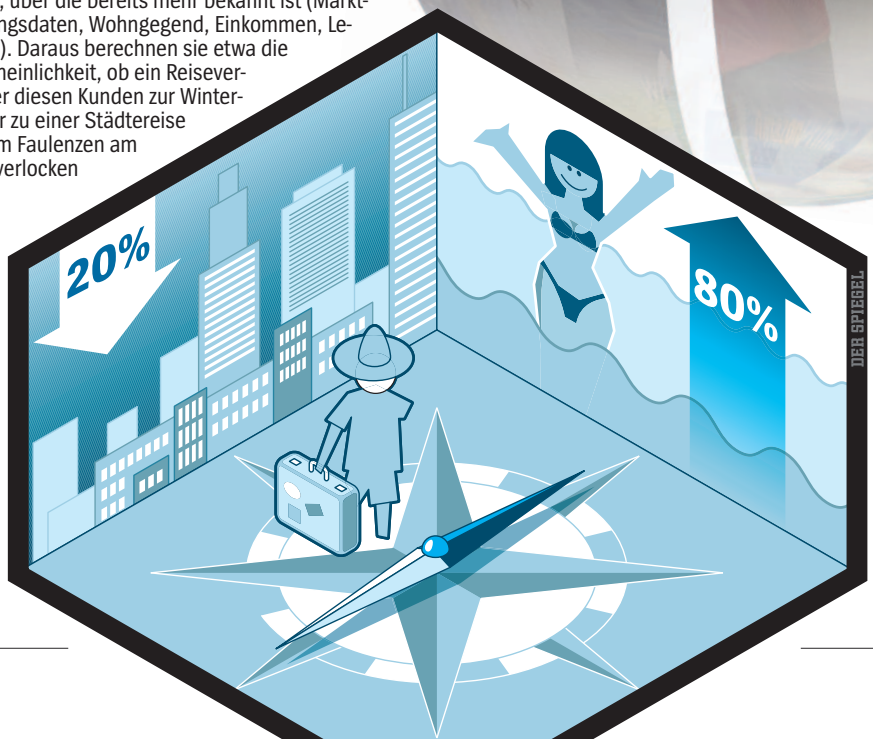
Der neueste Streich von Cataphora ist eine kostenlose Software namens „Digital Mirror“, die es jedem erlaubt, die Verhaltensanalyse im Kleinen an sich selbst zu erproben. Das Programm durchforstet E-Mails und Kalender des Nutzers und zeigt ihm dann etwa an, auf welche Themen er ungehalten reagiert hat und welche Korrespondenzpartner er gern mit kurzen Antworten abbürstet oder mit langen Wartezeiten quält – Ziel: das Optimieren des eigenen Verhaltens.

Die amerikanische Personensuchmaschine Intelius wiederum bietet eine Anwendung namens „Date Check“, mit der sich der nette Unbekannte in der Bar rasch auf seinen Hintergrund abklopfen lässt. Für knapp 15 Dollar pro Anfrage ermittelt die Software übers Internet etwaige Vorstrafen, Haus- und Grundbesitz, die aktuelle Wohnsituation (noch bei Mutti gemeldet?) und die Interessenprofile aus den einschlägigen sozialen und beruflichen Netzwerken.

Das Programm funktioniert nur auf dem US-Markt mit dem schwach ausgeprägten Datenschutz. Aber das wechselseitige Analysieren und Beurteilen von Privatleuten wird auch hierzulande zur Mode. Die Leute gewöhnen sich bereits daran, einander im Internet unentwegt zu bewerten – als Käufer bei Ebay, als Rezensenten bei Amazon, mit dem „Gefällt mir“-Schaltknopf bei Facebook. Speziell Lehrer und Ärzte wissen, wie es ist, im Internet als Gesamtperson benotet zu werden.

VERHALTENS-PROGNOSE

Verhaltensforscher begnügen sich nicht mit dem Sammeln und Kategorisieren von Informationen über Web-Nutzer. Sie versuchen, künftige Entscheidungen und Verhaltensweisen vorherzusagen. Dafür vergleichen sie den Kunden anhand seines Online-Verhaltens mit ähnlichen Nutzern, über die bereits mehr bekannt ist (Marktforschungsdaten, Wohngegend, Einkommen, Lebensstil). Daraus berechnen sie etwa die Wahrscheinlichkeit, ob ein Reiseveranstalter diesen Kunden zur Winterzeit eher zu einer Städtereise oder zum Faulenzen am Strand verlocken könnte.



