Die Privatsphäre und das Netz

avenir spezial

2 _ Editorial
3 _ Inhaltsübersicht
4 _ Gläserne Gesellschaft
6 _ Neugierige Apps
7 _ Informationsblase
8 _ Datenschutzrecht
10 _ Transparenter Bürger
12 _ Transparenter Staat
13 _ Netzarchitektur
14 _ Lehren der Geschichte
16 _ Big Data – eine Begriffsklärung
17 _ Perspektiven der Assekuranz
18 _ Personalisierte Medizin
19 _ Werbewirtschaft
20 _ Intelligente Stromzähler
22 _ Bezahlsysteme
23 _ Daten- statt Bankgeheimnis
24 _ Anonymität dank Quantenphysik
26 _ Verschlüsselung
27 _ Datenschutz beim Wandern
28 _ Cloud versus Server
30 _ Ein gutes Passwort
31 _ Elternpflichten
32 _ Tipps für Hackingopfer
34 _ Datenkontrolle
36 _ Publikationen

Das Datenmeer

Posterbeilage

avenir suisse

Februar 2015

Gerhard Schwarz
Direktor Avenir Suisse

Als ich als Jugendlicher, etwa Mitte der 1960er Jahre, George Orwells «1984» las, erschien mir das Werk als furchterregende Utopie. Der grosse Lauschangriff, den wir in den letzten Jahren erlebt haben, macht die Beschreibungen Orwells zu harmlosen Geschichtchen. Die Realität hat den Visionär längst eingeholt. Aber ebenso erschreckend wie das selbstverständliche Eindringen des Staates – und von Unternehmen – in die Privatsphäre der Individuen ist der Verlust der Wertschätzung der Privatheit und damit vielleicht sogar der Scham. Es gibt unglaublich viele Menschen, die ohne Hemmungen ihr Privatleben im öffentlichen Raum ausbreiten, sich kaum für die Gefährdung ihrer Privatsphäre durch die vielen neuen technischen Möglichkeiten interessieren und sich nicht daran stören, dass sie fast permanent überwacht werden (können). Das ist in doppelter Hinsicht bedenklich. Zum einen ist die Privatheit für sich allein ein hoher menschlicher Wert. Ihr Schutz, das «Recht, in Ruhe gelassen zu werden», wie es 1890 in den USA der oberste Richter Louis Brandeis postulierte, zählt zu den modernsten grundrechtlichen Errungenschaften. Zum anderen, und das ist wohl noch wichtiger, ist die Privatheit der Sauerstoff der Freiheit. Der gläserne Mensch ist ganz grundsätzlich Gift für die freie Gesellschaft, ganz gleich, ob diese Transparenz staatlich erzwungen, von Privaten raffiniert «erschlichen» oder von den Individuen naiv und freiwillig bereitgestellt wird. Es ist die vor fremden Einblicken und Einflüssen geschützte Privatsphäre, die die Autonomie und Individualität jeder Person und somit die selbstbestimmte bürgerliche Gesellschaft erst ermöglicht.

Es läge natürlich auch an der Politik, die Privatsphäre zu schützen, ja zu hegen und zu pflegen. Zu oft tut sie das Gegenteil. Aber es liegt – gerade in einem liberalen Verständnis – auch in der Verantwortung jedes und jeder Einzelnen, achtsam zu sein gegenüber den Gefährdungen der Privatheit, die Privatsphäre der anderen zu respektieren sowie für sich selbst eine klare Grenze zu ziehen zwischen privat und öffentlich und sorgfältig umzugehen mit dem kostbaren Gut der geschützten eigenen Privatsphäre. Das gilt auch, oder sogar erst recht, für den digitalen Raum.

Über Privatsphäre, Datenschutz und das Netz

Welche Bedeutung haben Datenschutz und Datensicherheit in unserem Alltag? Was können wir von Edward Snowden lernen? Die Beiträge in diesem «avenir spezial» beantworten zentrale Fragen zu unserem Leben mit dem Internet.

01_ Gesellschaft
Wie gläsern wollen wir sein? Seite 04

02_ WhatsApp & Co.
Warum verwanzen wir uns freiwillig? Seite 06

03_ Medien
Leben wir in einer Informationsblase? Seite 07

04_ EDÖB
Wen beschützt das Datenschutzrecht? Seite 08

05_ Transparenter Bürger
Müssen wir die Daten vor dem Steueramt schützen? Seite 10

06_ Transparenter Staat
Was ist das Öffentlichkeitsprinzip? Seite 12

07_ Geopolitik
Was bedeutet die Netzarchitektur für den Datenschutz? Seite 13

08_ Lehren der Geschichte
Können wir von den Zünften lernen? Seite 14

09_ Datenflut
Was ist eigentlich Big Data? Seite 16

10_ Assekuranz
Günstigere Lebensversicherungen dank Big Data? Seite 17

11_ Personalisierte Medizin
Gehört meine DNA mir? Seite 18

12_ Werbewirtschaft
Was schenken wir täglich Google? Seite 19

13_ Smart Metering
Was verrät der Stromzähler über mich? Seite 20

14_ Bezahlsysteme
Wie sicher ist E-Banking? Seite 22

15_ Chancen
Statt des Bankgeheimnisses das Datengeheimnis? Seite 23

16_ Quantenphysik
Gibt es noch Anonymität? Seite 24

17_ Verschlüsselung
Was muss man über Datenübermittlung wissen? Seite 26

18_ Netzabdeckung
Auf welchem Berggipfel ist noch Ruh? Seite 27

19_ Cloud versus Server
Wo soll ich meine Daten speichern? Seite 28

20_ Passwörter
Wie merke ich mir ein gutes Passwort? Seite 30

21_ Elternpflichten
Wie geht Kindererziehung 2.0? Seite 31

22_ Erste Hilfe
Ich wurde gehackt! Was jetzt? Seite 32

23_ Datenkontrolle
Haben Sie heute schon ein Gesetz gebrochen? Seite 34

Wie gläsern wollen wir sein?

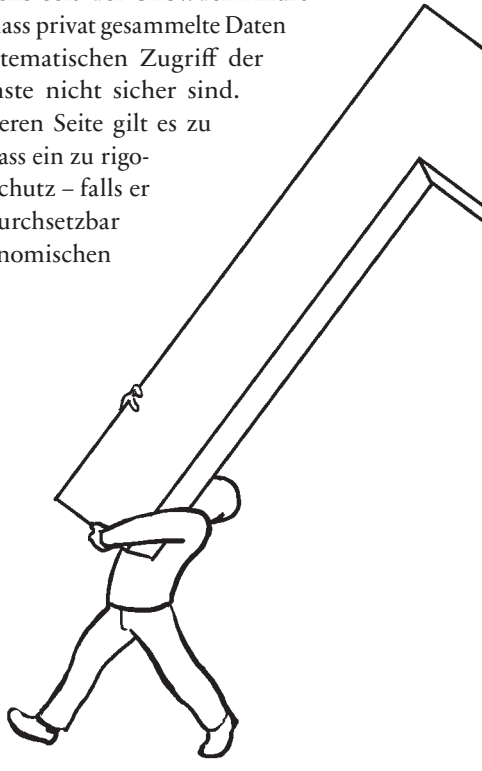
Überwiegen die Chancen von «Big Data» die Bedenken vor dem Verlust der Privatsphäre, ja sogar vor dem Extremszenario vom gläsernen Menschen? Diese drängende Frage kümmert die grosse Mehrheit bisher kaum. Das irritiert.

Patrik Schellenbauer

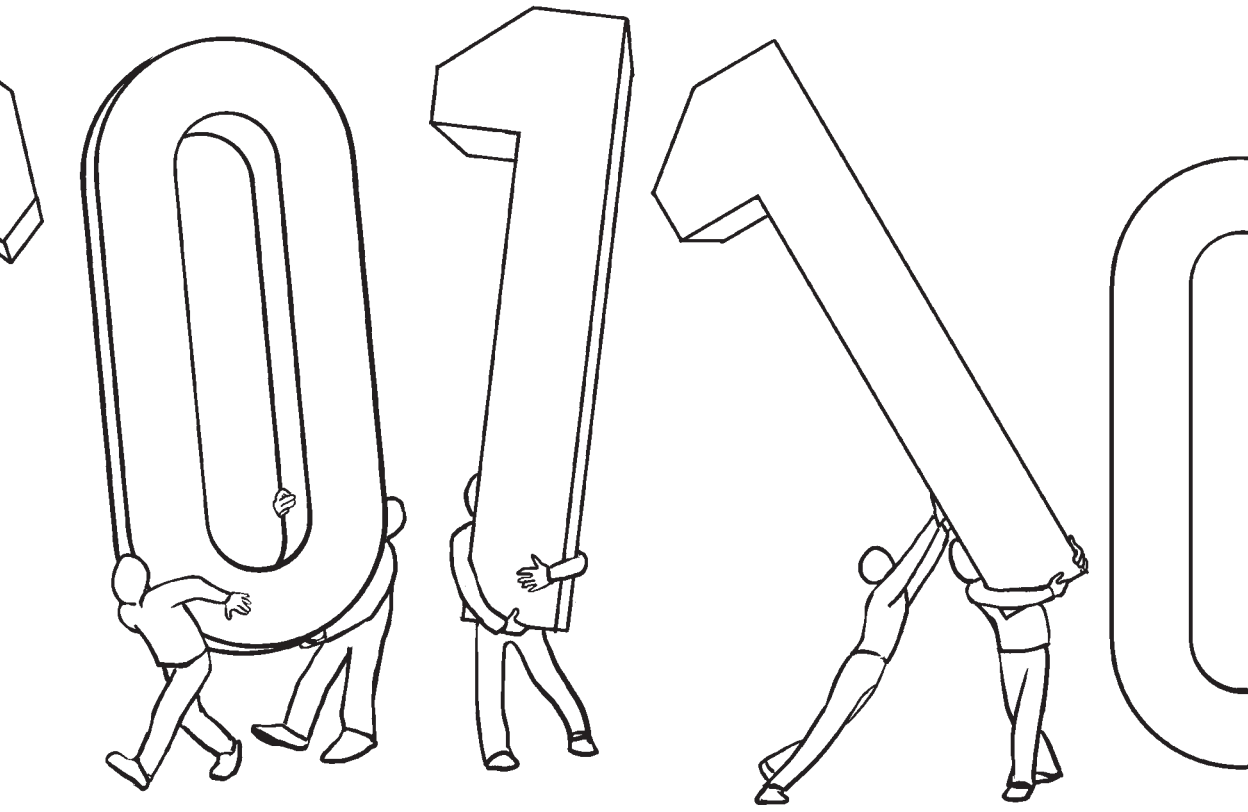
Sollen wir uns vor «Big Data» fürchten oder uns als Optimisten auf ressourcenschonende Produktion und ein besseres Leben freuen? Überwiegt die Dividende der digitalen Revolution die Bedenken vor dem Verlust der Privatsphäre oder – im Extremszenario – vor dem gläsernen Menschen wie in Orwells Schreckensvision «1984»? In dieser Frage zeichnet sich eine mögliche Lösung nicht einmal schemenhaft am Horizont ab. Sehen wir es zuerst positiv. Die automatische Analyse unserer Daten eröffnet unzählige neue Möglichkeiten, von Buchtipps bis zu massgeschneiderten Finanzprodukten. Smart Metering, die vernetzte Echtzeitmessung des Stromverbrauchs in den Haushalten, könnte schon heute Nachfragespitzen brechen und nötige Kraftwerkskapazitäten reduzieren. Beim Mobility Pricing ermöglicht ein Tarifsystem mit zeitnaher Nachfragemessung eine gleichmässigere Auslastung von Schiene und Bahn. Eine datengestützte Weiterentwicklung der Medizin verspricht personalisierte Medikamente mit weniger Nebenwirkungen oder den massgeschneiderten 3D-Druck von Gelenken oder gar Organen. Schon steht das Internet der Dinge vor der Tür, etwa der intelligente Kühlschrank, der automatisch Vorräte nachbestellt. Nicht wenige Ökonomen halten diese vierte industrielle Revolution für den einzigen Wachstumstreiber der nächsten 25 Jahre. Doch diese Segnungen brauchen eines: Daten über uns, unser Verhalten und unsere Vorlieben, laufend und in sehr grosser Zahl. Und Daten werden produziert, mit jedem Mausklick, mit jedem Tippen auf den Touch Screen des Smartphones, mit jedem Wechsel der Funkantenne im mobilen Netz, mit jedem Kauf per Kreditkarte, mit jedem Statement in sozialen Netzwerken. Wirken allein schon die gespeicherten Datenberge unheimlich, übersteigen die Möglichkeiten geschickter Verknüpfung und Auswertung unser Vorstellungsvermögen.

Die Schweiz braucht eine breite öffentliche Debatte über Daten, deren Eigentum und Schutz, vor allem aber über die Privatsphäre und persönliche Freiheit.

