

1/1
GANZE SEITE

Datenschutz



INHALT

- 70 *Die Verknüpfung von Daten bedroht ein Grundrecht*
- 71 *Das Deutschland-Netz*
- 72 *Die kleinen Spione der großen Konzerne*
- 76 *Wenn den Staat die Sammelwut packt*
- 77 *So schützen Sie ihre Privatsphäre*

BEI JEDEM KLICK IM NETZ, jedem Behördengang, jedem Einkauf hinterlassen wir Daten. Das macht den Alltag zwar bequemer, ermöglicht anderen jedoch auch, *detaillierte Profile von uns zu erstellen*. Was mit unserem Datenschatten geschieht, können wir längst nicht mehr kontrollieren. *Viele wollen das nicht mehr hinnehmen*: Sie sind beunruhigt, mit welcher ausgefeilten Methoden KONZERNE WIE FACEBOOK oder Google Daten sammeln, während BEHÖRDEN neue Vollmachten bekommen, die Bürger digital zu vermessen. Die Sorge um den Datenschutz wird zur *Sorge um die Bürgerrechte* in einer digitalen Welt.

Dossier

Thema

Die wachsende Gier

Die zunehmende Vernetzung verleitet Staat und Wirtschaft dazu, immer mehr Daten über uns zu sammeln – ein GRUNDRECHT ist in Gefahr

Kaum ein Monat vergeht, ohne dass Datenschützer Alarm schlagen: Zum Beispiel, weil das soziale Netzwerk Facebook ankündigt, die Profildaten seiner Nutzer an Dritte zu verhöckern. Weil Google dabei erwischt wird, wie es mithilfe seiner **Streetview**¹-Fahrzeuge den Datenverkehr privater Funknetze aufzeichnet, angeblich aus Versehen. Oder weil Konzerne wie die Telekom oder die Bahn die digitale Post ihrer Mitarbeiter ausspähen.

Dass die Gier nach unseren Daten wächst, hat einen einfachen Grund: Es gibt immer mehr davon. In unserer voll vernetzten Gesellschaft hinterlassen wir ständig digitale Spuren. Bei jedem Gang zum Geldautomaten, jedem Klick im Internet, jedem Behördenbesuch geben wir etwas über unsere Gewohnheiten, Bedürfnisse und Vorlieben preis – so wächst ein digitales Alter Ego heran.

Löschen können wir die meisten dieser Informationen jedoch nicht mehr, das Netz vergisst nichts. Jeder, der schon einmal in einem Internetforum auf einen Jahre alten, unbedacht geschriebenen Beitrag von sich gestoßen ist, kennt die Hilflosigkeit, ihn nicht mehr löschen zu können. Das verleitet manche zu dem Fatalismus, die Tage des Datenschutzes seien gezählt. Andere versichern trotzig, man habe ohnehin nichts zu verbergen. Solange das digitale Ich unbescholten sei, entstünden ja auch keine Nachteile.

Eine problematische Haltung. Sie zeugt von einem mangelnden Verständnis des Rechtsstaats, und sie ist naiv. Im **Volkszählungsurteil**² von 1983 hat das Bundesverfassungsgericht das Recht auf »informationelle Selbstbestimmung« zum Grundrecht erhoben, abgeleitet von der Unverletzlichkeit der Menschenwürde und dem Recht auf freie Entfaltung der Persönlichkeit – Grundrechten, die über Jahrhunderte erstritten wurden. Informationelle Selbstbestimmung heißt: Wer welche Informationen über eine Person wozu verwenden darf, entscheidet diese selbst.

Grundrechte bedürfen keiner Rechtfertigung, wenn sie in Anspruch genommen werden. Sie gelten

bedingungslos. Wer also Informationen über sich, und seien sie noch so unerheblich, nicht preisgeben will, muss das nicht begründen. Selbst nach dem 11. September nicht, auch im Internetzeitalter nicht.

Nun sind Daten ein begehrtes Gut. Unternehmen wollen wissen, wie sie Verbrauchern ihre Produkte schmackhaft machen können. Sicherheitsbehörden wollen wissen, welche Bürger Kriminelles im Schilde führen. Das ist natürlich in Ordnung.

Nicht in Ordnung ist jedoch, wenn sie dabei maßlos werden. Wenn Unternehmen Daten mit technischen Tricks abfischen oder gar Kunden regelrecht ausspähen (siehe Seite 72); wenn Behörden Informationen erzwingen, ohne die Verhältnismäßigkeit zu wahren (siehe Seite 76).

Noch bedenklicher wird es, wenn Behörden oder Konzerne ohne Kontrolle durch die Betroffenen die Informationen, die in unzähligen Datenbanken gespeichert sind, zusammenführen – Daten, die eigentlich nur zur einmaligen Verwendung preisgegeben wurden. Denn verknüpfte Daten können Dinge enthüllen, die der Verbraucher, der Bürger vielleicht nicht öffentlich machen will.

Diese neue Stufe der Vernetzung unterminiert das Recht auf informationelle Selbstbestimmung – wir riskieren eine dauerhafte Überwachung durch Big Brother und die Little Brothers aus der Wirtschaft.