Unter der Adresse Honestly.com ist gerade ein umstrittenes Reputationsportal in Betrieb gegangen, wo jedermann seine Kollegen, Kunden oder Vorgesetzten bewerten darf. Angeblich der Ehrlichkeit halber sind die Urteile anonym; Kritiker befürchten Exzesse der Niedertracht. Die Firma dagegen setzt auf die Mechanismen der Selbstkorrektur: Auch die Bewertung darf – ebenfalls anonym – bewertet werden; bloße Lästereien sollten folglich mit der Zeit an Gewicht verlieren.

In der Tat fallen die meisten Urteile bislang positiv und kollegial aus. Aber Bruno B., Programmierer bei Google, muss nun damit leben, dass ihm ein Anonymus in der Kategorie „Produktivität“ nur 2 von 10 Punkten zuerkannt hat. Noch härter traf es Richard S., Ex-Manager der Software-Firma VMWare. Ihm wird „Totalversagen“ attestiert; er habe seine Abteilung in den Abgrund geführt.

Gut möglich also, dass der Privatmensch bald genötigt ist, seine öffentliche Erscheinung im Netz wie eine kostbare Ressource zu bewirtschaften. Soziologen sprechen von Reputationsmanagement. Es wird wichtiger in dem Maß, in dem wir uns immer häufiger im Internet übereinander informieren. Internetexperte Jonathan Zittrain vermutet deshalb, dass diese Aufgabe in Zukunft spezialisierte Vermittler, sogenannte Reputationsbroker, übernehmen werden.

Die deutsche Personensuchmaschine Yasni.de strebt diese Rolle auf dem hiesigen Markt an. Schon jetzt kann dort jeder die Liste der Fundstellen zu seinem Namen neu arrangieren: erwünschte Links nach oben stellen, erklärungsbedürftige Funde kommentieren, Namensvettern aussondern. Versprochen ist eine aufgeräumte Repräsentanz im Internet. Die Mitmenschen dürfen sie dann als „glaubwürdig“ bewerten – Flunkerern wird so das Handwerk erschwert. „Schon über eine Million Nutzer haben ein solches ‚Exposé‘ bei uns angelegt“, sagt Yasni-Gründer Steffen Rühl.

In der Tat gibt es Gründe, die persönliche Reputation nicht dem freien Spiel der Kräfte im Internet zu überlassen. Was irgendwelche Suchmaschinen auf Anfrage auswerfen, ist den Zufälligkeiten ihrer Algorithmen und den Launen der Netzwelt überlassen. Selten findet sich jemand durch die Ergebnislisten angemessen dargestellt. Eines der größten Probleme dabei ist, dass es im Internet vor der Vergangenheit kein Entrinnen gibt; es vergisst keinen Murks und keine Dummheit.

So gut wie alles, was der Mensch je gesagt und gezeigt, geblödelt und gemunkelt hat, ruht auf ewig im Speicher, frisch wie am ersten Tag. Der Urheber altert und reift, aber sein Ebenbild im Netz bleibt jung und dumm.

Den kanadischen Psychotherapeuten Andrew Feldmar holte seine Vergangenheit im gesetzten Alter von 66 Jahren ein, und zwar ausgerechnet bei der Einreise

Mit eingebauter Gesichtserkennung wird die Kamera zum Ermittlungsorgan für jedermann.

in die USA. Die Grenzer stoppten den Mann. Sie googelten nach „Andrew Feldmar“ und fanden heraus, dass er mal mit LSD experimentiert hatte – vor fast 40 Jahren. Feldmar darf nun nie wieder US-Boden betreten.

Alles Zusammenleben ist aber darauf eingerichtet, dass Erinnerungen mit der Zeit vergehen, verwittern, verbleichen. Selbst nach einem schweren Fehltritt darf jeder auf einen Neuanfang hoffen. Fürs digitale Ego jedoch ist das Leben ein immerwährendes Examen, und jede Tat geht ein in die Endnote.

Wer begreift, was das bedeutet, wird leicht von einem kreatürlichen Erschrecken gerührt. Deshalb schalten sich jetzt auch die Politiker ein. Innenminister Thomas de Maizière warf das Recht auf einen „digitalen Radiergummi“ in die Debatte, der persönliche Daten nach einer Weile tilgt – freilich ohne zu sagen, wie sich so etwas verwirklichen ließe.