Können wir darauf vertrauen, dass der Staat unsere Privatsphäre schützt und Missbräuche verhindert? Dies scheint allzu naiv, wenn man bedenkt, dass die Bürokratie selber zu den Produzenten und Nutzern unserer Daten gehört – auch wenn Big Data noch kaum Einzug gehalten hat. Spätestens seit der Snowden-Affäre wissen wir, dass privat gesammelte Daten vor dem systematischen Zugriff der Geheimdienste nicht sicher sind. Auf der anderen Seite gilt es zu bedenken, dass ein zu rigoroser Datenschutz – falls er überhaupt durchsetzbar ist – die ökonomischen



Vorteile von Big Data zunichte machen könnte. Dieses drängende Thema kümmert die grosse Mehrheit bis heute kaum. Das irritiert, wenn man an den Aufschrei denkt, den die Fichenaffaire vor gut 20 Jahren auslöste. Der damalige Schuldige war aber greifbar: übereifrige und kaum kontrollierte Staatsschutzbeamte, die im Vergleich zu heute mit Steinzeitmethoden arbeiteten. Gegen welchen Gegner müsste sich ein Protest heute richten? Big Data hat Züge eines unheimlichen Leviathans, der nicht national und nicht staatlich fassbar ist, sondern irgendwo und überall im globalen Datenmeer schwimmt. Oft wird vermutet, die Privatsphäre sei den Menschen nicht mehr wichtig. Viel wahrscheinlicher scheint, dass wir das Problem verdrängen, weil wir nicht wissen, wie damit umzugehen wäre. Symptomatisch dafür ist das geringe Medienecho, das die laufende Revision des Büpf, des «Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs», ausgelöst hat. Was soll und kann der einzelne tun? Ein wichtiges Stichwort ist «digitale Mündigkeit». Zuerst sollten wir uns über mögliche Folgen des eigenen Tuns im digitalen Raum klar werden. Die nötige Bewusstseinsbildung reicht dabei weit über das Internet hinaus. Lohnt es sich z. B. wirklich, dem Grossverteiler per Kundenkarte für ein paar Rabattprozente sein ganzes Konsumverhalten zu offenbaren? Freilich reicht dies nicht, um das Grunddilemma zu lösen. Über kurz oder lang braucht die ganze Gesellschaft eine breite öffentliche Debatte über den Umgang mit unseren Daten und über die sinnvollen Grenzen, die wir dem Staat und den Unternehmen in diesem Zusammenhang setzen wollen.



Warum verwanzen wir uns freiwillig?

Die grosse Masse der Smartphone-Besitzer verwanzt sich freiwillig und akzeptiert, dass ihre privatesten Informationen auf beliebigen Servern gespeichert und weiterverarbeitet werden – aus Bequemlichkeit, oder weil uns Privatsphäre nichts mehr bedeutet?

Verena Parzer Epp

Haben Sie das Vertrauen in Ihren Ehepartner verloren und möchten wissen, wo er sich den lieben langen Tag aufhält? Möchten Sie mithören, wie der Lehrer mit Ihrem Kind in der Schule redet? Oder den SMS-Verkehr Ihres Chefs lesen? Privatdetektiv kann heute jeder spielen. Und dabei zu Ergebnissen kommen, von denen die Stasi dereinst geträumt hätte. Man muss dafür nur zwei relativ niedrige Hürden überwinden. Erstens, den Download einer Spy-Software aus dem Internet. Zweitens, ein paar Minuten Zugriff auf das Smartphone des «Ziels». Dass bei Bundesratssitzungen schon seit Jahren ein Handy-Verbot gilt, hat seinen guten Grund. Smartphones können nämlich selbst dann noch manipuliert werden, wenn sie ausgeschaltet sind.

Dass bei Bundesratssitzungen schon seit Jahren ein Handy-Verbot gilt, hat seinen guten Grund. Smartphones können nämlich selbst dann noch manipuliert werden, wenn sie ausgeschaltet sind.

Die meisten Menschen haben – wahrscheinlich zu Recht – wenig Angst vor Abhöraktionen aus ihrem näheren Umfeld. Aber es ist zu bezweifeln, dass zum Beispiel das beliebte «Whatsapp» 600 Millionen User auf der Welt hätte, wenn diese die Nutzungsbedingungen vor der Installation genau studiert hätten. Whatsapp lässt sich unter anderem folgende Handlungen auf dem Smartphone bewilligen: Bilder und Videos mit der Kamera aufnehmen, Informationen zu anderen Apps abrufen, Kontakte lesen und Kontakte ändern, Audio-Aufnahmen mit dem Mikrofon, Konten auf dem Gerät verwenden, hinzufügen oder entfernen. Vor diesem Hintergrund ist es nicht mehr erstaunlich, dass Facebook sich kürzlich diesen Neuzugang in seinem Firmenportfolio 19 Mrd. $ kosten liess.

Die grosse Masse der Smartphone-Besitzer verwanzt sich also freiwillig und akzeptiert explizit, dass ihre privatesten Informationen auf beliebigen Servern gespeichert und weiterverarbeitet werden. Für dieses Verhalten gibt es wohl nur die Erklärung, dass wir alle unglaublich bequem geworden sind und aufgehört haben, unsere Privatsphäre als etwas Besonderes zu schätzen.

Für alle, die jetzt trotzdem die Sicherheit im Umgang mit ihrem geliebten Gerät erhöhen wollen, gibt es hier noch ein paar Tipps:

01_ Vergeben Sie eine PIN für die SIM-Karte.
02_ Achten Sie darauf, welche Apps sie installieren, und bevorzugen sie solche mit verschlüsselter Datenübertragung.
03_ Das Smartphone nicht immer am Körper tragen – und es aus dem Schlafzimmer verbannen.
04_ Abhörsichere Handytaschen («Off-Pockets») verwenden oder bei sehr wichtigen geschäftlichen Verhandlungen die Batterie aus dem Gerät herausnehmen.

Leben wir in einer Informationsblase?

Verengt das Internet unseren Horizont, statt ihn zu erweitern, weil wir zunehmend nur personalisierte Inhalte lesen? Der beste Schutz gegen die Informationsblase ist der aufgeklärte Mediennutzer – online wie offline.

Michael Mandl

Print-Medien haben eines gemeinsam. Sie publizieren jeweils eine Zeitungsausgabe für alle Leser. Nicht so Online-Medien. Sie können aufgrund neuer technischer Möglichkeiten ihren Lesern personalisierte News zusammenstellen. In seinem Buch «The Filter Bubble: What the Internet Is Hiding From You» hat Eli Pariser im Jahr 2011 erneut das erschreckende Bild einer Welt gezeichnet, in der die Medienkonsumenten in ihren eigenen Informationsblasen leben und ihr Horizont durch den Medienkonsum laufend enger statt weiter wird. Werden z.B. die Inhalte einer Online-Zeitung aufgrund von Datenprofilen ausgeliefert, finden kontroverse, neue Informationen viel seltener oder nie den Weg zum User. Dies ist besonders aus demokratietheoretischer Sicht problematisch, weil die User sich dessen oftmals nicht bewusst sind. Kritisch zu bewerten ist auch die mangelnde Transparenz der algorithmischen Gatekeeper im Unterschied zu klassischen Zeitungsredaktoren, bei denen zumindest aufgrund der Positionierung des Mediums Rückschlüsse auf die Werthaltung möglich sind.

Mit dem steigenden Online-Konsum von News ist eine kontroverse Diskussion über eine neue, kritische Dimension der Meinungsbildung entstanden – die algorithmengesteuerte Informationsblase.

Die wohl bekanntesten Produzenten gefilterter Online-Inhalte sind die alteingesessenen Suchmaschinen-Anbieter Google oder Yahoo. Aber auch praktisch alle sozialen Medien nutzen die immensen Datenspeicher, um die Interessen ihrer Kunden bis ins kleinste Detail zu analysieren und personalisierte Werbung oder Inhalte anzubieten.

Noch werden in der Schweiz kaum individualisierte Online-News ausgeliefert – abgesehen von Google-News. Die lokalen Verlage sind aber bereits in der Experimentierphase. Stark personifiziert ist bereits die Online-Werbung, wo die Banner oftmals über komplexe Ausschreibungen in Echtzeit verkauft werden.

Die zuweilen ziemlich pessimistische Sicht, dass die Online-Mediennutzer zunehmend in ihren selbst gefilterten Informationsblasen leben, muss aus diversen Gründen jedoch relativiert werden.

- Erstens gibt es auch in den Offline-Medien seit jeher Gatekeeper, die Informationen filtern. Das Ideal eines vollkommen ausgewogen informierten Bürgers ist online wie offline utopisch.
- Zweitens hören Menschen generell lieber Gleichgesinnten zu. Von sich aus tendieren viele Medienkonsumenten zu den Inhalten, die ihnen am meisten entsprechen – egal ob online oder offline.
- Drittens gibt es durchaus Möglichkeiten, sich dieser Informationsblase zu entziehen: Der Online-Nutzer kann beispielsweise Add-ons bzw. Apps wie Ghostery oder Blur installieren, die das automatische Tracking seiner Online-Handlungen verhindern. Noch viel einfacher: Nicht immer nur googlen. Eine alternative Suchmaschine aus der Schweiz ist Swisscows, die gänzlich auf die Speicherung von IP-Adressen oder persönliche Angaben verzichtet. Und der Informationsfilter kann auch bei Facebook und Google ausgeschaltet werden.

Schliesslich ist die beste Waffe gegen die Informationsblase der aufgeklärte Mediennutzer selber, der sich über die Folgen seiner Handlungen im Internet bewusst ist und seine Informationen deshalb gezielt aus unterschiedlichen Quellen bezieht.

Wen beschützt das Datenschutzrecht?

Wofür ist das Datenschutzrecht eigentlich zuständig, und wofür nicht? Ein Interview mit Hanspeter Thür, dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB).

Hanspeter Thür im Interview mit Verena Parzer Epp

Herr Thür, wie beeinflusst der EDÖB den Alltag eines durchschnittlichen Schweizer Bürgers?

Ein wichtiger Aspekt unserer Arbeit ist die Beratung von Privatpersonen und Firmen, die Auskunft im Bereich Datenschutz wünschen. Es sind dies zum einen Bürgerinnen und Bürger, die von einer Datenbearbeitung betroffen sind und sich nach ihren Rechten erkundigen. Zum anderen beraten wir Firmen, die im Zusammenhang mit einem neuen Projekt wissen wollen, was sie im Umgang mit den anfallenden Personendaten beachten müssen. Ein wichtiges Instrument hierfür sind die Erläuterungen auf unserer Website. Einen indirekten Einfluss übt der EDÖB im Bereich der Gesetzgebung aus, wo er bei Konsultationen darauf achtet, dass der Datenschutz ausreichend berücksichtigt wird.

«Das Datenschutzgesetz (DSG) wurde zu einer Zeit verabschiedet, als das Internet gerade in seinen Anfängen war.»

Stichwort Unternehmen: Wie stellt der EDÖB sicher, dass Firmen das Datenschutzgesetz einhalten? Und was geschieht bei Verstössen?

Personendaten fallen in zahllosen Bereichen an, etwa beim Einkauf mit Kundenkarten, durch Videoüberwachung, beim Surfen im Internet oder wenn wir den Arzt aufsuchen. Eine flächendeckende Beaufsichtigung der Datenbearbeitungen ist nicht realistisch; dazu fehlen uns schlicht die Mittel. Auch würde dies nicht dem Willen des Gesetzgebers entsprechen. Kontrollen führen wir dann durch, wenn eine grössere Anzahl Personen in ihrer Persönlichkeit verletzt sein könnte (Beispiele sind die neuen Dienstleistungen der Postfinance und die Kundenkarten von Migros & Coop). Bestätigt sich der Datenschutz-Verstoss, erlassen wir Empfehlungen an die Adresse der Beaufsichtigten.

Bekanntlich sammelt auch der Staat eifrig Daten seiner Bürger, etwa im Bereich der Überwachung des Fernmeldeverkehrs oder durch den Nachrichtendienst. Welche Aufgabe hat der EDÖB hier inne?

Datenbearbeitungen von Bundesbehörden und bundesnaher Betriebe unterliegen in der Regel der Aufsicht des EDÖB. Beispiele für unsere Tätigkeit in diesem Gebiet sind die Kontrolle der Schwarzfahrerdatenbank der SBB, die Überprüfung der Vergabeverfahren für Schengen-Visa und die Kontrollen von Krankenversicherern (die im obligatorischen Bereich als Bundesbehörden gelten) und deren Datenannahmestellen. Zudem prüfen wir Gesetzesvorhaben der Behörden auf ihre Datenschutzkonformität.

«Eine vom Bundesamt für Justiz eingesetzte Arbeitsgruppe, der auch der EDÖB angehört, prüft zurzeit wie man das DSG an die neuen Gegebenheiten anpassen könnte.»

Wofür ist der EDÖB nicht zuständig?

Nicht in die Zuständigkeit des EDÖB fallen die Datenbearbeitungen der kantonalen Behörden. Auch bei Unternehmen, die ihren Sitz ausschliesslich im Ausland haben, sind wir grundsätzlich nicht zuständig.

Ist das Schweizer Datenschutzgesetz den aktuellen Herausforderungen gewachsen?