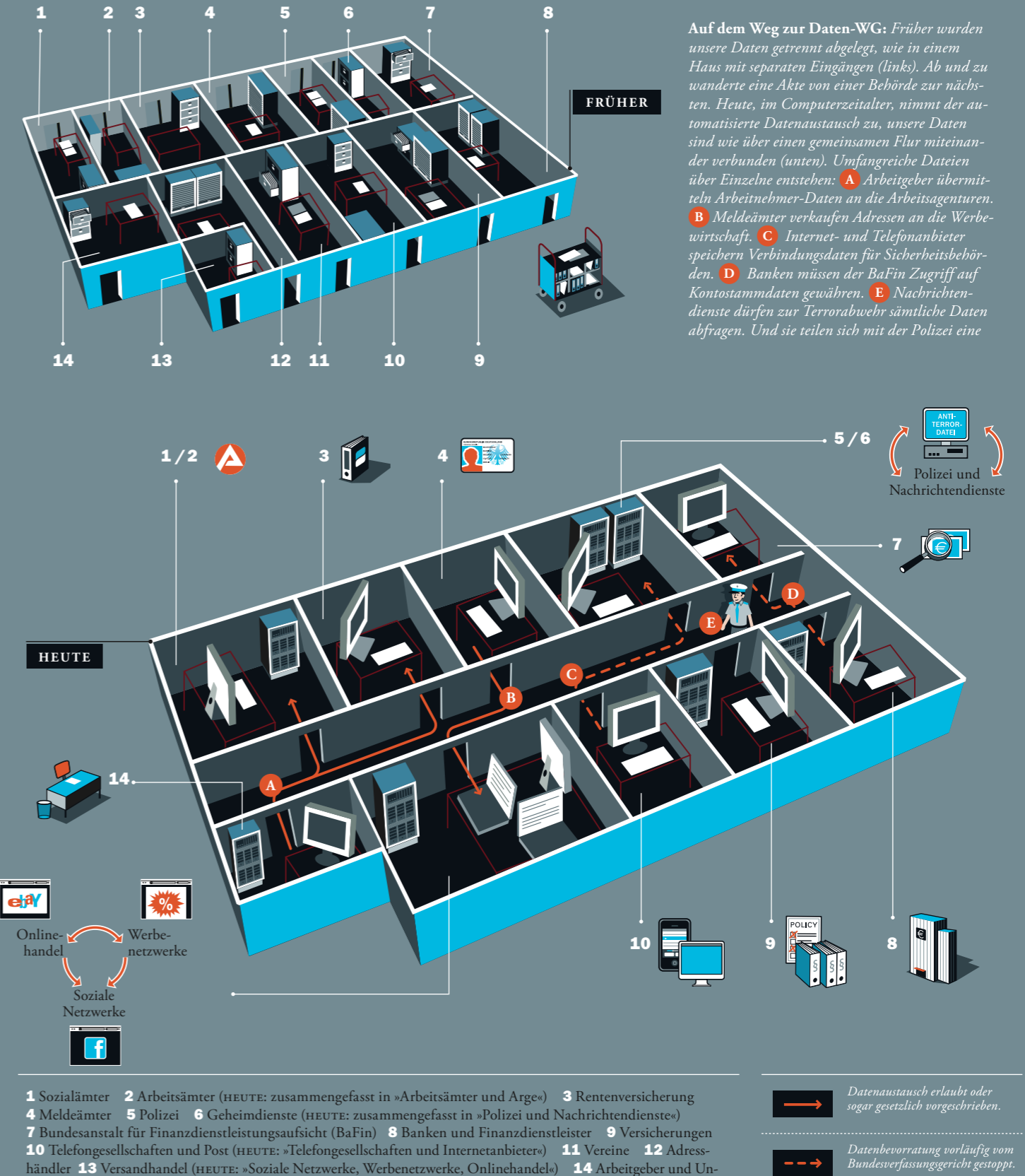
Lange Jahre schien diese Gefahr nur Datenschützer und Bürgerrechtler zu beschäftigen – doch nun wacht allmählich auch die Zivilgesellschaft auf. Internetautoren rufen zum Boykott von Facebook auf. Mit einer erfolgreichen Verfassungsklage haben 35 000 Deutsche die unmäßige Vorratsdatenspeicherung vorerst zu Fall gebracht. Und mit der Piratenpartei ist sogar eine politische Partei entstanden, deren zentrales Anliegen die Verteidigung der informationellen Selbstbestimmung ist.

Dieser Protest ist überfällig: Wer meint, Datenschutz sei ein Luxus, den wir uns nicht leisten können, will nichts weniger als einen anderen Staat. Ein Rechtsstaat, wie wir ihn kennen, wäre es nicht mehr. —

¹ **Google Streetview** ergänzt den Google-Dienst Google Earth durch Straßenansichten, die aus 360-Grad-Panoramabildern erzeugt werden. Diese werden von Kamerawagen mit je acht Kameras und drei Laserscannern aufgenommen. Die Idee ist, möglichst vollständige virtuelle Abbilder von Städten im Internet zu schaffen. Das Problem: In den Bildern stecken auch jede Menge privater Informationen über Häuser, die zum Beispiel Einbrüche erleichtern könnten.

² **Volkszählungsurteil** Grundsatzentscheidung des Bundesverfassungsgerichts (BVG) vom 15. Dezember 1983 zur ursprünglich für das Frühjahr 1983 angesetzten Volkszählung. Das BVG erklärte das Gesetz, das die Volkszählung regelte, für verfassungswidrig und gab damit mehreren Verfassungsbeschwerden recht. Das Urteil gilt als Meilenstein in der Entwicklung des Datenschutzes. Die Volkszählung wurde deshalb unter geänderten Bedingungen erst 1987 durchgeführt.

Wo in Deutschland die Daten lagern



Auf dem Weg zur Daten-WG: Früher wurden unsere Daten getrennt abgelegt, wie in einem Haus mit separaten Eingängen (links). Ab und zu wanderte eine Akte von einer Behörde zur nächsten. Heute, im Computerzeitalter, nimmt der automatisierte Datenaustausch zu, unsere Daten sind wie über einen gemeinsamen Flur miteinander verbunden (unten). Umfangreiche Dateien über Einzelne entstehen: **A** Arbeitgeber übermitteln Arbeitnehmer-Daten an die Arbeitsagenturen. **B** Meldeämter verkaufen Adressen an die Werbewirtschaft. **C** Internet- und Telefonanbieter speichern Verbindungsdaten für Sicherheitsbehörden. **D** Banken müssen der BaFin Zugriff auf Kontostammdaten gewähren. **E** Nachrichtendienste dürfen zur Terrorabwehr sämtliche Daten abfragen. Und sie teilen sich mit der Polizei eine

ANTI-TERROR-DATEN
Polizei und Nachrichtendienste

Onlinehandel
Werbenetzwerke
Soziale Netzwerke

Datenaustausch erlaubt oder sogar gesetzlich vorgeschrieben.
Datenbevorratung vorläufig vom Bundesverfassungsgericht gestoppt.