Die originellste Anregung äußerte Google-Chef Schmidt in einem Interview: Junge Leute sollten künftig zum Eintritt ins Erwachsenenleben einfach eine neue Identität bekommen. Dann seien sie nicht mehr mit den Peinlichkeiten in Verbindung zu bringen, die sie in ihren sozialen Netzwerken hinterlassen haben.

Es liefe darauf hinaus, die Jugend komplett in eine Art Zeugenschutzprogramm zu stecken. Hinterher wollte Schmidt das als Witz verstanden haben.

Ohnehin hilft selbst ein neuer Name nichts, wenn dieser eines Tages gar nicht mehr nötig ist, um eine Identität festzustellen. Computer werden immer besser im Erkennen von Gesichtern – und die lassen sich nicht so einfach wechseln.

Als Google vor gut einem Jahr die Software „Goggles“ für Mobiltelefone vorstellte, war die Aufregung groß: „Goggles“ verwandelt die eingebaute Kamera in ein Ermittlungsorgan. Was immer ihr vors Objektiv gerät, versucht sie zu identifizieren: den Protzbau mit der Glaskuppel als Berliner Reichstagsgebäude, die Flasche mit dem angeschimmelten Etikett als Château Pétrus von 1956 – und eines Tages vielleicht auch die kühle Fremde an der Bar als Beatrix, samt Facebook-Profil, den letzten Twitter-Botschaften und dem Eintrag im Telefonbuch.

Die Kamera gleicht, was sie sieht, mit den Abermillionen Bildern ab, die in Googles Suchdatenbank lagern. Gesichter bleiben von der Erkennung zwar einstweilen ausgenommen, wie Google-Chef Eric Schmidt unlängst versicherte. Andere Pioniere aber treiben die Entwicklung umso beschwingter voran.

Die Technik der Firma Viewdle in Kiew etwa, hervorgegangen aus einem Militärforschungsprojekt, kommt bereits bei der Nachrichtenagentur Reuters zum Einsatz: Sie markiert Prominente in Videos – der Betrachter kann direkt zu den Passagen springen, in denen sie erscheinen.

Auch Facebook bietet seit Dezember – zunächst einem begrenzten Mitgliederkreis – Gesichtserkennung. Die Software sucht auf neuen Bildern nach Freunden und Bekannten der Nutzer und trägt automatisch deren Namen ein. Wenn sich die Technik bewährt, dürfte sie als allgemein durchgesetzt gelten. Denn Facebook ist inzwischen nebenbei auch noch die größte Fotoplattform der Welt – allein am Silvesterwochenende wurden 750 Millionen Schnappschüsse hochgeladen.

Wohlweislich sind die Programme bislang beschränkt auf das erklärte Umfeld der Nutzer. Die Firmen betreten dieses Minenfeld mit großer Vorsicht. Früher oder später aber dürfte das große Erkennen in den Weiten des Internets beginnen – zu groß ist die Macht der Neugier.

Auch der Werbewirtschaft käme die Technik gewiss nicht ungelegen. Das Gesicht des Kunden würde dann quasi als unlöschbares Cookie dienen, und die Kamera vorm Kaufhaus könnte ihn unbemerkt beim Vorbeischlendern erkennen. Spätestens dann stellt sich die Frage, ob es eines Tages schon als Übergriff zählen wird, Fotos anderer Leute irgendwo im Netz zu veröffentlichen.

Der Informatiker Michael Backes an der Universität des Saarlandes will dem Netzbürger zumindest eine gewisse Kontrolle über die eigenen Bilder ermöglichen. Am Dienstag dieser Woche stellt er im Berliner Ministerium für Verbraucherschutz ein kleines Zusatzprogramm für den Webbrowser Firefox vor, das jedes Bild verschlüsselt, ehe der Anwender es bei Facebook, Picasa oder sonstwo hochlädt. Wer das Foto ansehen will, bekommt automatisch den Schlüssel zugespielt – aber nur, solange der Urheber das will. Dieser kann jederzeit für beliebige Bilder den Schlüssel zurückziehen.

Die Technik namens X-pire funktioniert elegant und fast ohne Zutun des Nutzers; er könnte etwa die Laufzeit generell auf ein Jahr beschränken und nur ausgewählte Fotos auf Dauer ins Netz stellen. Die Entscheidung ist jederzeit revidierbar.