Das Datenschutzgesetz (DSG) wurde zu einer Zeit verabschiedet, als das Internet gerade in seinen Anfängen war. Seither hat die Zahl der Datenbearbeitungen um ein Vielfaches zugenommen. Die ständig wachsenden Datenberge und der technologische Fortschritt haben dazu geführt, dass es gerade für Unternehmen immer einfacher geworden ist, Daten zu sammeln, miteinander zu verknüpfen und auszuwerten, z. B. zu Marketing- und Werbezwecken. Dadurch hat sich auch das Risiko von Datenschutzverletzungen stark erhöht. Für die Bürgerinnen und Bürger ist es angesichts dieser Entwicklung schwierig, die Kontrolle über ihre Daten zu behalten. Eine vom Bundesamt für Justiz eingesetzte Arbeitsgruppe, der auch der EDÖB angehört, prüft zurzeit, wie man das DSG an die neuen Gegebenheiten anpassen könnte.

Wie liessen sich die Datenschutzrechte der Betroffenen denn stärken?

Häufig genannte Ansätze sind Privacy by Design, wonach bei neuen Technologien und (Online-) Diensten der Datenschutz von vornherein in die Gesamtkonzeption einzubeziehen ist, und Privacy by Default, bei dem Anbieter verpflichtet werden, Geräte und Dienstleistungen mit möglichst datenschutzfreundlichen Einstellungen auf den Markt zu bringen. Auch ein Ausbau der Informationspflicht bei der Bearbeitung von Daten und eine Ausweitung der Sanktionsmöglichkeiten bei Verstössen stehen im Raum. Es bedarf internationaler Anstrengungen, um den Datenschutz im Internet-Zeitalter gewährleisten zu können.

Müssen wir die Daten vor dem Steueramt schützen?

Der nahezu gläserne Steuerzahler ist eine notwendige Bedingung für die rekordhohe Steuerquote der nordischen Länder. Anreize für eine hohe Erwerbsquote sorgen dafür, dass das nordische Steuersystem auch ergiebig bleibt.

Marco Salvi

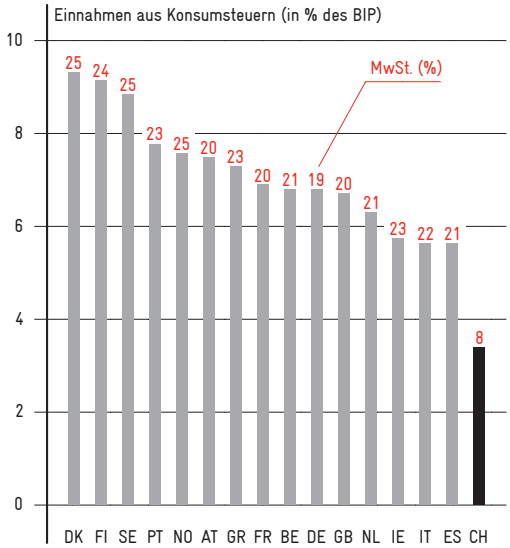
Der Weihnachtsmann kommt bekanntlich aus dem hohen Norden, sein Geschäftsmodell ist für skandinavische Verhältnisse aber eher untypisch: Das Steuerdomizil konnte noch niemand genau festlegen, die Verkaufszahlen bleiben geheim, die Lieferungen erfolgen unter dem Schutz der Dunkelheit und es werden selten Rechnungen gestellt. Dass ein derart intransparentes Familienunternehmen von den lappländischen Steuerbehörden geduldet wird, erstaunt, denn sonst herrscht in Skandinavien der Grundsatz der vollkommenen Offenlegung. Wie kaum woanders haben die Steuerbehörden einen ungehinderten Zugang zu Kreditkartentransaktionen, Bankkonten und Lohnabrechnungen. Fast nichts bleibt ihnen verborgen. In Dänemark lassen sich über 95 % der versteuerten Einkommen mit Angaben einer unabhängigen Drittpartei, wie der Bank oder des Arbeitgebers exakt überprüfen. Die Steuererklärung flattert bereits ausgefüllt in den Briefkasten. Fehlt nur die Unterschrift des Steuerzahlers. Einzig die Selbständigkeit bietet noch ein wenig «Spielraum» bei der Bestimmung des Einkommens. Wegen der flächendeckenden Verbreitung des bargeldlosen Zahlungsverkehrs wird jedoch auch dieser Spielraum bald verschwinden.

Stellt der gläserne Steuerzahler den Grund für die rekordhohe Steuerquote der nordischen Länder dar? Müssen sich die Vertreter eines schlanken und minimalen Staates vor «zu viel» Transparenz gegenüber dem Steueramt fürchten? Nicht nur davor, glaubt man dem dänischen Ökonomen Henrik Kleven von der London School of Economics. Laut Kleven bildet Transparenz eine notwendige, jedoch keine hinreichende Bedingung für die Ausweitung des staatlichen Einflussbereichs. Es reicht also nicht, dass die Steuerhinterziehung eingedämmt wird; der Staat muss auch die Steuervermeidung in engen Grenzen halten. Mit anderen Worten muss er dafür sorgen, dass das Steuersystem ergiebig bleibt. Auch darin sind die Nordländer Spitze.

So greifen sie mehr als andere zu Abgaben mit einer breiten Bemessungsgrundlage, allen voran der Mehrwertsteuer. Diese macht mittlerweile

Das Unternehmen des Weihnachtsmanns ist reichlich undurchsichtig. Dass Lapplands Steueramt dies duldet, erstaunt sehr. Denn Skandinavien ist das Reich vollkommener Transparenz – zum Leid seiner Steuerzahler.

Konsumsteuern: im Norden ergiebig



Quelle: OECD

um die 30 % aller Steuereinnahmen der nordischen Länder aus. Einer umfassenden Konsumsteuer wie der Mehrwertsteuer kann man auch nicht mit einer vorübergehenden Konsumenthaltung ausweichen: früher oder später werden sämtliche Einkommen konsumiert. Abgesehen vom Nicht-Konsum bietet nur der Einkaufstourismus eine gewisse legale Umgehungsmöglichkeit, wenn auch eine umständliche. Angesichts von Mehrwertsteuersätzen um die 25 % (auf alkoholische Getränke deutlich mehr), wundert es kaum, dass die skandinavischen Konsumenten davon regen Gebrauch machen.

Doch das ist nicht genug. Will der Staat die Zitrone vollkommen auspressen, muss er laut Kleven auch dafür sorgen, dass die Produktion am helllichten Tag stattfindet. Dabei geht es nicht so sehr um die Bekämpfung von illegalen Schwarzmärkten, sondern vielmehr um die Einschränkung einer völlig legalen Aktivität – der Hausarbeit. Im Gegensatz zur Erwerbsarbeit lässt sich nämlich die Hausarbeit kaum besteuern. Aus Sicht des Steueramtes ist somit eine hohe Erwerbsquote besonders wünschenswert, und auch diesbezüglich sind die nordischen Länder führend. Dank massiver Subventionierung von Kinderbetreuung, Alterspflege, Mobilität und Ausbildung – alles Dienstleistungen, die in einer komplementären Beziehung zur Erwerbsarbeit stehen –, haben sie die nötigen Anreize dazu geschaffen. So sehr, dass einmal im Jahr sogar ein älterer, weissbärtiger Mann, der in anderen Ländern längst seine Rente geniessen würde, seine bequeme Holzhütte verlässt und in der Polarnacht die Rentiere spannt.

Im Gegensatz zur Erwerbsarbeit lässt sich die Hausarbeit kaum besteuern. Aus Sicht des Steueramtes ist somit eine hohe Erwerbsquote besonders wünschenswert. Auch diesbezüglich sind die nordischen Länder führend.

Was ist das Öffentlichkeitsprinzip?

Heutzutage sind grundsätzlich alle Verwaltungsdaten öffentlich – ausser, sie werden gesetzlich geschützt. Ein Interview mit Bruno Baeriswyl, Zürichs oberstem Datenschützer, über das juristische Gegenstück zum Datenschutz.

Bruno Baeriswyl im Interview mit Verena Parzer Epp

Herr Baeriswyl, können Sie das Öffentlichkeitsprinzip in wenigen Worten erklären?

Das Öffentlichkeitsprinzip besagt, dass Bürger grundsätzlich über die Aktivitäten der Verwaltung informiert werden und Zugang zu Dokumenten haben, um so ihre demokratischen Rechte besser wahrnehmen und auch die Verwaltung kontrollieren zu können. Auf Bundesebene wurde das Öffentlichkeitsprinzip im Jahr 2004, im Kanton Zürich im Jahr 2007 eingeführt.

Warum beschäftigen Sie sich als Datenschutzbeaufragter des Kantons auch mit dem Öffentlichkeitsprinzip?

Weil es sich bei Datenschutz und Öffentlichkeitsprinzip um zwei Seiten derselben Medaille handelt. Ich nenne Ihnen ein paar Beispiele: Adressen und Autonummern sind im Kanton Zürich öffentliche Informationen. Grundsätzlich hat aber jeder das Recht, diese schützen zu lassen. Es gibt eine Reihe von öffentlich zugänglichen Informationen, die aus datenschutzrechtlicher Sicht unproblematisch sind, Schülerzahlen oder Verkehrsströme etwa. «Open Government» bringt aber auch knifflige Fragen mit sich. Welchen gesellschaftlichen Mehrwert etwa hätte ein elektronisches Grundbuch? Welche Informationen dürfen die Sozialämter preisgeben, ohne dabei Persönlichkeitsrechte zu verletzen? Welchen Umgang müssen die Spitäler mit ihren Daten pflegen? Bei allen diesen Fragestellungen geht es immer darum, eine möglichst klare Grenze zwischen der Öffentlichkeit und der Privatsphäre der Menschen zu ziehen.

«Ich bin mir ziemlich sicher, dass irgendwann eine breite öffentliche Diskussion über die Privatsphäre kommen wird.»

Ist das Leben für die Bürger durch das Öffentlichkeitsprinzip besser geworden?

Grundsätzlich ja, denn ihre Rechte wurden gestärkt. Heute hat jeder ohne Angabe von Gründen Anspruch auf alle Informationen, die sich bei öffentlichen Organen befinden. Einschränkungen bestehen nur bei überwiegenden öffentlichen Interessen oder Informationen, die die Privatsphäre von Drittpersonen betreffen. Einigen Handlungsbedarf sehe ich aber noch bei der Umsetzung. Die Einführung des Öffentlichkeitsprinzips war ein Paradigmenwechsel, dessen Auswirkungen sich viele Menschen – und viele Verwaltungsangestellte – noch nicht genug bewusst sind. Auch in der politischen Debatte, wenn neue Gesetze ausgehandelt werden, fehlt zu oft die Dimension der Privatsphäre.

Glauben Sie, wenn Sie an die globalen Entwicklungen denken, dass Sie als lokaler Zürcher Advokat der Privatsphäre überhaupt noch etwas ausrichten können?

Das hoffe ich doch! Ich kann zumindest versuchen, diese wichtigen Fragen in die Diskussion einzubringen. Natürlich steht auf einem anderen Blatt, wie die Gesellschaft sie aufnimmt. Ich bin mir aber ziemlich sicher, dass irgendwann eine breite öffentliche Diskussion über die Privatsphäre kommen wird. Und je früher diese stattfindet, desto eher können wir den Umgang mit unseren Daten proaktiv gestalten statt aus der Defensive zu reagieren.

Was bedeutet die Netzarchitektur für den Datenschutz?

Datenschutz hat auch eine geopolitische Komponente. Vor allem geht es dabei um die Frage: Wer kontrolliert das Kabel? Ein Interview mit Jovan Kurbalija, dem Geschäftsführer der auf Internet-Governance-Fragen spezialisierten «Diplofoundation».

Jovan Kurbalija im Interview mit Verena Parzer Epp

Herr Kurbalija, können Sie den Aufbau des Internets in einfachen Worten erklären?
Grundsätzlich ist das Internet ein grosses, dezentral organisiertes Netz. Das hat vor allem mit seiner Geschichte zu tun: Der Vorläufer des Internets, Arpanet, wurde ab den 1970er Jahren entwickelt als ein internationales Rechnernetzwerk, das sogar einen nuklearen Angriff überstehen würde. Im Vordergrund stand lange Zeit nur die Verbindung der Computer untereinander. Die Kommunikation zwischen den Menschen ergab sich quasi als «Nebenprodukt».

Wie ist die Kommunikation im Internet organisiert?
Ähnlich wie im Strassennetz. Es gibt Autobahnen mit schnellerem Verkehr und Landstrassen. Um von A nach B zu kommen kann ein Auto, also ein Datenpaket, eine beliebige Route wählen. Die Lenker der Autos sind jeweils eindeutig gekennzeichnet – also einer IP-Adresse zugeordnet. Dieses «Telefonbuch» des Internets wird durch die in den USA domizilierte Icann koordiniert.

Könnte man sagen, dass die Amerikaner letztlich kontrollieren, wer sich im Netz tummeln darf?
Nein. Oder zumindest haben sie das bisher nicht gemacht, sondern sich vielmehr als vernünftige Verwalter bewiesen. Icann erfüllt quasi die Funktion eines Buchhalters und konzentriert sich vor allem auf die Top-Level-Domains, also z.B.«.ch» oder «.org». In den Ländern selbst werden die IP-Adressen und Domainnamen durch Unterorganisationen vergeben. Ausserdem hat das US-Handelsministerium angekündigt, die Aufsicht über Icann per September 2015 abzugeben. Es ist richtig, dass die USA lange nicht bereit waren, auf diese Kontrollmöglichkeit zu verzichten. Aber in Zukunft wird Icann unter internationaler Aufsicht stehen. Ohnehin ist die Icann-Story ein Nebenschauplatz.