Die kleinen Spione der großen Konzerne

Es ist ein einfaches Experiment: Man stelle den Laptop eines Freundes neben den eigenen Computer. Dann gebe man auf beiden Rechnern auf der Google-Suchseite das Stichwort »Krankenversicherung« ein. Wer nun beide Enter-Tasten gleichzeitig drückt, wird feststellen, dass die Suchergebnisse und Textanzeigen, die Google auf den beiden Rechnern ausgibt, nicht identisch sind. Da kann es etwa passieren, dass Google auf dem einen Gerät Links zur gesetzlichen Krankenversicherung ganz oben platziert, auf dem anderen hingegen privaten Krankenversicherungen den Vorzug gibt.

Denn Google lernt und kombiniert wie ein Profiler. Aus all den Begriffen, die man im Laufe der Zeit googelt, gewinnt der Internetgigant aus Kalifornien ein immer feiner aufgelöstes Bild des Nutzers, dem er dann möglichst mundgerechte Informationen – und das heißt vor allem: Onlinewerbung – serviert. Google ist berüchtigt für den Umfang seiner Datensammelei und die notorische Intransparenz ihrer Verarbeitung. Aber auch viele andere Unternehmen zapfen die Daten an, die bei jedem Klick, bei jeder Verbindung in einem sozialen Netzwerk und zunehmend auch bei Handytelefonaten anfallen.

Das geschieht zwar schon seit den Anfangstagen des World Wide Web. Doch die technischen Möglichkeiten entwickeln sich so rasant weiter, dass Daten- und Verbraucherschützer kaum hinterherkommen. Und viele Verbraucher ahnen gar nicht, wie sie manipuliert und durchleuchtet werden können.

»Eines der schwierigsten Felder im Netz ist aus unserer Sicht das Behavioral Targeting«, sagt Falk Lüke vom Verbraucherzentrale Bundesverband (vzbv). »Hier wird ohne Wissen der Verbraucher eine Historie ihres Verhaltens im Web erstellt, um daraus Informationen über sie zu gewinnen.« Was klickt ein Nutzer an, wie lange verharrt er auf einer Seite, in welcher Reihenfolge ruft er Webseiten auf? Antworten auf diese Fragen gewinnen Werbenetzwerke mithilfe ausgefeilter Datenanalysen. Dafür wird der Nutzer – genauer gesagt: sein Browser – am Anfang des Prozesses einmal mit einer Kennnummer versehen, die in der Datenbank des Werbenetzwerks gespeichert wird.

Dies kann über kleine Zusatzdateien (Cookies und **Flash-Cookies**³) oder über eingebettete Einzelpixel (**Beacons**⁴) geschehen. Jeder Inhalt, den der Nutzer daraufhin anklickt, lässt sich dann über diese kleinen Hilfsmittel der Kennnummer zuordnen. Dank neuer Rechenverfahren und leistungsfähiger Computer entstehen aus den Historien in Windeseile Verhaltensprofile. Bei der nächsten passenden Gelegenheit schickt das Werbenetzwerk dem Nutzer eine auf ihn zugeschnittene Anzeige auf den Bildschirm.

»Behavioral Targeting ist erfolgreicher als herkömmliche Online-Werbung«, sagt Howard Beal von der George Washington University in Seattle und kann dies mit Zahlen belegen. In einer Studie fand er heraus, dass 12 der 15 größten Online-Werbenetzwerke die Nutzer mittels Behavioral Targeting rund zweieinhalb Mal häufiger als mittels klassischer Bannerwerbung dazu bringen konnten, etwas zu kaufen. Der Erfolg hat sich herumgesprochen: Gaben US-Firmen 2006 erst 350 Millionen Dollar für Behavioral Targeting aus, waren es 2009 bereits über eine Milliarde Dollar.

Wo ist das Problem, solange es sich nur um Werbung handelt?, könnte man einwenden. Wer ohnehin gern verreist, wird sich an einer Anzeige für einen Schnäppchenflug auf seine Lieblingsinsel nicht stören. Wer übers Internet viele Kochbücher kauft, freut sich womöglich über Anzeigen für Kochtöpfe.

Das erste Problem ist, dass manche Online-Anbieter die Menschen über das Ausmaß der Datenerhebung schlicht belügen. Ein Beispiel ist der Levis Online Store, den Catherine Dwyer von der Pace University in New York untersucht hat. In seiner Datenschutzerklärung weist Levis zwar explizit darauf hin, dass die Firma Avenue A anonymisierte Daten des Online-Käufers erhebt. In einer einfachen Analyse fand Dwyer aber heraus, dass bei einem Seitenaufwurf des Online-Stores neun andere, nicht erwähnte Werbefirmen digitale Kennungen auf dem Rechner des Nutzers platzieren, um damit Daten zu gewinnen. Eine Firma las gar Kontaktdaten aus, die den Nutzer persönlich identifizieren konnten.

Das zweite Problem ist, dass die Verbraucher nur eine unzureichende Kontrolle über diese Datensammelei haben. Flash-Cookies und Beacons lassen sich nicht deaktivieren. Gewöhnliche Cookies zwar schon – allerdings muss man sich bislang aktiv dagegen entscheiden, im Fachjargon »Opt-out« genannt. Und viele Nutzer wissen nicht, wo in den Einstellungen eines Browsers sie das entsprechende Häkchen entfernen müssen. »Unsere Position ist, dass User der Nutzung solcher Techniken immer per Opt-in zustimmen müssen«, sagt Falk Lüke vom vzbv. Die im November 2009 verabschiedete **ePrivacy-Richtlinie**⁵ der EU interpretieren Datenschützer wie der Bundesbeauftragte Peter Schaar dahingehend, dass Online-Dienste den Gebrauch von Cookies sich beim erstmaligen Ansurfen genehmigen lassen müssen. Einige Internetrechtler hingegen teilen diese Auslegung nicht.

3 Flash-Cookies
Dateien, die Angaben über den Rechner eines Nutzers enthalten und von Seiten mit Flash-Animationen erzeugt werden. Während klassische Cookies nur für einen bestimmten Browser wie Firefox gelten, sind Flash-Cookies browserunabhängig.