Doch wirkt auch hier der Fluch des Digitalen: Suchmaschinen schaufeln be-

kanntlich das ganze erreichbare Internet in ihre Speicher – dort wären auch die Fotos, die der Urheber bereits gesperrt hat, weiter problemlos abrufbar. Deshalb ist bei X-pire eine kleine Schikane eingebaut: Wer ein Bild sehen will, muss ein „Captcha“ entziffern, ein Bildchen aus krummen Buchstaben, die für Computer kaum zu lesen sind. So sollen die Suchmaschinen ferngehalten werden. Aber der kleine Umstand könnte auch menschliche Betrachter nerven.

Wer das Bild beizeiten kopiert hat, kann damit ohnehin machen, was er will. „Gegen das Kopieren kann es technisch keinen Schutz geben“, sagt Backes. „Zur Not nimmt man eine Kamera und knipst das Bild auf dem Monitor.“ Dennoch hält der Forscher seine Software für einen guten Anfang: „Im Alltag genügt es ja meist, die Hürden zu erhöhen.“

Für die Zukunft sind gewiss radikalere Methoden gefragt. Jonathan Zittrain, Professor an der Harvard Law School, fordert das Recht auf eine Art Privatinsolvenz des digitalen Ich. Zittrain spricht von „Reputationsbankrott“. Etwa alle zehn Jahre, meint der Jurist, solle jeder auf Wunsch kompromittierende Daten tilgen können.

Zittrains Kollege Viktor Mayer-Schönberger, Professor in Oxford, hat in seinem Buch „Delete“ auch schon skizziert, wie sich ein solches Recht auf Vergessen umsetzen ließe: Alle Rechner müssten so konstruiert werden, dass die jeweiligen Daten zu einem vorgegebenen Verfallsdatum automatisch verlöschen – technisch wäre das möglich. Aber ob es sich je durchsetzen lässt?

Wenn das Vergessen so schwierig ist, liegt die Zukunft möglicherweise eher in einer allgemeinen Kultur des Verzeihens: Wo alle alles voneinander erfahren können, erschöpft sich vielleicht auch die Lust am Skandalisieren. In den Straßen von Holland gestatten bekanntlich oft große Fenster den freien Blick in die Wohnzimmer – und kaum jemand guckt. Vorhänge gelten den Holländern als merkwürdig. Wäre also offensive Freizügigkeit nicht das beste Mittel, die Neugier der Mitwelt durch Überangebot zu zermürben?

Wenn alle alles voneinander wissen, erschöpft sich vielleicht auch die Lust am Skandalisieren.

Die Datenschützer mögen sich damit nicht begnügen. Sie fordern stattdessen Härte ein: Die US-Sozialforscherin Danah Boyd, Expertin für soziale Netze, würde Facebook am liebsten wie einen öffentlichen Versorgungsbetrieb unter Aufsicht stellen. Und auch in Europa regt sich Widerstand gegen die Sammelwut der Internetkonzerne: EU-Kommissarin Viviane Reding will den Datenschutz neu regeln. Anfang November legte sie einen Entwurf vor, der ein „Recht vergessen zu werden“ enthält. Die Bürger sollen jederzeit das Tilgen ihrer Daten verlangen können.

Die Privatsphäre, so fordern Datenschützer, soll als Regel gelten, nicht als Ausnahme. Das allerdings ist politisch schwer durchzusetzen, zumal gegenüber Firmen im Ausland. Die Berliner Koalition hat das Thema immerhin erkannt, so wenig Handfestes daraus auch bisher erwachsen ist.

Verbraucherschutzministerin Ilse Aigner machte vor allem in der Debatte um „Street View“ mit aufgeregten Wortmeldungen auf sich aufmerksam – obwohl sie für den Datenschutz allenfalls am Rande zuständig ist.

Innenminister de Maizière wiederum stellte im Dezember einen Gesetzentwurf vor, demzufolge private Unternehmen weiterhin nach Herzenslust Daten sammeln dürfen. Nur für das Veröffentlichen will er eine „rote Linie“ ziehen: „Je mehr Daten über Private gesammelt, miteinander verknüpft und veröffentlicht werden, desto größer ist die Gefahr von gravierenden Verletzungen des Persönlichkeitsrechts“, sagt de Maizière. „Wir benötigen hier eine Grenze, die mit klaren Sanktionen und Schmerzensgeld bewehrt ist.“

Zudem arbeite man an Regeln für das Sammeln von Aufenthaltsdaten, sagt Rainer Stentzel von der Projektgruppe Netzpolitik im Bundesinnenministerium. Auch die Gesichtserkennung per Software soll eingeschränkt werden.

Ansonsten setzt de Maizière eher auf freiwillige Selbstverpflichtungen der Industrie. Der Hintergedanke: Wenn die Sorge um den Datenschutz um sich greift, könnten Firmen sich die Kundschaft durch klare Regeln gewogen machen.