Warum?
Der wahre Verteilkampf dreht sich um die Daten, nicht um das Telefonbuch. Heute reden alle von der «Cloud». Allzu leicht geht dabei vergessen, dass es sich immer noch um Daten handelt, die gespeichert und transportiert werden müssen. Auch wenn es scheint, dass sich das Internet rapid rund um den Globus ausgebreitet hat – in technischer Hinsicht hat es sich eher zentralisiert.

Könnten Sie das näher erklären?
Heute läuft der gesamte globale Datenverkehr über einige wenige Glasfaserkabel. Die international wichtigen Netzschnittstellen lassen sich an zehn Fingern abzählen. Besonders offensichtlich ist die geografische Konzentration bei den Unterwasser-Glasfaserkabeln. Der Datenverkehr wird immer voluminöser. Damit einzelne Länder nicht von der Kommunikation abgeschnitten und die digitalen Informationen sicher transportiert werden können, brauchen sie Anbindungen an verschiedene Glasfaserkabel. Macht hat im Netz, wer über Zugang zu den «Autobahnen» verfügt. Hinzu kommt, dass – auch als Folge der Snowden-Enthüllungen – die Bemühungen um Datensouveränität zugenommen haben. Dass China die Grenzen seines Internets streng kontrolliert, ist hinlänglich bekannt. Dass nun aber auch die EU über Grenzkontrollen nachdenkt, ist neu. Wenn wir verhindern wollen, dass sich die Staaten aus Angst voreinander immer mehr abschotten, braucht es einen globalen Deal, der den Zugriff auf die Datenleitungen klar regelt.

Können wir von den Zünften lernen?

Die Geschichte der Zünfte zeigt: Die berechtigte Sorge um allfällige Wirtschaftsspionage im digitalen Zeitalter darf nicht zur Abkapselung führen. Sonst verpassen wir am Ende den Fortschritt.

Alois Bischofberger

Der Schutz vor der Weitergabe politisch relevanter Informationen treibt die Machthaber seit Jahrtausenden um. Verschlüsselungen, Geheimschriften und Geheimcodes dienten dem Informationsschutz und bieten Romanautoren und Filmemachern bis heute reichlich Stoff. An Einfallsreichtum mangelte es nicht. Der antike griechische Autor Herodot etwa berichtet, dass der Herrscher von Milet seinem Schwiegersohn eine geheime Nachricht übermittelte, indem er sie auf den rasierten Kopf eines Sklaven tätowierte. Als dessen Haare nachgewachsen waren, wurde er zum Empfänger der Botschaft durchgelassen. Eine Kopfrasur genügte, um die Nachricht zu offenbaren.

Im Wirtschaftsleben wurden Informationsschutz und Geheimhaltung schon in vorindustrieller Zeit grossgeschrieben.

Im Wirtschaftsleben wurden Informationsschutz und Geheimhaltung schon in vorindustrieller Zeit grossgeschrieben. Das lässt sich am Beispiel des Zunftwesens zeigen.

In wirtschaftlicher Hinsicht waren die Zünfte Interessenvertreter gegenüber den Behörden, Ausbildungsstätten für den beruflichen Nachwuchs, Instanzen für die Sicherung der Produktqualität und nicht zuletzt Organisationen zum Schutz vor fremder Konkurrenz. Rechte und Pflichten der Zunftgenossen waren in äusserst detaillierten Zunftordnungen festgeschrieben, Zuwiderhandlungen wurden als Verstösse gegen Ehre und Solidarität mit Geldbussen und im Wiederholungsfall mit dem Ausschluss aus der Zunft, einem faktischen Berufsverbot, bestraft. Die Anreize für Regeltreue waren also gross. Dem Schutz vor der Weitergabe des Wissens dienten auch Wanderverbote.

Wanderverbote waren im Zunftwesen aber ungleich verteilt: In gewissen Berufen, etwa bei den Bürstenbindern, bestand für die Gesellen sogar eine Pflicht zur mehrjährigen Wanderung. Üblich waren Wanderungen auch bei Schneidern, Schustern, Kürschnern und Müllern. Das gemeinsame Merkmal dieser Handwerke war ihre geringe Know-how-Intensität. Es bestand also keine Gefahr, dass geschäftsrelevante Produktionsgeheimnisse über wandernde Gesellen der Konkurrenz zugespielt werden konnten.

Ganz anders waren die Vorschriften in technisch fortgeschrittenen, hoch spezialisierten Handwerken, die Erfindungen kommerziell nutzten. Die Gesellen durften dort gar nicht wandern, und selbst die Meister nicht auswandern. Ausserdem war der Verkauf von Werkzeugen über den Einzugsbereich der Zunft hinaus verboten. Mit diesen Massnahmen verschafften sich die Zünfte ein regionales Monopol. Der Austausch von Wissen liess sich aber trotzdem nicht völlig unterbinden. Das Wissen bahnte sich so oder so seinen Weg aus den Stadtmauern hinaus.

Gravierend und voraussehbar waren die Folgen der Monopolsituation: Der fehlende Wettbewerb schwächte die Innovationskraft, die Handwerke fielen hinter die Konkurrenz zurück.

Mit einem Wanderverbot belegte Handwerke wurden «gesperrte Handwerke» genannt. Dazu zählten in heutigen Ohren fremdartig tönende Berufe wie Beckenschlager, Goldspinner, Heftleinmacher, Kompassmacher, Messingbrenner, Schellenmacher, Trompetenmacher, Brillenmacher oder Drahtzieher. Ihnen gemeinsam waren höhere

Anforderungen an das Wissen und die Fertigkeiten der Belegschaft – und eine höhere Preissetzungsmacht. In Nürnberg, einem Wirtschaftszentrum des damaligen Europa, waren in der ersten Hälfte des 17. Jahrhunderts 21 der aufgelisteten 117 Handwerke gesperrt. Gravierend und voraussehbar waren die Folgen der Monopolsituation: Der fehlende Wettbewerb schwächte die Innovationskraft, die Handwerke fielen hinter die Konkurrenz zurück, und der Wirtschaftsstandort wurde zweitklassig. Nicht zuletzt die Einsicht in solche Mechanismen veranlasste Adam Smith 1776 zu seiner fundamentalen Kritik an den wettbewerbsverhindernden Monopolen und Kartellen. In der Folge setzte sich die Handels- und Gewerbefreiheit als Prinzip durch; die auf ständischen Privilegien fussenden Zunftordnungen hatten ausgespielt.

Von der Geschichte der Zünfte können wir vielleicht dieses lernen: Die berechtigte Sorge um allfällige Wirtschaftsspionage im digitalen Zeitalter darf nicht zur Abkapselung führen. Sonst verpassen wir am Ende den Fortschritt.

Was ist eigentlich Big Data?

Grob versteht man unter Big Data automatisch erfasste und ausgewertete Daten. Während Unternehmen Milliarden investieren, überwiegen bei Privaten und Datenschützern Vorbehalte und Skepsis.

Jörg Naumann

Big Data zählt wie Cloud Computing oder Social Business zu den Schlagworten aus dem IT-Umfeld. Doch was genau ist darunter zu verstehen? 2011 definierte die Consultingfirma Gartner den Begriff als eine Datenmenge, die «zu gross ist, um mit konventionellen Software-Tools empfangen, gespeichert, gemanagt oder analysiert zu werden». Wieviele Daten heute in aller Welt herumschwirren, weiss niemand genau. Laut Schätzungen werden täglich 2,5 Quintillionen (eine Zahl mit 30 Nullen) Bytes produziert – und selbst diese Grösse soll sich alle zwei Jahre verdoppeln. Klassische relationale Datenbanksysteme oder Statistikprogramme sind nicht in der Lage, derartige Datenmengen zu verarbeiten, weshalb für Big Data eine neue Art von Software zum Einsatz kommt, die parallel oft auf Hunderten Prozessoren bzw. Servern arbeitet.

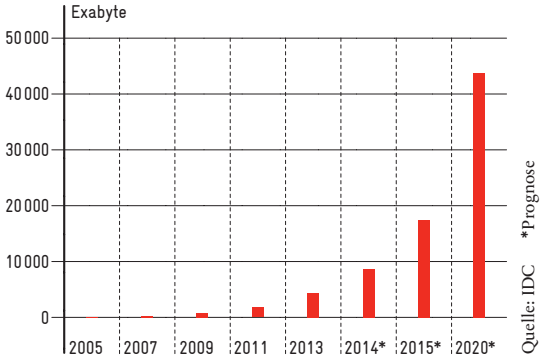
Neben den Datenschutzproblemen gibt es noch einen weiteren Kritikpunkt an Big Data: Können Maschinen aus dem unstrukturierten Datensalat wirklich herausfiltern, was relevant ist?

Das Neue an Big Data ist die Vielzahl der Quellen, aus der heute Daten fliessen, und die potenziellen Verknüpfungen, die sich daraus ergeben. Gesammelt werden neben maschinell erzeugten Meta-Daten (z.B.: Kommunikationsprotokolle über Telekom-Verbindungen, Web-Zugriffe, Sensoren) ja auch Daten aus der Finanzindustrie, aus dem Verkehrs- und dem Energiesektor, dem Gesundheitswesen und der Wissenschaft. Eine Unzahl von Daten wird mehr oder weniger heimlich auf privaten Computern von Apps erzeugt und an ihre Auftraggeber übermittelt. Nicht zu vergessen natürlich die Privatpersonen, die mit dem Einsatz ihrer Kredit- und EC-Karten und Handys selbst viel zum Wachstum der weltweiten Datenmengen beitragen.

Unternehmen sehen in der automatisierten Echtzeit-Analyse eine Chance zur Erlangung von Wettbewerbsvorteilen. Je schneller sie herausfinden können, welches Produkt oder welche Dienstleistung für einen Kunden gerade wichtig ist, desto eher können sie ein passendes Angebot machen. Wissenschafter oder Verwaltungen erhoffen sich aus der Analyse der Datenflut Erkenntnisse über wichtige Entwicklungen wie Epidemien, Verkehrsflüsse, etc. Bei Privatpersonen wächst nicht zu Unrecht die Sorge, dass ihre Persönlichkeitsrechte zunehmend degradiert werden.

Neben den offensichtlichen Datenschutzproblemen gibt es noch einen weiteren Kritikpunkt an Big Data: Können Maschinen aus dem unstrukturierten Datensalat wirklich herausfiltern, was relevant ist? Wie glaubhaft sind die Ergebnisse, sodass die Menschen ihre Entscheidungen darauf gründen? Noch befindet sich die Entwicklung von Software für die Verarbeitung von Big Data in einer relativ frühen Phase. Und entgegen anders lautenden Versprechungen konnte auch Google bisher Grippe-Epidemien nicht klar vorhersagen.

Weltweit generiertes Datenvolumen



Günstigere Lebensversicherungen dank Big Data?

Statistische Modelle und systematische Datenanalyse gehören seit jeher zum Geschäftsmodell von Versicherungen. Die Folgen von Big Data für die Branche sind trotzdem noch unklar.

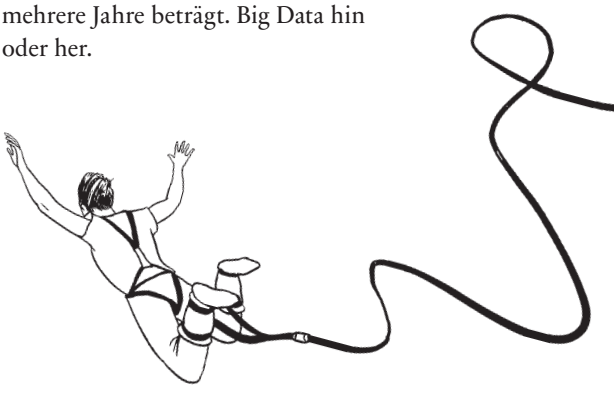
Jérôme Cosandey

Beim Abschluss einer Lebensversicherung profitiert der Kunde von einem gewichtigen Vorteil: Er kann seinen Gesundheitszustand oft besser als der Versicherer beurteilen. Ist der Kunde überdurchschnittlich fit, wird er eher eine Leibrente kaufen, fühlt er sich krank, sich eher gegen Todesfall versichern. Versicherer versuchen auf unterschiedliche Arten, dieser Informationsasymmetrie zu begegnen. Sie können Abklärungen, z. B. ärztliche Gutachten, verlangen. Diese sind oft zeitaufwendig und kostenintensiv, und können für den Kunden wie für den Kundenberater abschreckend wirken. Sie können Risikozuschläge für alle Kunden verrechnen, was jedoch den Risikoschutz «guter» Kunden unnötig verteuert. Oder sie können schlicht auf den Abschluss des Vertrags verzichten und einzelne Kunden ablehnen. Der Einbezug von Informationen, die die Kunden dem Versicherer freiwillig zu Verfügung stellen, oder von Big Data kann diese Asymmetrie-Probleme entschärfen.

Den technischen Möglichkeiten von Big Data, also einer sehr individualisierten Risikoeinschätzung und Prämienberechnung, stehen gegensätzliche legale Entwicklungen gegenüber.