4 Beacons
In Webseiten oder E-Mails eingebettete Bilddateien, die nur ein Pixel groß sind. Über die Kommunikationsdaten des Internetprotokolls verrät ihr Aufruf Uhrzeit, Browser, Betriebssystem und IP-Adresse des Nutzers. Hilfsprogramme können sie sichtbar machen.

5 ePrivacy-Richtlinie
EU-»Datenschutzrichtlinie für elektronische Kommunikation« (2002/58/EC), die erstmals 2002 in Kraft trat. In der neuen Fassung, die die EU-Staaten bis Mai 2011 umsetzen müssen, werden Firmen verpflichtet, den Diebstahl von Kundendaten bekannt zu machen. Nutzer sollen juristisch leichter gegen Spam-Belästigungen vorgehen, Datenschützer Rechtsbrüche besser ahnden können.

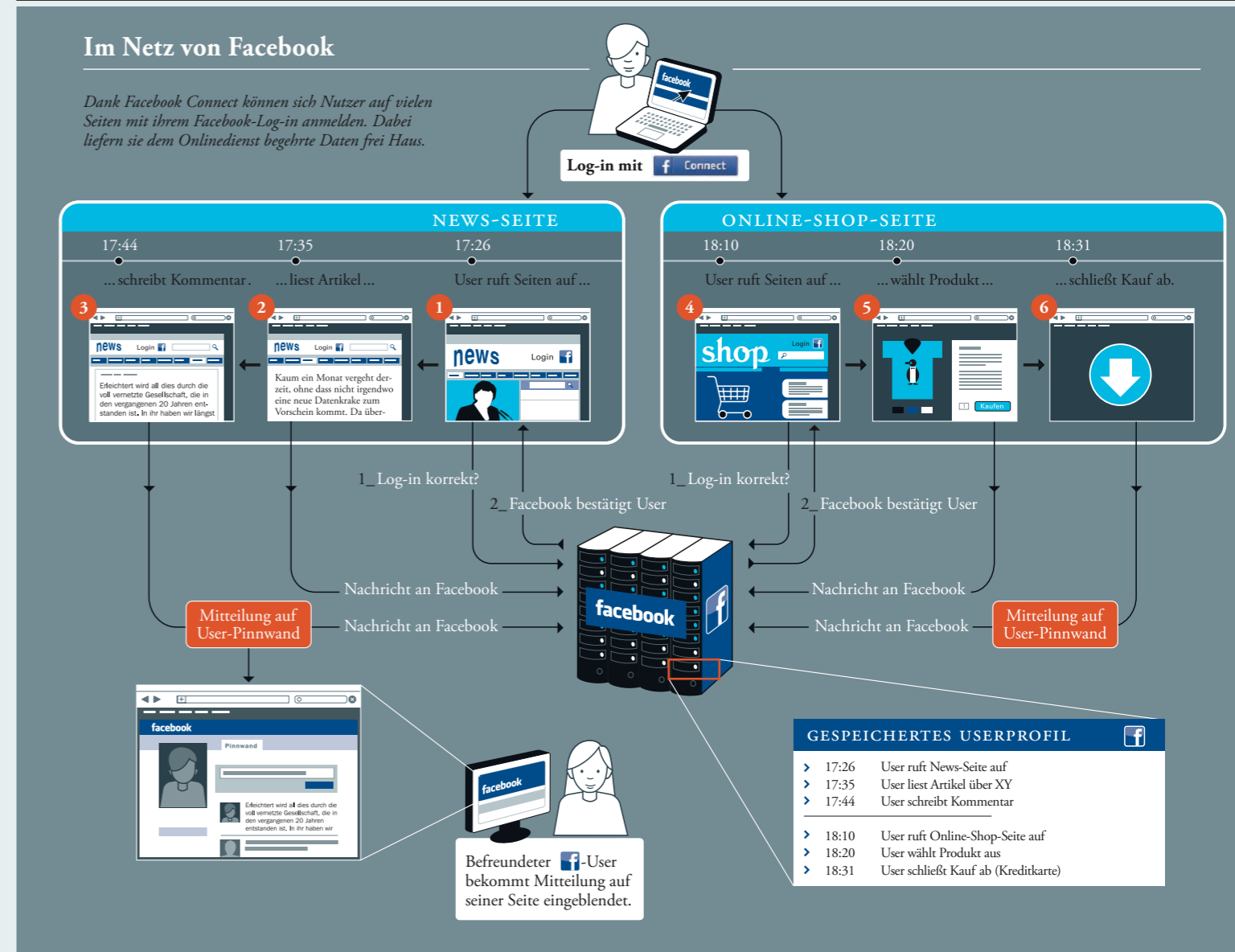
6 Facebook
Die Firma im kalifornischen Palo Alto betreibt das größte soziale Netzwerk der Welt. Während die Konkurrenz spezielle Nutzergruppen anzieht – MySpace: Musiker, StudiVZ: Studierende, XING: Angestellte, Freiberufler –, vereint Facebook alle Milieus.

Nehmen wir nun an, jemand habe derartigen Praktiken in seinem Browser selbst einen Riegel vorgeschoben – ist er dann auf der sicheren Seite? Leider nein: Denn es gibt noch ganz andere Möglichkeiten des Profiling. Ein Beispiel ist das soziale Netzwerk **Facebook**⁶, das wegen seines laxen Umgangs mit Datenschutz seit Monaten Schlagzeilen macht. Gut 400 Millionen Menschen haben sich angemeldet, von denen nicht wenige dort »leben«: Sie tauschen sich mit ihren Freunden aus – die sie mitunter noch nie gesehen haben –, veröffentlichen private Fotos, vielleicht sogar intime Gedanken. Obwohl viele sich durchaus der Tatsache bewusst sind, dass sie damit öffentlich existieren, unterschätzen sie doch die Macht der Daten.