Ob der Bürger diese wirklich zu würdigen weiß, wird sich erweisen. Bisher zeigte er sich recht lernfaul. „Ich verstehe nicht, warum 90 Prozent zum Suchen noch Google nutzen“, sagt Datenschützer Weichert. „Es gibt schließlich längst sichere Suchmaschinen wie Ixquick, die keine Nutzerdaten speichern.“

Ein Feldversuch des US-Ökonomen Alessandro Acquisti ergab: Viel hängt davon ab, wie die Leute die allgemeine Lage beurteilen.

Der Forscher verteilte in einem Einkaufszentrum Gutscheine über 10 Dollar. Dann bekamen die Beschenkten 12 Dollar zum Tausch geboten – sie mussten dafür allerdings Name und Adresse angeben. Nur jeder zweite Passant ließ sich so billig kaufen.

Dann aber drehten die Forscher hinterlistig die Reihenfolge um. Sie verteilten erst die 12-Dollar-Gutscheine. Wer diese anschließend umtauschte gegen 10 Dollar, bekam dafür seine Daten zurück. Nun wollte nur noch einer von 10 Probanden seine Beute wieder hergeben.

Offenbar lassen sich die Leute von der Ausgangssituation leiten: Haben sie den Eindruck, die Privatsphäre sei geschützt, so schätzen sie das hoch. Falls nicht, ist sie ihnen auch nichts mehr wert.

MANFRED DWORSCHAK

ABWEHRSTRATEGIEN

Im Netz zu surfen und sich gleichzeitig vor allen digitalen Spähern abzuschotten ist schier unmöglich. Dennoch gibt es einige Möglichkeiten, seine Privatsphäre besser zu schützen.

Spione ausschalten

In jedem Browser kann sich der Nutzer die installierten Cookies anzeigen lassen und diejenigen entfernen, die ihm nicht geheuer sind. Es ist aber nicht ganz einfach, „gute“ Cookies, die für den Nutzer hilfreich sind, von den lästigen Spionen zu unterscheiden.

Anonyme Suchmaschinen verwenden

Die Suchmaschine Ixquick etwa speichert keine Nutzerdaten; sie ist nach EU-Datenschutzrecht geprüft.

Wechselnde Anmeldenamen nutzen

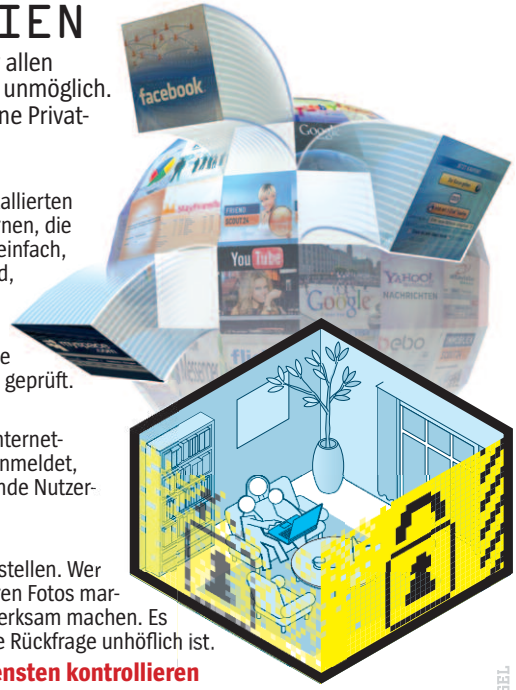
Wer sich bei Web-Foren, Online-Portalen und Internethändlern immer mit dem selben Pseudonym anmeldet, erleichtert es den Datensammlern, übergreifende Nutzerprofile zu erstellen.

Vorsicht mit Fotos

Möglichst keine Fotos von sich selbst ins Netz stellen. Wer sich etwa daran stört, dass Freunde ihn auf ihren Fotos markiert („getaggt“) haben, sollte sie darauf aufmerksam machen. Es spricht sich langsam herum, dass Taggen ohne Rückfrage unhöflich ist.

Sicherheitseinstellungen bei Online-Diensten kontrollieren

Google etwa bietet über die Option „Dashboard“ einen komfortablen Zugriff auf vieles, was über den jeweiligen Nutzer gespeichert ist. Auch andere Firmen folgen dem Beispiel. Allerdings muss der Kunde noch bei jeder Firma einzeln tätig werden.



DER SPIEGEL