Erstens kann Big Data helfen, eine gezieltere Prüfung des Gesundheitszustandes beim Kunden vorzunehmen. Dank modellbasierten Algorithmen kann neu in manchen Fällen auf den aufwendigen Arztbesuch verzichtet werden. Das spart nicht nur Kosten, sondern auch Zeit. Der Entscheid des Versicherers kann innert Stunden statt Wochen gefällt werden. Zweitens werden dank tieferen Prozesskosten neue Zielgruppen und Märkte attraktiv, die bisher für Versicherer unrentabel waren – zum Beispiel Kunden aus der unteren Mittelschicht. Drittens kann Big Data für gezielte Marketingaktivitäten eingesetzt werden. Kunden profitieren von einem besseren Beratungserlebnis, weil sie auf Produkte angesprochen werden, die eher ihren Bedürfnissen entsprechen. Und die Kundenberater werden effizienter und können ihre Abschlussquote verbessern.

Wird also Big Data eine neue Ära der Versicherungsbranche einläuten? Bedingt. Versicherung ist ein Vertrauensgeschäft. Versicherer werden sehr vorsichtig Drittdaten von ihren Kunden einsetzen, auch wenn diese öffentlich zugänglich sind. Sie werden eher auf Daten zurückgreifen, die ihnen Kunden freiwillig und bewusst vermitteln. Dieser freiwillige Austausch setzt das Vertrauen voraus, dass der Versicherer sorgfältig mit den Daten umgeht, und er bedingt einen unmittelbaren Nutzen für den Kunden. Und den technischen Möglichkeiten von Big Data, also einer sehr individualisierten Risikoeinschätzung und Prämienberechnung, stehen gegensätzliche legale Entwicklungen gegenüber. In der Europäischen Union ist es zum Beispiel seit Dezember 2012 aufgrund eines Entscheids des Europäischen Gerichtshofs nicht mehr möglich, die Tarife von Lebenspolicen für Frauen und Männer zu differenzieren, obwohl der Lebenserwartungsunterschied zwischen beiden Geschlechtern mehrere Jahre beträgt. Big Data hin oder her.



Gehört meine DNA mir?

Mit der Entschlüsselung des menschlichen Genoms liegt das Leben eines Menschen vor uns wie ein offenes Buch. Leider kann es auch schnell zum Besitz Dritter werden.

Claudia Wirz

Seit 1485 ist er tot und begraben. Gefallen in der Schlacht. Und weil bekanntlich die Sieger die Geschichte schreiben, galt er jahrhundertelang als ebenso skrupellos wie entstellt. Die Rede ist vom buckeligen Richard III., dem letzten englischen Herrscher aus dem Hause Plantagenet, zur Strecke gebracht von Heinrich Tudor und für die Nachwelt geprägt von William Shakespeare während der Herrschaft von Heinrichs Enkelin Elisabeth I. Als lahmender, ekliger Bösewicht ging Richard in die Geschichte ein.

Bis 2012. Dann kam die Wende. Dafür brauchte es einen archäologischen Skelettfund, die Möglichkeit der DNA-Analyse und das Glück, lebende verwandte Vergleichspersonen finden zu können. Das Bild über Richard hat sich seither gewandelt. Einen Buckel hatte er wohl nicht, aber eine Skoliose (Fehlstellung der Wirbelsäule). Er war wohl eher blond als wie bis anhin geglaubt dunkelhaarig. Und er war wohl kaum verbrecherischer als andere Machtmenschen seiner Zeit.

Selbst nach Hunderten von Jahren kann die DNA-Analyse private Einsichten eröffnen, Geschichte umdeuten und höchstpersönliche Geheimnisse lüften.

Aber die Analyse des Skeletts förderte auch Erkenntnisse zutage, die kaum ohne Rechtsfolgen veröffentlicht werden könnten, würde es sich um einen lebenden Monarchen handeln: In der königlichen Familie gab es in der mütterlichen Linie nachweislich eheliche Untreue und eine Reihe von Kuckuckskindern. Das heisst: Man darf damit rechnen, dass mindestens ein englischer König – wenn nicht mehrere – unberechtigterweise auf dem Thron sassen.

Der Fall Richard zeigt: Mit der Entschlüsselung des menschlichen Genoms liegt das Leben eines Menschen vor uns wie ein offenes Buch. Selbst nach Hunderten von Jahren kann die DNA-Analyse private Einsichten eröffnen, Geschichte umdeuten und höchstpersönliche Geheimnisse lüften. Und dabei steht diese Technologie erst am Anfang.

Richard mag das egal sein. Ein Mensch von heute aber sollte sich gut überlegen, wie freizügig er mit dem genetischen Buch seines Lebens umgeht. Seit das menschliche Genom 2001 erstmals vollständig entschlüsselt wurde, entstehen überall immense Datenbanken für genetische Informationen. Dass solche Profile – auch wenn sie anonymisiert sind – mit ein bisschen Geschick leicht zu knacken sind und personalisiert werden können, bewies kürzlich der Computerspezialist Yaniv Erlich.

An DNA-Profilen haben viele Akteure Interesse: Ahnenforscher, Lebens- und Krankenversicherer, Arbeitgeber, die Forensik, die Terrorabwehr, die Forschung. Insbesondere die Krebsforschung setzt auf die personalisierte Medizin, die den Patienten Hoffnung bringt. Aber das Sammeln und Speichern genetischer Daten hat seinen Preis. Das persönliche Genom kann zum Besitz Dritter werden. Das mussten die Nachkommen von Henrietta Lacks, einer 1951 an Krebs verstorbenen Afroamerikanerin, am eigenen Leib erfahren. Ein Assistenzarzt entnahm Lacks ohne ihr Wissen und ohne Benachrichtigung der Familie Zellen. Seither sind die sogenannten HeLa-Zellen um das Hundertfache der Körpermasse von Henrietta Lacks vermehrt worden und werden weltweit für die Forschung gebraucht, vermarktet und gehandelt. Zehntausende von wissenschaftlichen Publikationen basieren auf HeLa-Zellen. Nur: Die Familie der unfreiwilligen Spenderin hatte nichts davon.

Was schenken wir täglich Google?

Bei allen Gratisangeboten im Netz ist der Kunde die eigentliche Ware. Aber wieviel ist diese Ware wert? Zum Beispiel für Google? Eine grobe Schätzung für den Schweizer Markt.

Verena Parzer Epp

«Wir wissen, wo du bist. Wir wissen, wo du warst. Wir wissen mehr oder weniger, worüber du nachdenkst.» Im Jahr 2010 erregte Eric Schmidt, der damalige CEO von Google, mit diesem Ausspruch einiges Aufsehen. Dass dieser gar nicht so weit weg von der Realität war, lässt sich durchaus in der Umsatz- und Gewinnentwicklung des Internetgiganten ablesen. Googles Umsatz wuchs in den letzten zehn Jahren von 3,2 Mrd. $ (2004) auf knapp 60 Mrd. $ (2013), sein Gewinn von 400 Mio. $ (2004) auf 12,0 Mrd. $ (2013).

18 Rappen pro Tag. Das ist der Preis, den die Werbewirtschaft für unsere Daten zu zahlen bereit ist.

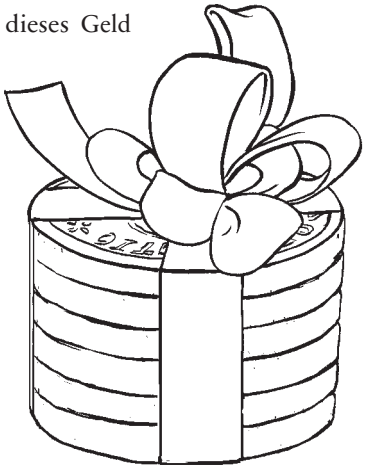
Google erntet nun die Früchte seiner jahrzehntelangen Datensammlerei, wobei das zentrale Stichwort für alle seine Produkte «Relevanz» lautet. Je beliebter die Google-Angebote bei den Kunden sind, desto mehr Daten können für die Erstellung der Kundenprofile ausgewertet werden, und desto attraktiver wird Google als Werbeplattform.

Laut Schätzungen landete weltweit jeder dritte Dollar, der 2013 für Onlinewerbung ausgegeben wurde, bei Google. Bei Werbung auf mobilen Geräten war es sogar jeder zweite Dollar.

Die aktuellen Zahlen für den Schweizer Online-Werbemarkt zeigen einmal mehr nach oben: Im ersten Halbjahr 2014 wurden in der Schweiz 145 Mio. Fr. für Suchmaschinenwerbung ausgegeben. Da hierzulande 95 von 100 Usern Google als Suchmaschine verwenden, gingen geschätzte 137 Mio. Fr. dieses Kuchens auf sein Konto. Unter Berücksichtigung des stetigen Wachstums und auf das ganze Jahr extrapoliert ergibt das für 2014 ca. 300 Mio. Fr.

Hinzuzurechnen wären noch die Einnahmen aus der «Displaywerbung», die z.B. über Banneranzeigen oder Werbevideos auf diversen Webangeboten und Medienportalen aufgeschaltet wird. Laut eigenen Angaben generiert Google 23,9 % des weltweiten Anzeigenumsatzes über derartige Drittwebseiten aus seinem Werbenetzwerk. Vom gesamten Schweizer Markt für sogenannte Display Ads in der Höhe von 91 Mio. Fr. (1. HJ. 2014) schreibt Raphael Bienz, Geschäftsführer von Blueglass Interactive, wiederum ca. 30 % Google zu. Hinzu kommen Werbeumsätze von weiteren Google-eigenen Plattformen wie YouTube, Gmail oder Google Maps. Hochgerechnet auf das ganze Jahr ergäbe das einen geschätzten Gesamtumsatz von ca. 75 Mio. Fr. – und in beiden Geschäftsbereichen zusammengenommen mindestens 375 Mio. Fr.

Teilt man diese Summe auf die (laut BFS) 5,8 Millionen aktiven Schweizer Internetnutzer auf, ergibt das ca. 65 Fr. Umsatz pro Person und Jahr, oder 18 Rappen pro Tag – Tendenz steigend. Natürlich «schenken» wir dieses Geld Google nicht wirklich, und notabene wird auch niemand gezwungen zum Googeln. Aber es ist der Preis, den die Werbewirtschaft für unsere Daten zu zahlen bereit ist.



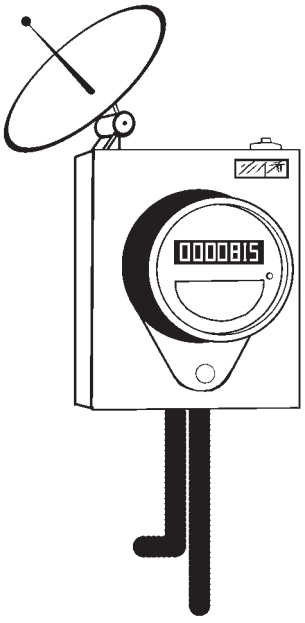
Was verrät der Stromzähler über mich?

Intelligente Stromzähler können den Energieverbrauch im Haushalt optimieren. Die Feinheit der von ihnen gesammelten Daten lässt aber auch detaillierte Rückschlüsse auf Lebens- und Konsumgewohnheiten zu.

Urs Meister

Vernetzte, intelligente Stromzähler, sogenannte «Smart Meter», gelten als Schlüssel zur Optimierung des Energieverbrauchs im Haushalt. Ziel ihrer Anwendung ist weniger die Minimierung des Strombezugs, sondern eine sinnvolle Verteilung über die Zeit. Ein Smart Meter kann etwa den Einsatz von Elektrogeräten mit kurzfristig variierenden Preisentwicklungen im Strommarkt koordinieren. Dabei wird der Smart Meter zur eigentlichen Datenplattform: Einerseits erhält er Informationen über aktuelle Tarifentwicklungen zur Optimierung der Gerätesteuerung. Anderseits sammelt er Verbrauchsdaten in kurzen Zeitintervallen (stündlich, viertelstündlich, minuten- oder sekundengenau). Diese leitet er an den Stromversorger weiter, der sie für die Rechnungsstellung verwendet. Selbst wenn diese Verbrauchsdaten (Lastgang) nur in aggregierter Form weitergegeben werden, lässt sich daraus recht genau eruieren, welche Haushaltgeräte zu welcher Zeit im Einsatz stehen. Versuche haben gar gezeigt, dass bei sekundengenauer Messung theoretisch eine Identifikation des eingeschalteten TV-Programms möglich ist, da mit der variierenden Helligkeit der Bilder auch spezifische Stromverbrauchsprofile resultieren. Je nach Genauigkeit der Messung und zeitlicher Auflösung lassen sich daher detaillierte Rückschlüsse über Lebens- und Konsumgewohnheiten machen, etwa über den Lebensrhythmus, das Kochverhalten, die Häufigkeit von Ferienabwesenheiten, die Art und (Alters-) Struktur der Haushaltgeräte oder die Hygienegewohnheiten. Solche Informationen helfen nicht nur bei der Stromverbrauchsoptimierung. Sie wären auch für personalisiertes Marketing nützlich – oder im Falle von Rechtsstreitigkeiten.

Intelligente Stromzähler können den Energieverbrauch im Haushalt optimieren. Die Feinheit der von ihnen gesammelten Daten lässt aber auch detaillierte Rückschlüsse auf Lebens- und Konsumgewohnheiten zu.