Da ist etwa der »Gefällt mir«-Button: Mit dem kann ein Facebook-Nutzer im Netz Inhalte markieren, die ihm gefallen. Diese Inhalte sind dann aber nicht nur mit ihm verknüpft, sondern automatisch auch mit

seinen Facebook-Kontakten. Facebook, das Unternehmen, kann solche Verbindungen auswerten – und erlaubt im kürzlich gestarteten »Instant Personalization«-Programm einigen Empfehlungsmaschinen Zugang zu den Daten.

haben ein paar Freunde ein bestimmtes Produkt gekauft und es gleich noch mit dem Klick auf den Gefällt mir-Button geadelt, könnte nun auf der eigenen Facebook-Seite eine entsprechende Empfehlung auftauchen: »Deine Freunde Benny, Kalle, Anne und Sven haben X gekauft. Check das mal.« Dass solche Tipps viel mehr Überzeugungskraft haben als gewöhnliche Werbung, ist in der Marketingforschung seit Langem bekannt. Im Netz können sie jedoch viel schneller und direkter platziert werden als in der Offline-Welt. Na-



türlich hat Facebook seine Nutzer nicht gefragt, ob sie in den Genuss des Programms kommen wollen, sondern es kurzerhand eingeschaltet.

Die Analyse von Freundesnetzwerken lässt weitere Schlüsse zu, wie etwa die Informatiker Carter Jernigan und Behram Mistree vom Massachusetts Institute of Technology (MIT) im Oktober 2009 in einer aufsehenerregenden Studie zeigten. Sie demonstrieren anhand von 4080 Facebook-Profilen aus dem MIT-Netzwerk, dass sich aus einer statistischen Analyse, wer mit wem auf Facebook befreundet ist, mit 78-prozentiger Wahrscheinlichkeit auf die Homosexualität von männlichen Nutzern schließen lässt – und zwar auch dann, wenn diese sie bewusst nicht offen angeben. Bereits im April 2009 hatten zwei Informatiker der Universität von Texas in Dallas mit einer Analyse von 167 000 Nutzern belegt, dass sich allein aus den Freund-Verknüpfungen auf die politische Haltung eines Nutzers schließen lässt, auch wenn der sie nicht explizit vor sich her trägt.

Die Ergebnisse ihrer Studie, schreiben Jernigan und Behram, könnten für solche Nutzer ein Einbruch in die Privatsphäre sein. Nur: »Unsere Studie nutzt keine anderen Informationen als die, die schon öffentlich auf Facebook zugänglich sind.« Den Nutzern entgleite die Kontrolle über persönliche Informationen,

schreiben die Forscher: »Wer sagt uns, dass Unternehmen nicht schon derartige Netzwerkanalysen hinter verschlossenen Türen durchführen?«

Mit dem Siegeszug der Internet-Handys wie dem iPhone hat sich zudem ein neues Feld für die Nutzeranalyse eröffnet. Eine der ersten Firmen, die sie betreibt, ist Sense Networks aus New York, hervorgegangen aus einem Forschungsprojekt am MIT. Sie verfolgt anhand von Gesprächsdaten, wie sich Handynutzer durch die Stadt bewegen, weil jedes Gespräch über die Sendemasten der **Funkzellen**⁷ zu einem bestimmten Zeitpunkt einem Ort zugeordnet werden kann. In den USA dürfen Mobilfunkbetreiber solche Daten anonymisiert verkaufen. Die Handynutzer sind dann »Knoten« in einer mathematischen Struktur, die als **Graph**⁸ bezeichnet wird. Ein einfaches Beispiel für einen Graphen ist ein U-Bahn-Netzplan.

Aus den ungleich komplexeren Mobilfunkgraphen kann Sense Networks – in Abhängigkeit von Ort und Zeit – Nutzergruppen herausdestillieren. Ein Beispiel: Wer in einem trendigen Stadtteil wohnt, sich tagsüber im Bankenviertel und abends in einer Gegend mit teuren Szenereaurants aufhält und dann häufig

⁷ **Funkzelle**

Der Raum, in dem der Sendemast eines Mobilfunknetzes Handysignale überträgt oder empfängt. Jedes Handy ist dabei mit einer ID-Nummer in der Zelle angemeldet.

⁸ **Graph**

In der Graphentheorie der Mathematik eine Menge von Punkten, deren Beziehungen untereinander durch Linien dargestellt werden.

Allein mithilfe der Handyortung können Firmen Spitzenverdiener identifizieren.

mit Leuten telefoniert, die ein ähnliches Bewegungsprofil haben, kann mit einiger Sicherheit in die Gruppe von Spitzenverdienern einsortiert werden. Diese Information kann Sense Networks wiederum an Werbenetzwerke verkaufen, die passende Werbung auf die Handys schicken.

»Vor fünf Jahren hätte man solche Analysen noch nicht machen können«, sagt Vincent Blondel, Data-Mining-Forscher an der Université Catholique im belgischen Löwen. Damals hätte es noch keine geeigneten Algorithmen gegeben, um Netzwerke mit Millionen Knoten schnell zu analysieren. »Heute können Sie die mathematische Auswertung über fünf, sechs Ebenen bis an eine einzelne Person heranzoomen«, sagt Blondel. Er selbst hat in einer Untersuchung der Daten von zwei Millionen belgischen Handynutzern festgestellt, dass französisch und niederländisch sprechende Belgier in zwei getrennte Gruppen zerfallen, die miteinander so gut wie gar nicht kommunizieren – und damit ein Abbild der kulturellen Spaltung Belgiens produziert.

In der Datenschutzdebatte hat man sich lange damit beruhigt, dass alle, die Datenmassen anhäufen, kaum in der Lage wären, sie sinnvoll zu verarbeiten. Das ändert sich allmählich. Solange Datensätze anonymisiert sind und ihre Analyse Verbrauchern noch mehr

Werbung beschert, ist das nur ein Ärgernis. Der Übergang zur gezielten Manipulation ist jedoch fließend.

Besonders heikel wird es, wenn die Anonymität der Daten verloren geht. Durch einen Abgleich mit anderen Datenbanken könnte man aus Zeitpunkt und Aufenthaltsort in einem Mobilfunkdatensatz auf einzelne Personen zurückschließen, sagt Blondel. Die Informatiker Arvind Narayanan und Vitaly Shmatikov haben einen Algorithmus entwickelt, mit dem sie bekannte Nutzer des Mikroblogging-Dienstes Twitter auch aus einer anonymisierten Analyse von Twitter-Nachrichten identifizieren können, wenn sie Daten aus dem Fotodienst Flickr hinzunehmen. Zwar beträgt die Fehlerrate noch 12 Prozent, aber die beiden Forscher warnen davor, die Möglichkeiten einer »De-Anonymisierung« zu unterschätzen.

Verknüpfungen von Datensätzen und Identität sind oft rechtswidrig, ja gar kriminell. Doch gibt es im Datenschutzrecht genug Grauzonen, die von den neuen Profiliern in der Wirtschaft kreativ genutzt werden – nach dem Motto: Was nicht explizit verboten ist, ist erlaubt. Für die vernetzte Gesellschaft müsste dieser Grundsatz dringender denn je umgedreht werden. Carola Elbrecht vom vzbv formuliert es so: »Nichts darf geschehen, ohne dass der Verbraucher eingewilligt hat und Bescheid weiß.« —

Ja, ich teste DIE ZEIT 3 Wochen gratis!
 Schicke nSia mir bitte DIE ZEIT von der nächstreichbaren Ausgabe an gratis für 3 Wochen zur Probe. Wenn mir DIE ZEIT gefällt, brauche ich nichts weiter zu tun. Ich erhalte sie dann 52x im Jahr für zeit. nur €3,40 pro Ausgabe (inkl. Versandkosten) statt €3,80 im Einzelkauf und spare über 10%. Der Versand des Geschenkes erfolgt nach der 1. Zahlung. Sollte ich mich gegen das Abonnement entscheiden, kündige ich spätestens nach Erhalt des 2. Exemplars. Eine formlose Mitteilung an den Leser-Service genügt. Pro Be nur im Inland gültig. Auslandspost auf Anfrage.
 Mein Wunschgesche ist: (bitte nur ein Kreuz machen)
 Bergmann popcube: Weiß Dunkelbraun

Name, Vorname _____
 Straße/ Nr. _____
 PLZ/Wohnort _____
 Telefon _____
 E-Mail _____

Ich bin Student und spare nach dem Test sogar 42% (zeit. nur €2,20 pro Ausgabe). Mein gültige Immatrikulationsbescheinigung liegt bei. Zusätzlich erhalte ich als Student 6x pro Jahr ZEIT CAMPUS.
 Wenn ich DIE ZEIT weiterlese, zahle ich:
 bequem per Bankinzug und erhalte 2 weitere Ausgabe kostenlos

Geldinstitut _____
 Kontonummer _____ Bankleitzahl _____
 per Rechnung
 Ja, ich möchte von Ihnen weitere Vorteile profitieren. Ich bin daher interessiert, dass mich DIE ZEIT per Post, Telefon oder E-Mail über interessante Medien-Angebote und kostenlose Veranstaltungen informiert.

Datum _____ Unterschrift _____

DIE ZEIT, Leser-Service, 20080 Hamburg
 ☎ 0180 / 52 52 908* ☎ 0180 / 52 52 909*
 🌐 www.zeit.de/abo 📧 abo@zeit.de

731844 N3/731845 Stud. N3
 731846 N5/731847 Stud. N5

Testen Sie DIE ZEIT 3x gratis!

DIE ZEIT
 WER DENKT FÜR WISSEN?
 WER DENKT FÜR WISSEN?

DIE ZEIT ist die Wochenzeitung für Politik, Wirtschaft, Wissenschaft und Kultur. ZEIT-Leser schätzen ihre Kompetenz und Meinungsvielfalt.

Geschenk zur Wahl!

Bergmann popcube
 Retro-Radio mit Echtholzgehäuse, Aluminiumfront, beleuchtetem Display, Weckfunktion und Temperaturanzeige. Kompatibel mit iPod und anderen MP3-Playern. In Braun und Weiß erhältlich. Maße: ca. 15x15x12 cm. Lieferung ohne iPod.

Genießen Sie DIE ZEIT



Sprachen lernen? Betrachten Sie es als ein Kinderspiel.

Erinnern Sie sich daran, wie Sie als Kind Ihre Muttersprache erlernt haben. Die Welt war Ihr Klassenzimmer, aber es gab keine Schulstunden. Sie haben auf eine spielerische Weise, aktiv am Lernprozess teilgenommen. Es war ein Kinderspiel.

Das ist das Geheimnis von Rosetta Stone. Wir fördern Ihre natürliche Fähigkeit, eine Sprache zu erlernen. Unsere Dynamic Immersion™ Methode hilft Ihnen von Anfang an in der neuen Sprache zu denken, nämlich ganz ohne Übersetzungen und lästiges Auswendiglernen von Vokabeln. Sie haben Spaß und finden es leicht Ihre Sprachlernziele zu verwirklichen.

In 31 Sprachen erhältlich

6 MONATE GELD-ZURÜCK GARANTIE

10% Rabatt + Gratis Lieferung
 Geben Sie 'wissen08' beim Bestellvorgang an

Informieren Sie sich jetzt
0800 200 11 882
 RosettaStone.de/wissen08

RosettaStone

* 0180-Ziffern sind Gebührenfrei. In der Regel sind 0180-Ziffern nur von Mobiltelefonen aus erreichbar. Die Gebühren für 0180-Ziffern sind abhängig von Ihrem Mobilfunktarif. Die Gebühren für 0180-Ziffern sind in der Regel höher als für gewöhnliche Rufnummern. Die Gebühren für 0180-Ziffern sind in der Regel höher als für gewöhnliche Rufnummern. Die Gebühren für 0180-Ziffern sind in der Regel höher als für gewöhnliche Rufnummern.

Dossier

Thema

Wenn den Staat die Sammelwut packt

So hatte sich Dorothee Wolter den Beginn ihres Urlaubs nicht vorgestellt: Als sie im Hafen von Piräus das Fährticket kaufen wollte, fehlte das Portemonnaie in der Handtasche. Im Gedränge eines Athener Busses hatten offenbar ein paar Diebe zugegriffen. »Personalausweis, Führerschein, Fahrzeugschein, Kreditkarte – alles weg«, sagt Wolter. Zwar wurde es doch noch eine sonnige Zeit in der Ägäis, aber der Ärger folgte zu Hause in Hamburg: Um einen neuen Führerschein zu bekommen, verlangte das zuständige Amt nicht nur Meldebescheinigung und Personalausweis, sondern auch einen Nachweis der Behörde, die den Führerschein zuerst ausgestellt hatte – vor vielen Jahren im fernen Westfalen. »Der musste erst zugefaxt werden«, wundert sich Wolter.