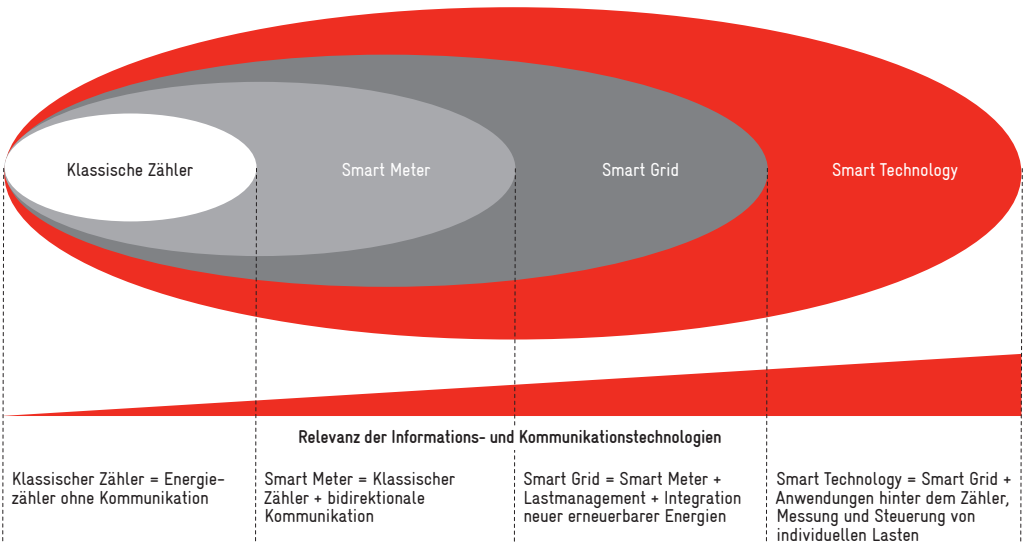
Verbraucher können nicht in jedem Fall sicher sein, dass ihr Stromlieferant diese Daten ausschliesslich im Rahmen der Energietarifierung verwendet. Im liberalisierten Markt treten neue Akteure als Energielieferanten und Smart-Meter-Betreiber auf, die parallel noch in anderen Geschäftsbereichen tätig sind. Umgekehrt expandieren die bisherigen Energieversorger vermehrt in neue Märkte, etwa Energieberatung oder Telekomleistungen. Die von einem Smart Meter gewonnenen Daten wären für Mar-

ketingmassnahmen in diesen Geschäftsfeldern durchaus attraktiv. Dem Thema Datenschutz kommt deshalb grosse Bedeutung zu: Welche Daten und in welcher Granulation gehen an den Versorger? Wer hat Zugriff auf die Daten (Versorger, Netzbetreiber, nur bestimmte Personen oder Abteilungen)? An wen dürfen (wenn überhaupt) Daten weitergegeben werden? Wie werden die Daten technisch übertragen (Übertragungstechnologie, Verschlüsselung)? Wie lange werden die Daten gespeichert? In welcher Weise hat der Verbraucher Zugriff auf seine Daten?

Vermutlich gibt das geltende Datenschutzgesetz auf solche Fragen unzulängliche Antworten, so dass über weitere, spezifischere Regelungen diskutiert wird. Besonders restriktive (gesetzliche) Rahmenbedingungen bei der Datennutzung könnten die potenziellen Vorteile der Smart-Meter-Technologie beschränken. Denn je aggregierter die gesammelten Daten und je eingeschränkter die Verwendungsmöglichkeiten sind, desto geringer ist ihr ökonomischer Wert. Umgekehrt können gänzlich fehlende Regelungen und allfällige Missbräuche das Vertrauen auf Seiten der Verbraucher erodieren lassen, so dass die eigentlich sinnvolle Verbreitung gehemmt wird. Auch sollte es dem Verbraucher selber überlassen werden, in welchem Ausmass er Transparenz gewähren will. Immerhin könnte es für ihn auch lohnend sein, Daten über das eigene Verhalten Dritten zugänglich zu machen – etwa wenn damit eine finanzielle Kompensation verbunden ist. Nutzen und Gefahren eines Smart Meter Einsatzes sind in jedem Fall heterogen verteilt. Letztlich können Fragen zur Datensicherheit im Zusammenhang mit Smart Metern nicht isoliert beantwortet werden. In der zunehmend digitalisierten Welt werden solche und ähnliche Informationen auch von anderen Akteuren gesammelt – beispielsweise Social Media Plattformen, Digital-TV- und Streaming-Anbietern, anderen internetbasierten Medienplattformen sowie Online-Detailhändlern.

Verbraucher können nicht in jedem Fall sicher sein, dass ihr Stromlieferant diese Daten ausschliesslich im Rahmen der Energietarifierung verwendet.

Intelligente Stromzähler optimieren den Energieverbrauch im Haushalt



Quelle: Thoma / BKW 2011

Wie sicher ist E-Banking?

Ob E-Banking sicher ist, hängt einerseits von den bei den Banken implementierten Sicherheitsstandards ab. Anderseits trägt aber auch der Kunde selbst viel Verantwortung.

Verena Parzer Epp

Nüchtern betrachtet ist Hacking ein Geschäftsmodell, wenn auch eine illegales. Deshalb kann man davon ausgehen, dass Hacker, so wie andere Geschäftsleute auch, Aufwand-Ertrags-Überlegungen machen. Je niedriger die Früchte hängen, desto eher werden sie gepflückt. Bei einem Einbruch suchen sie gezielt nach Schwachstellen im System.

Es ist wahrscheinlich korrekt, zu sagen, dass grundsätzlich alle in der Schweiz heute angebotenen E-Banking-Systeme sicher sind.

Es ist wahrscheinlich korrekt, zu sagen, dass grundsätzlich alle in der Schweiz heute angebotenen E-Banking-Systeme sicher sind.

Es ist wahrscheinlich korrekt, zu sagen, dass grundsätzlich alle in der Schweiz heute angebotenen E-Banking-Systeme sicher sind. Die Banken verfügen über grosse Abteilungen mit viel technischem Know-how, um ihre Systeme zu betreuen. Und sie tauschen sich in einem schweizweiten Netzwerk intensiv untereinander aus, wie unsere Nachfragen gezeigt haben. Mittlerweile ist die Zwei-Faktor-Authentifizierung Standard, bei der zusätzlich zur Vertragsnummer und zum Passwort (Erster Faktor «Wissen») auf einem zweiten Gerät (beispielsweise einem Handy; Zweiter Faktor «Haben») ein einmaliger Zugangsschlüssel bereitgestellt wird.

Die Schwachstelle in diesem System sind weniger die Banken-Websites als die Kunden. Sie sind es, die entweder durch Schadsoftware auf ihren Computern oder Umleitungen auf gefälschte Websites («Phishing») gefährdet sind. «Grundsätzlich müssen wir davon ausgehen, dass ein Grossteil der Kundengeräte infiziert ist.», meint auch ein jahrelang im Online-Banking tätiger IT-Spezialist. Leider sind noch immer zu wenig Kunden konsequent bei der Einhaltung der Sicherheitsstandards, wie sie etwa von einer auf Internet-Banking spezialisierten Website des Kompetenzzentrums Informationssicherheit der Hochschule Luzern empfohlen werden:

01_ Regelmässige Sicherung der Daten auf externen Speichermedien
02_ Verwendung eines Virenschutzprogrammes
03_ Einsatz einer Firewall
04_ Regelmässige Softwareupdates
05_ Gebrauch von starken Passwörtern

Technisch interessierte User haben ferner die Möglichkeit, ihr E-Banking auf einem Passwort-geschützten USB-Stick mit separatem Betriebssystem zu betreiben, der einzig für diesen Zweck zum Einsatz kommt. Ein derartiger «Computer im Computer» ist weniger einbruchsgefährdet, weil er in den Funktionalitäten eingeschränkt ist und damit weniger Angriffsfläche bietet.

Dass E-Banking für die Kunden in der Schweiz sehr sicher ist, findet übrigens auch Volker Birk vom Chaos Computer Club Schweiz – wenn auch aus einem anderen Grund: Banken selbst haben grosses geschäftliches Interesse am Online-Banking, da sie damit viele Kosten sparen. Manipulationen und Fehlbuchungen fänden immer wieder statt, aber in der Regel seien die Finanzinstitute im Schadensfall sehr kulant. Anders als beim «Plastic money» würden Kunden selten zur Kasse gebeten, wenn beim E-Banking etwas schief laufe.

Es gibt noch einen dritten Grund, warum E-Banking, relativ zu anderen Zahlungsarten, sicher ist: Internationale Überweisungen dauern mehrere Tage, während derer sie von bankinterner Warnsoftware überprüft und gegebenenfalls blockiert werden können. Das Hacking im E-Banking verspricht kein schnelles Geld. Beim Skimming von Bankomatkarten und beim Missbrauch von Kreditkarten durch gestohlene Passwörter hängen die Früchte viel tiefer.

Statt des Bankgeheimnisses das Datengeheimnis?

Die Chancen der Schweiz, zum internationalen Zentrum für Datenspeicherung aufzusteigen, stehen gut. Kaum ein anderes Land kann auf nahezu 200 Jahre Frieden und eine stabile Rechtsordnung verweisen.

Verena Parzer Epp und Rudolf Walser

Freud und Leid liegen, so sagt man, nah beieinander. Das Leid – und vor allem der Ärger – über die weltweiten Schnüffeleien der US-Geheimdienste (und vieler anderer) könnten gerade der Schweiz viel Freude bringen. Die konkrete Chance, die es zu packen gilt, liegt darin, dass die weltweite Aufmerksamkeit zu den Daten schwenkt, unter anderem zu deren sicherer Aufbewahrung. Das hat auch handfeste wirtschaftliche Gründe. In einer wissensbasierten Gesellschaft sind Daten der Rohstoff schlechthin.

Daten sind das neue Kapital der Unternehmen, und es wird immer offensichtlicher, dass sie an einem wirklich sicheren Ort gespeichert werden müssen.

Der Wert eines Autos der Zukunft wird weniger in seinem Getriebe liegen, sondern in der Technologie, die es steuert und mit seiner Umwelt vernetzt. Daten sind das neue Kapital der Unternehmen, und es wird immer offensichtlicher, dass sie an einem wirklich sicheren Ort gespeichert werden müssen. Nicht nur Unternehmen und Privatpersonen, auch Regierungen und Verwaltungen haben Grund zur Vorsicht. Sie können ihre Funktionen nur so lange ausüben und Pensionen zahlen, Steuern erheben oder Wahlen organisieren, wie der Zugriff auf die Daten gewährleistet ist.

Für die Entwicklung des Internets hat das kalifornische Silicon Valley als Technologiehub Grossartiges geleistet. Die mittlerweile hochentwickelte Internetbranche braucht neben Innovationen und Investitionen nun aber eines: Verlässliche Institutionen, die den Unternehmern helfen, die Früchte ihrer Arbeit zu ernten – und vor Interventionen der Geheimdienste zu schützen. Der NSA-Skandal hat Silicon Valley direkt geschadet. Die «Big Five» des Internets (Apple, Microsoft, Google, Amazon, Facebook) sind letztlich, wie alle Unternehmen, auf das Vertrauen ihrer Kunden angewiesen. Und diese sind immer weniger geneigt, ihre Daten in den USA zu wissen.

Die Schweiz hat in mehrfacher Hinsicht gute Chancen, sich als Datenhort zu etablieren:

- Starke Vernetzung: Die Schweiz ist bereits heute in hohem Ausmass globalisiert.
- Geschichte: Kaum ein anderes Land kann auf zweihundert Jahre Frieden zurückblicken.
- Geopolitischer Bonus: Traditionell ist die Schweiz Standort internationaler Organisationen. Auch in den USA wäre die Schweiz als zentraler Datenspeicherort wohl eher toleriert als andere Länder.
- Das «kleinere logistische Übel»: Es wäre für die betroffenen Internetfirmen einfacher, die Server in einem Land zu betreuen als in hundert verschiedenen.
- Gute Rechtsgrundlage: International geniesst der Schweizer Datenschutz einen guten Ruf.
- Professionalität: Der Erfolg des Schweizer Bankwesens hatte – neben dem Bankgeheimnis – ohne Zweifel auch mit den professionellen Dienstleistungen gerade in der Handhabung und Verwaltung von finanziellen und persönlichen Daten zu tun.
- Interessante Standorte: Die vielen leeren Festungsbauwerke in den Alpen könnten umgenutzt werden.
- Technisches Know-how: Mit den beiden ETHs verfügt das Land über viel technische Expertise, auch einige grosse IT- Unternehmen haben den Sitz bereits hier.

Die Zukunft wird weisen, ob sich in der Schweiz ein derartiger Cluster entwickeln kann. In Anlehnung an Silicon Valley bräuchte es dafür wohl auch einen spritzigen Namen. Wie wäre es mit «Memory Mountains»?

Gibt es noch Anonymität?

Bei der Entwicklung hochgradig sicherer Kommunikationssysteme könnte die Quantenkryptographie eine Schlüsselrolle spielen, weil dabei keine klassische Datenübertragung mehr stattfindet.

Tibère Adler

Kann man im Zeitalter von Big Data überhaupt noch seine Privatsphäre wahren, wo doch alle Daten scheinbar jederzeit und allerorten zugänglich sind? Ungeschützt vor dem Zugriff Dritter werden heute unsere Daten gesammelt, geteilt, analysiert und immer neuen Algorithmen zum Frass vorgeworfen. Nicht zuletzt der NSA-Skandal hat die Angst vor dem totalen Verlust der Intimsphäre geschürt. Aber immerhin: Es gibt eine Technologie, die diesem Transparenzwahn ein Ende setzen und den Weg zu wirklich sicherer Datenübertragung ebnen könnte. Die Rede ist von der «Quantenkryptographie».

Ungeschützt vor dem Zugriff Dritter werden heute unsere Daten gesammelt, geteilt, analysiert und immer neuen Algorithmen zum Frass vorgeworfen.

Am Lehrstuhl für Physik der Universität Genf gehört die Quantenphysik zu den bedeutendsten Disziplinen. Sie ist das Forschungsgebiet von Professor Nicolas Gisin, der erst kürzlich für seine Arbeiten auf den Gebieten der Quantenmechanik und Quantenkryptographie mit dem «Prix Marcel Benoist» 2014 ausgezeichnet wurde. Mit seinem Buch «Der unbegreifliche Zufall» hat er seine Erkenntnisse auch einem breiteren Publikum zugänglich gemacht.

Konkret untersucht Nicolas Gisin bei seinen quantenphysikalischen Experimenten das Phänomen der sogenannten «Quantenverschränkung», von der man spricht, wenn zwei physikalische Teilchen unabhängig von ihrem Abstand eine Gesamtheit bilden. Bei der Berührung eines der beiden Teilchen wird auch das andere berührt – der Zustand des einen bestimmt den Zustand des anderen. Diese «Verschränkung» beruht auf dem zweiten Grundsatz der Quantenmechanik, der sogenannten «Nichtlokalität». Verhalten sich zwei unabhängige Teilchen gleich, dann ist die Verbindung zwischen ihnen «nichtlokal». Die Interaktion zwischen nichtlokalen Teilchen kann mit klassischer Physik nicht erklärt werden. Aber sie könnte der Schlüssel für die Entwicklung hochgradig sicherer Kommunikationssysteme sein.

Genaugenommen ist die Datenübertragung der Schwachpunkt jeder Datencodierung: Sobald Daten physisch von einem Punkt auf einen anderen transferiert werden, können sie ausspioniert werden. Und angesichts der ununterbrochen wachsenden Rechnerleistung können alle verschlüsselten Daten irgendwann geknackt werden.

Das Besondere an der Quantenkryptographie ist, dass es bei ihr die klassische Phase der Daten-

übertragung nicht gibt – und so entfallen auch die damit verbundenen Risiken. Stark vereinfacht muss man sich eine quantenkryptographische Datenübertragung folgendermassen vorstellen:

01_ «Quantenverschränkung»: Quanten-Sender und Quanten-Empfänger werden miteinander in Verbindung gebracht. (Laut bisherigen Studien sind Verschränkungen über Distanzen von bis zu 300 km möglich). Bei Kontrollmessungen liefern Sender und Empfänger durch einen «unbegreiflichen Zufall» (um den Buchtitel von Professor Gisin aufzunehmen) immer das gleiche Ergebnis, d.h. sie generieren stets absolut identische Daten.

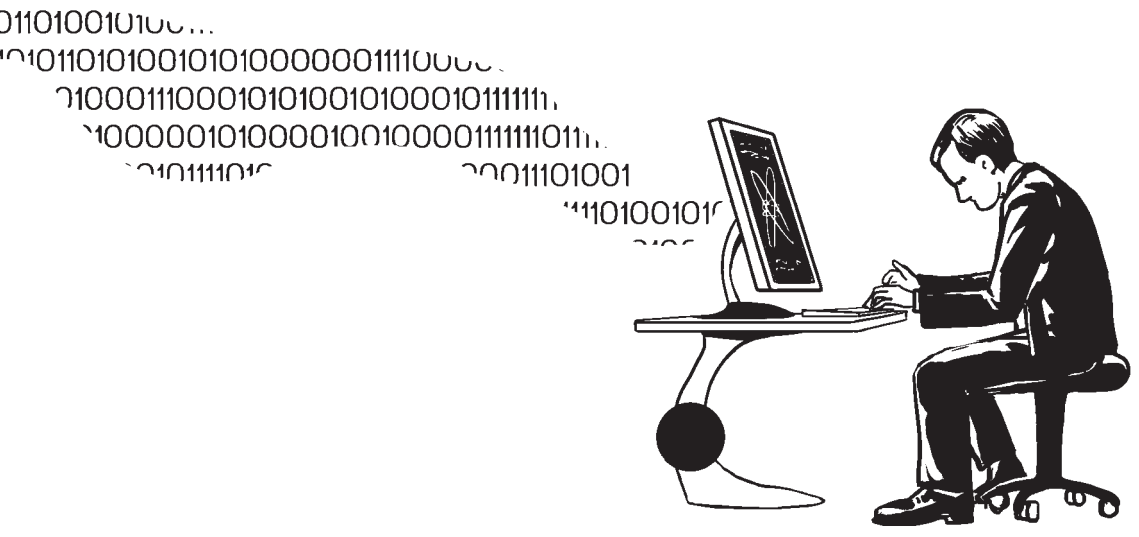
02_ Identifikation möglicher Lauschangriffe: Durch die Eindeutigkeit der Verschränkung kann überprüft werden, ob der Kanal zwischen Quantensender und Quantenempfänger abgehört wird. Im Fall eines Lauschangriffes findet kein Datentransfer statt, sondern wird eine neue Quantenverschränkung hergestellt. Besteht jedoch keine Abhörgefahr, können die Daten ausgetauscht werden.

03_ Der eigentliche Datenaustausch findet idealerweise per «Quantenteleportation» statt, bei der die Daten beim Empfänger aufgebaut werden, kurz nachdem sie beim Sender verschwunden sind – und zwar ohne, dass zwischen beiden eine physische Verbindung bestünde. Eben dieser Prozess garantiert maximale Sicherheit.

Zumeist beruhen quantenkryptographische Verschlüsselungen allerdings immer noch auf einem gemeinsamen Kodierungsschlüssel, der bei jeder Verwendung neu berechnet wird. Das ist gleichzeitig eine weitere praktische Anwendung quantenphysikalischer Erkenntnisse: die zuverlässige Generierung echter Zufallszahlen.

Das Besondere an der Quantenkryptographie ist, dass es bei ihr die klassische Phase der Datenübertragung nicht gibt – und so entfallen auch die damit verbundenen Risiken.

Unsere derzeit scheinbar vollkommen von Angreifern umzingelte Anonymität könnte mit der Quantenkryptographie durchaus ihren Retter gefunden haben.



Was muss man über Datenübermittlung wissen?

Juristisch liegt die Verantwortung für die sichere, verschlüsselte Übertragung sensibler Daten immer beim Sender. Besonders heikle Nachrichten und Datensätze gehören nicht ins Netz. Sie sollten direkt überbracht werden.

Alexandra Christen

Heutzutage werden immer mehr heikle Daten über das Internet verschickt. Dabei ist vielen Menschen zu wenig bewusst, dass ihre Informationen nicht immer nur vom eigentlichen Empfänger gelesen werden. Der NSA-Skandal hat gezeigt, dass eine Firewall allein keine genügende Datensicherheit gewährleisten kann. Daten werden nämlich häufig nicht nur direkt auf den Rechnern, sondern auch auf dem Weg zwischen ihnen in grossem Umfang abgeschöpft. Dessen sollten sich, wenn schon nicht alle Internet-User, zumindest die Unternehmen und öffentlichen Organisationen bewusst sein.

Sicher ist die Verschlüsselung der Daten nicht immer notwendig. Wenn man einen Gruss übermitteln will, kann die Nachricht unverschlüsselt gesendet werden. Sobald aber eine Nachricht heikle Informationen (z.B. vertrauliche Daten wie Finanz- oder Personaldaten) beinhaltet, ist eine Verschlüsselung angezeigt. Mittlerweile sind die Verschlüsselungsmechanismen sehr effizient, sodass der Inhalt der Daten für Aussenseiter nur mit erheblichem Aufwand lesbar ist. TLS (Transport Layer Security), der Nachfolger von SSL, ist ein Protokoll zum Schutz persönlicher Daten, die im Internet versendet werden. Es gewährleistet nicht nur den verschlüsselten Transport von Informationen, sondern auch die Identifikation des Empfängers. Praktisch alle Browser unterstützen TLS. Es wird auch beim Abruf von Mails über POP3 und IMAP verwendet.

Mit einer vorsorglichen Verschlüsselung des E-Mail-Verkehrs kann eine Firma nicht nur Nerven, sondern auch viel Geld sparen.

Werden die Daten über eine Website übermittelt, sollte man immer darauf achten, dass das Verschlüsselungssymbol angezeigt wird und «https» am Anfang der Adresszeile erscheint. (Das zusätzliche «s» nach dem Kürzel «http» steht dabei für «secure».) Jede Webseite sollte ein Zertifikat besitzen. Darüber kann man erfahren, ob die Seite wirklich vom richtigen Absender stammt. Diese kann man mit einem Klick auf den Schlüssel vor dem Hyperlink kontrollieren.

Eines gilt es jedoch zu beachten: Sicherheit ist ein relativer Begriff, und eine zu 100% sichere Datenübertragung ist grundsätzlich nicht möglich. Selbst bei verschlüsselten Nachrichten können trotz geschütztem Inhalt die Metadaten wie Sender, Empfänger und Uhrzeit ausgelesen werden. So können Überwacher herausfinden, mit wem man im Kontakt steht. Besonders heikle Nachrichten und Datensätze gehören nicht ins Internet. Sie sollten (idealerweise) direkt überbracht werden.

Auch wenn es auf der technischen Seite viele offene Fragen gibt – rechtlich ist die Angelegenheit klar: Die Verantwortung für die Verschlüsselung sensibler Daten liegt immer beim Sender – solange er sich nicht explizit, etwa durch eine Vereinbarung, von der Aufgabe der Verschlüsselung befreit. Personendaten dürfen laut Gesetz niemals unverschlüsselt gesendet werden. Geschieht dies trotzdem und werden die Daten von unbefugten Drittparteien ausgelesen, so kann dies rechtliche Konsequenzen nach sich ziehen. Mit einer vorsorglichen Verschlüsselung des E-Mail-Verkehrs kann eine Firma also nicht nur Nerven, sondern auch viel Geld sparen.

Auf welchem Berggipfel ist noch Ruh?

Eine Hochtour ist ein gutes Rezept, um dem Datenmeer für ein paar Stunden zu entrinnen. Die digitale Ruhe hat auch ihre Schattenseiten, ebenso der Bewilligungsprozess für die Handy-Ortung bei Rettungseinsätzen.

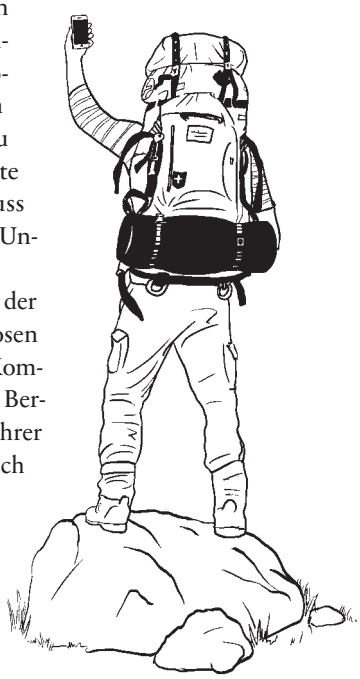
Simone Hofer Frei

Im Sommer in den Walliser Alpen: auf der Hinterseite einer SAC-Hütte drängen sich auffallend viele Wanderer und Bergsteiger rund um eine kleine Sitzbank – und blicken gespannt auf ihr Mobiltelefon. Es ist der einzige Ort in Hüttennähe, wo die Geräte wenigstens einen Netzstrich anzeigen, gerade genug, um das sichere Erreichen des Übernachtungsorts per SMS zu bestätigen. Dann heisst es für alle: Handy möglichst rasch abschalten, denn aufladen lassen sich die Geräte in hochgelegenen Berghütten, die Strom aus eigenen Solaranlagen oder über einen Generator beziehen, in der Regel nicht. Doch längst nicht alle Hütten haben Mobilnetzempfang. Wo in den Bergen Schnee und Eis liegt, weisen auch die Netze der Mobilfunkanbieter ausgedehnte weisse Flecken auf, wie die Swisscom-Netzabdeckungskarte zeigt. Im Hochgebirge und in abgelegenen Gebieten herrscht noch mehr digitale Ruhe, als viele wahrhaben wollen. Und das kann im Notfall zum Problem werden.

Wo in den Bergen Schnee und Eis liegt, weisen auch die Netze der Mobilfunkanbieter ausgedehnte weisse Flecken auf. Im Hochgebirge herrscht noch mehr digitale Ruhe, als viele wahrhaben wollen. Das kann im Notfall zum Problem werden.