Im Zeitalter der totalen Vernetzung, könnte man meinen, sollte das einfacher gehen: Warum können die verschiedenen Ämter nicht in einem großen Datensatz, der über eine Nummer eindeutig mit einem Bürger verknüpft ist, überprüfen, welche Dokumente ihm in der Vergangenheit ausgestellt wurden – schnell und unbürokratisch?

Einen solchen Datensatz gibt es in der Bundesrepublik aus guten Gründen nicht. Um einem Überwachungsstaat vorzubeugen, sind die Datenbestände von Behörden, Polizei und Nachrichtendiensten getrennt. Und bereits 1969 entschied das Bundesverfassungsgericht, dass ein Personenkennzeichen gegen die Menschenwürde verstoße, weil es »den Menschen zum bloßen Objekt im Staat« mache.

Die Entwicklung der vergangenen Jahre zeigt: Das sehen nicht alle so. »Es gibt eine Tendenz, dass staatliche Behörden mehr Daten teilen als früher«, sagt der Bundesbeauftragte für Datenschutz und Informationssicherheit, Peter Schaar. Vor allem die Sicherheitsbehörden drängen, flankiert von besorgten Politikern, darauf, im Namen der Terrorismusbekämpfung ihre Datenbestände miteinander zu vernetzen.

Eine erste Brandmauer fiel am 1. Dezember 2006, als der Bundestag die Einführung der sogenannten Antiterror-Datei beschloss. Auf die können sowohl Polizei als auch Nachrichtendienste zugreifen – eine

direkte Verbindung zwischen den Sicherheitsapparaten, die man nach den Erfahrungen des »Dritten Reichs« bewusst gekappt hatte. Umfasste sie beim Start am 30. März 2007 rund 13 000 Personen, waren drei Jahre später schon 18 875 potenziell Verdächtige registriert. Ob auch Einträge wieder gelöscht werden und wie oft die angeschlossenen Behörden bislang darauf zugegriffen haben, verrät das BKA nicht.

Andere Datenbanken haben einen noch beeindruckenderen Umfang erreicht: An die 800 000 DNA-Analysen, mehr als zwei Millionen Fingerabdrücke und »erkennungsdienstliche« Daten von knapp sechs Millionen Menschen hat die deutsche Polizei gespeichert. Auch auf EU-Ebene wachsen die Datenberge von Europol, dem Visa-Informationssystem, der Fingerabdrucksammlung Eurodac und dem Schengener Informationssystem an. Solche Sammlungen sind nicht nur wegen ihres Ausmaßes problematisch. Durch den Zugriff der Geheimdienste aufgrund der Antiterror-Gesetze könnten sie zu Profilen verknüpft werden, die unbescholtene Bürger zu potenziell Verdächtigen machen. So wird die Unschuldsvermutung, ein Grundprinzip des Strafrechts, untergraben.

Behörden träumen vom digitalen Bürger und spannen zunehmend die Wirtschaft ein, für sie Daten zu sammeln. Jüngstes Beispiel ist der elektronische Entgeltnachweis, abgekürzt Elena. Seit Januar dieses Jahres sind sämtliche Arbeitgeber verpflichtet, für jeden Angestellten einmal im Monat einen Datensatz an die Zentrale Speicherstelle (ZSS) in Würzburg zu schicken. Dort werden sie verschlüsselt und »pseudonymisiert«, also getrennt vom Namen des Arbeitnehmers, abgelegt.

Die Idee dahinter klingt praktisch: Wer seinen Job verliert, muss beim Arbeitsamt keine Papierbelege mehr vorlegen. Er schaltet stattdessen mit einer Signaturkarte, die seine Identität elektronisch verbürgt, seinen Elena-Datensatz zur Bearbeitung frei. So kann dann der Sachbearbeiter alle Informationen über den letzten Job bei der ZSS abrufen und berechnen, wie viel Sozialleistung dem Betroffenen zusteht.

Der Haken: Die rund 280 möglichen Datenfelder enthalten neben Angaben zur Person und zum Einkommen auch brisante Informationen zu Kündigungsumständen, Krankheitszeiten und Abmahnungen. Diese Daten würden auch heute schon – nur auf dem Papierweg – übermittelt, um Sozialleistungen bewilligen zu können, heißt es aus dem Bundeswirtschaftsministerium. Doch was als Bürokratieabbau daherkommt, führt praktisch zu Dossiers über Arbeitnehmer, die lückenlos deren Jobbiografie über Jahre hinweg dokumentieren, eine Art soziale Vorratsdatenspeicherung. »Es haben sich viele Arbeitgeber bei uns gemeldet, die Elena als Vertrauensbruch empfinden«, berichtet Rena Tangens vom Verein Foebud. Die Bielefelder Organisation für digitale Bürgerrechte hatte im April eine Verfassungsklage gegen das Elena-

Behörden haben begonnen, viele Daten wie mit dem Staubsauger zu sammeln. Was machbar ist, wird gemacht.

ERSTE HILFE

So schützen Sie Ihre Privatsphäre im Internet

Online-Werbung
Sperrten Sie in den Browser-Einstellungen unter »Sicherheit«, »Datenschutz« oder »Privatsphäre« das Setzen von Cookies – wenigstens die von Drittanbietern (sprich: Werbenetzwerken).

Soziale Netzwerke
• einfacher Schutz: Machen Sie sich die Mühe und gehen Sie die Datenschutz-Einstellungen genau durch. In vielen Netzwerken sind manche Informationen anfangs automatisch öffentlich, sodass Sie aktiv sperren müssen, was privat bleiben soll.
• mittlerer Schutz: Melden Sie sich unter einem Pseudonym an, sperren Sie Daten-

freigaben, und veröffentlichen Sie keine Bilder von sich. Mit geschickten Analysen können Sie aber auch dann noch enttarnt werden.
• starker Schutz: Verzichten Sie auf soziale Netzwerke – auch wenn Ihnen dadurch etwas entgeht.

Internet-Surfen
Um sich möglichst unerkannt durch das Netz zu bewegen, rufen Sie Webseiten mit Anonymisierungswerkzeugen auf: zum Beispiel mit TOR, ursprünglich von der Electronic Frontier Foundation entwickelt (www.torproject.org), oder mit JonDonym, das aus dem Projekt »Java Anon Proxy

JAP« der Technischen Universität Dresden hervorgegangen ist (www.jondos.de).

Google
Wenn Sie vermeiden möchten, dass Google Ihre Suchabfragen für seine Werbekunden auswertet, deaktivieren Sie den Mechanismus auf www.google.com/ads/preferences. Oder verwenden Sie eine andere Suchmaschine.

Rabatt- und Bonusprogramme
Verzichten Sie etwa auf die Payback-Karte und die DeutschlandCard (als Verbundsystem verschiedener

Firmen) ebenso wie auf Kundenkarten einzelner Unternehmen. Im Tausch für Bonuspunkte können die Unternehmen sonst ihr Konsumverhalten auswerten.

Adresshandel
Nach dem Bundesdatenschutzgesetz sind alle Unternehmen verpflichtet, Ihnen mitzuteilen, welche Daten sie über Sie gespeichert haben. Auf dem Portal des Verbraucherzentrale Bundesverbands zu »Verbraucherrechten in der digitalen Welt« – www.surfer-haben-rechte.de – finden Sie unter »Checklisten und Materialien« Musterbriefe, mit denen Sie Auskunft über

die eigenen Daten verlangen, deren gewerbliche Nutzung untersagen sowie eine Löschung der Daten veranlassen können.

Sicherheitsbehörden
Mit dem »Auskunfts-generator« auf der Seite <http://datenschmutz.de/moin/AuskunftErsuchen> können Sie Briefe an Polizeibehörden verfassen, in denen Sie gemäß Paragraf 19, Absatz 1 des Bundesdatenschutzgesetzes erfragen können, welche Daten dort über Sie gespeichert sind. Die Polizeibehörden verlangen allerdings in ihrer ersten Antwort eine glaubwürdige Kopie des Personalausweises.

Verfahren organisiert, die etwa 21 000 Bundesbürger unterzeichnet haben. Tatsächlich will das Wirtschaftsministerium Elena nun erst einmal aussetzen – aber nicht aus Datenschutzgründen, sondern wegen der ausufernden Kosten.

Es ist nicht ausgeschlossen, dass die Gerichte noch eingreifen. Foebud hatte mit einer Klage schon einmal Erfolg: Gemeinsam mit anderen Bürgerrechtsorganisationen hatte der Verein eine Sammelklage gegen die Vorratsdatenspeicherung in der Telekommunikation auf den Weg gebracht. Der Staat hatte Internetanbieter und Telefongesellschaften dazu verpflichtet, vom 1. Januar 2008 an sämtliche Verbindungsdaten von Telefongesprächen, Kurzmitteilungen und Internetnutzungen für sechs Monate zu speichern. Vor vier Monaten kippte das Bundesverfassungsgericht das Gesetz. Die Daten von Millionen ohne Anlass zu speichern führe dazu, »ein diffus bedrohliches Gefühl des Beobachtetseins hervorzurufen, das eine unbefangene Wahrnehmung der Grundrechte in vielen Bereichen beeinträchtigen kann«, befanden die Richter.

Der Staat verhält sich in diesen Fällen nicht anders als viele Internetnutzer, die auf ihren Festplatten immer mehr Musik, Videos und andere Dokumente aufhäufen. Hauptsache, man hat sie erst einmal. Bei den Behörden sei der Trend erkennbar, möglichst viele Daten »wie mit einem Staubsauger« zu sammeln, wenn das technisch machbar sei, sagt Peter Schaar.

Durch die Hintertür wird nun auch noch ein Personenkennzeichen eingeführt. Seit dem 1. Juli 2007 haben alle Menschen, die in Deutschland leben, eine

Steueridentifikationsnummer. Neugeborene bekommen sie mit der Geburt zugeteilt. Verwenden dürfen sie nicht nur Finanzämter, auch im Elena-Verfahren wird sie übermittelt. Das Problem: Die Steuer-ID gilt lebenslanglich und kann nicht gewechselt werden. »Überall in der digitalen Welt, wo wir Identifikationsnummern haben, muss es möglich sein, sie zu ändern«, sagt Marit Hansen vom Unabhängigen Landeszentrum für Datenschutz in Schleswig-Holstein, allein schon, um im Falle eines sogenannten Identitätsdiebstahls wieder Sicherheit zu bekommen. Wird die Steuer-ID erst einmal mit weiteren Daten verknüpft, könnte sie dazu führen, dass eindeutig identifizierbare digitale Lebensläufe von uns allen entstehen.

In Italien muss man die Steuer-ID bereits angeben, wenn man seine Stromrechnung bezahlen will. Dass es so schlecht um den Datenschutz in Deutschland noch nicht bestellt ist, liegt nicht an der Weitsicht der Politik. Vielmehr hat das Bundesverfassungsgericht Angriffe auf die informationelle Selbstbestimmung bislang immer abgewehrt. »Wir können uns aber nicht auf Dauer nur darauf verlassen«, warnt Rena Tangens. »Denn im Grunde geht es um viel mehr: Wie machen wir die Grundrechte im digitalen Zeitalter wirklich sicher?« Eine schlüssige Antwort steht noch aus. Datenschützer und Bürgerrechtler sind sich aber darin einig, dass wir ein neues, striktes Datenschutzgesetz brauchen. Es müsste nicht nur sämtliche Datensammelereien für den Bürger einsehbar machen, sondern auch jegliche Form von Datenbevorratung verbieten, solange kein konkreter Verdacht vorliegt. —

BUCHTIPPS

Ilija Trojanow, Juli Zeh:
»Angriff auf die Freiheit. Sicherheitswahn, Überwachungsstaat und der Abbau bürgerlicher Rechte« *Hanser; 170 Seiten, 14,90 Euro*

Matthias Becker:
»Datenschatten. Auf dem Weg in die Überwachungsgesellschaft« *Heise; 192 Seiten, 16,90 Euro*