Die vermeintliche Sicherheit, dass «die mich dank der App schon finden werden», verleitet zuweilen zur Sorglosigkeit. Immer wieder muss die Bergrettung überforderte oder erschöpfte Berg- und Tourengänger holen. Gemäss Auskunft der Alpinen Rettung Schweiz dürfen sich Berggänger nicht darauf verlassen, dank ihrem Mobiltelefon im Notfall rasch gefunden zu werden. Wo kein Netzempfang ist, gehen auch keine Notrufe ab. Und wenn Empfang da ist, scheitert die Ortung regelmässig an profaneren Ursachen: Der Akku ist leer, oder die GPS-Funktion wurde ausgeschaltet, um den Akku zu schonen, der sich in den Bergen bei Kälte und Wind besonders schnell leert.

Hinzu kommt ein weiteres Problem: Auch wenn die Ortung technisch funktionieren würde, dürfen die Bergretter vorerst nur auf Sicht suchen, denn jede Handyortung braucht eine Bewilligung, einzuholen bei der Polizei desjenigen Kantons, auf dessen Boden der Gesuchte vermutet wird. Da aber Bergketten in vielen Fällen auch Kantonsgrenzen darstellen, sind häufig mehrere Kantone mit unterschiedlichen Bewilligungsprozessen involviert. Oft müsste die Polizei selber noch eine Bewilligung bei einer übergeordneten Stelle einholen. Die Folge: Es dauert zu lange, bis die Bewilligung für die Ortung des Mobiltelefons einer vermissten Person eintrifft. Zudem lässt sich die Position auch dann noch zu wenig genau definieren. Der letzte Ortungspunkt muss nicht zwingend der Unfallort sein.



Selbst im Zeitalter der scheinbar grenzenlosen mobilen digitalen Kommunikation setzen Bergrettung und Bergführer deshalb auch heute noch auf eine alte, zwar nicht abhörsichere, aber sehr zuverlässige Kommunikationstechnologie – den Funk.

Wo soll ich meine Daten speichern?

Wo sind Daten sicher abgelegt? In der Cloud? Oder auf dem eigenen Server? Das ist gar nicht so eindeutig, stellt Markus Brönnimann, Experte für IT-Governance und Informationssicherheit beim Datenschutzbeauftragten des Kantons Basel Stadt, fest.

Markus Brönnimann im Interview mit Verena Parzer Epp

Herr Brönnimann, was verstehen Sie unter einem sicheren Speicherort?

Einen wirklichen sicheren Speicherort gibt es nicht. Letztlich muss man davon ausgehen, dass jedes Sicherheitssystem geknackt werden kann. Es ist nur eine Frage der Fähigkeiten, der Ressourcen und der Zeit, die ein «Einbrecher» zur Verfügung hat. Mit Schutzmassnahmen kann man nur die Wahrscheinlichkeit, dass ein Einbruchversuch erfolgreich endet, beeinflussen.

Grundsätzlich stellt sich die Frage, welchen Wert die zu schützenden Daten haben und welcher Aufwand für ihren Schutz getrieben werden soll. Es gibt zwei Extreme: Auf der einen Seite die «kostenlosen» Cloud-Angebote. Hier sollte man beachten, dass das Businessmodell der Anbieter in vielen Fällen darauf aufbaut, aus den Kundendaten Gewinne zu erzielen. Andererseits könnte man die Daten auf einem Rechner ohne Netzwerkanschluss und mit einer «sicheren Verschlüsslung» speichern. Daten sind dann nur zugänglich, wenn jemand physischen Zugriff auf den Rechner hat. Es ist aber sehr unpraktisch, Daten auf einem Rechner ohne Netzverbindung abzulegen.

«Grundsätzlich stellt sich die Frage, welchen Wert die zu schützenden Daten haben und welcher Aufwand für ihren Schutz betrieben werden sollte.»

Berücksichtigen wir zusätzlich die Diskussionen um absichtlich eingebaute Sicherheitslücken und kompromittierte Verschlüsselungsalgorithmen, wie sie u. a. durch die Snowden-Enthüllungen allgemein bekannt wurden, kann man auch daran zweifeln, welche Massnahmen überhaupt zuverlässig sind. Man kann davon ausgehen, dass eingebaute «Soll-Schwachstellen» nicht ausschliesslich vom Urheber, sondern auch von Dritten genutzt werden können.

Welche Daten betrachten Sie bei Privatpersonen als besonders schützenswert?

Diese Frage wird immer schwieriger zu beantworten. Mit der zunehmenden Verbreitung der Big-Data-Analyse-Möglichkeiten können triviale Daten plötzlich neu interpretiert werden und es werden Schlüsse auf eine Person möglich, ohne dass diese ihre Daten je explizit preisgegeben hat. Grundsätzlich sind aus meiner Sicht folgende Daten schützenswert: Zum einen Daten, die ich meinem direkten Umfeld (Arbeitgeber, Familie oder Freunde) nicht oder zumindest nicht «ungesteuert» anvertrauen möchte. Zum anderen auch Daten, die an einem Ort (beispielsweise beim Hausarzt) frei zur Verfügung stehen sollen, aber nicht zu Dritten, etwa zum Arbeitgeber, gelangen sollen. Eine fundierte Vorstellung, wie schützenswert (persönliche) Daten sind, muss in einem ersten Schritt der Einzelne vornehmen. In vielen Bereichen müssen wir aber dringend als Gesellschaft einen qualifizierten Konsens finden, wie mit unseren Daten umgegangen werden soll.

«Mit der zunehmenden Verbreitung der Big-Data-Analyse-Möglichkeiten können triviale Daten plötzlich neu interpretiert werden und es werden Schlüsse auf eine Person möglich, ohne dass diese ihre Daten je explizit preisgegeben hat.»

Wie wichtig sind regelmässige Sicherheitsupdates?

Grundsätzlich sind Sicherheitsupdates wichtig – eben weil sie die Verwundbarkeit (durch bekanntgewordene Schwachstellen) verringern sollen. Aber auch hier muss man dem Anbieter vertrauen, da er auf diesem Weg problemlos und ungefragt Daten von meinem System abschöpfen könnte. Das System sollte zudem nach dem Update mindestens gleich gut funktionieren. Beides scheint nicht immer der Fall zu sein.

Gibt es eine sichere Cloud?

Auch diese Frage kann nicht pauschal beantwortet werden. Die erste Unsicherheit besteht darin, was eine Cloud ist. So kann beispielsweise eine Public Cloud schwerlich mit einer Private Cloud verglichen werden. Unabhängig davon, ob wir von einem Outsourcing, einer Cloud oder sonst einer Lösung sprechen, die ausserhalb unseres direkten Kontrollbereichs genutzt wird, sollten wir uns in Bezug auf den Anbieter zu folgenden Punkten Gedanken machen:

01_ Welche Interessen, welches Businessmodell hat der Anbieter?

02_ Kann er aufzeigen, wie er meine Daten schützen will? Ist das realistisch?

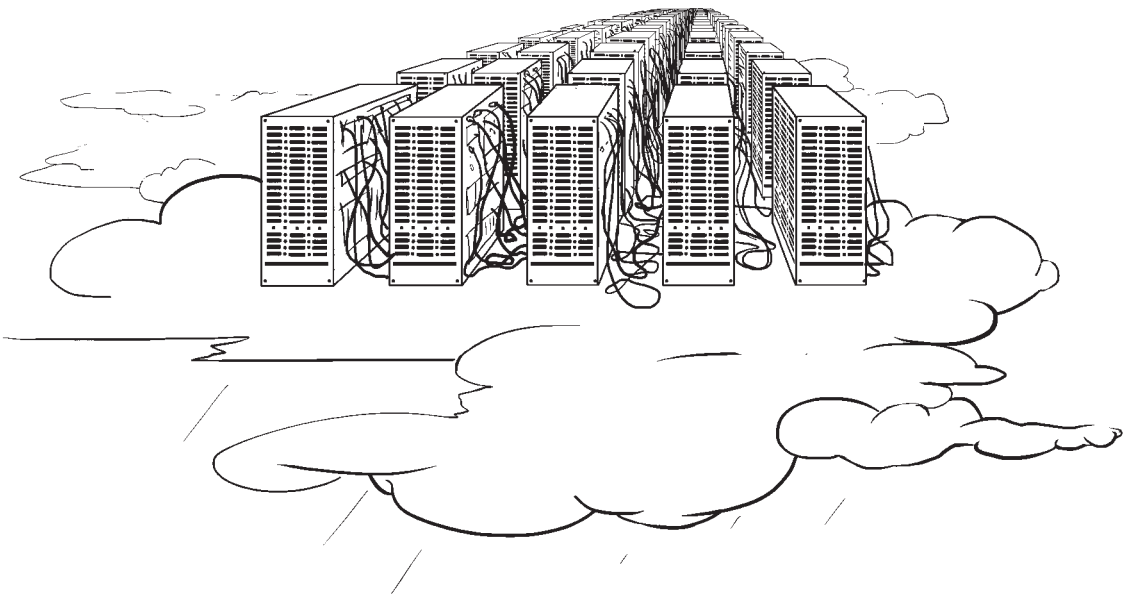
03_ Vertraue ich dem Anbieter?

04_ Was passiert dem Anbieter, wenn meine Daten bei ihm «verschwinden»? Muss er mit negativen Konsequenzen (Bussen oder Reputationsverlust) rechnen?

Soll man auch Vorkehrungen für Krankheit oder Todesfall treffen?

In einer Gesellschaft, in der das reale Leben immer mehr mit dem digitalen verschmilzt, scheint es sinnvoll, sich über dieses Thema Gedanken zu machen. Muss beispielsweise jemand die Passwörter meines E-Mails, meiner Bankkonten und Social-Media-Konten erhalten, um diese deaktivieren oder sperren zu können? Hier gibt es am Markt bereits erste Angebote, die einer Vertrauensperson nach einiger Zeit und nach dem Durchlaufen einiger Sicherheitsbarrieren Zugang gewähren. Aber auch hier steht – einmal mehr – das Vertrauen in den jeweiligen Anbieter im Vordergrund.

«Die erste Unsicherheit besteht darin, was eine Cloud ist. So kann beispielsweise eine Public Cloud schwerlich mit einer Private Cloud verglichen werden.»



Wie merke ich mir ein gutes Passwort?

Ein gutes, kreatives Passwort bietet Schutz vor Hackern. Mit ein paar einfachen Tricks kann man dem Gedächtnis beim Einprägen komplizierter Kombinationen auf die Sprünge helfen.

Simon Hurst

Lediglich einen Sekundenbruchteil benötigt ein normaler Computer, um eines der häufigsten Passwörter zu knacken. Es lautet schlicht: password. Gleich schnell geht es bei 123456 (Rang 2), 12345678 (Rang 3) und den übrigen 9997 Wort- und Zahlenkombinationen, die sich auf der Liste mit den 10 000 häufigsten Passwörtern vom Sicherheitsspezialisten Mark Burnett finden.

Um das Passwort «_%MnPizsl,tvien08!_» zu knacken, braucht ein durchschnittlicher PC geschätzte 364 Quintillionen Jahre.

Wie werden solche Ranglisten erstellt? Es vergeht kaum eine Woche, in der nicht grosse Mengen an Benutzername-Passwort-Kombinationen wegen Sicherheitslücken an die Öffentlichkeit geraten. Diese werden von Leuten wie Burnett gesammelt und ausgewertet. Zugegebenermassen sind diese Listen nicht repräsentativ, denn sie stammen meist von Anbietern mit tiefen Passwortanforderungen. Sie zeigen aber, dass die meisten Menschen nicht eben an die Grenzen ihrer Kreativität gehen, solange man ihnen freie Hand lässt: 40 % der User verwenden ein Passwort aus den Top 100, etwa football, batman oder test. Und über 90 % beschränken sich auf eine Auswahl von gerade mal 1000 Wörtern. Ein leichtes Spiel für Hacker.

Sichere Passwörter zu verwenden, die man sich auch ohne Elefantengedächtnis merken kann, muss gar nicht mühevoll sein. Die folgende Methode kann dabei helfen. Zuerst braucht es einen einfachen, einprägsamen Satz, z. B.: «Mein neues Passwort ist zwar sehr lang, trotzdem vergesse ich es nie.» Das neue Passwort wird dann aus Anfangsbuchstaben und Satzzeichen konstruiert: «MnPizsl,tvien.» Diese Kombination kann man noch um Ziffern oder Sonderzeichen ergänzen, die für einen selbst Sinn ergeben (z. B. Jahreszahlen). Um das Passwort «_%MnPizsl,tvien08!_» zu knacken, braucht ein durchschnittlicher PC geschätzte 364 Quintillionen Jahre – eine Zahl mit immerhin 30 Nullen.

Eine andere, unter Umständen noch einfachere Variante ist, mehrere zufällig gewählte Worte in wilder Reihenfolge anzuordnen: Für «PferdeLachenTanzen» braucht ein PC immerhin schon 61 Trillionen Jahre.

Grundsätzlich erhöhen Sie mit folgenden Massnahmen die Sicherheit Ihrer Passworte:

01_ Je länger, desto besser: mindestens 12 bis 16 Zeichen
02_ Zufällige Zeichenfolge: keine real existierenden Worte aus dem Lexikon
03_ Kombination von Gross- und Kleinbuchstaben, Zahlen, Satz- und Sonderzeichen
04_ Abwechslung: für jeden Dienst ein anderes Passwort
05_ Häufige Wechsel: neue Passwörter alle paar Monate
06_ Passwörter auswendig lernen – und nirgends aufschreiben
07_ Sicherheitsfragen auslassen: Die Antworten auf solche Standardfragen sind meist einfach zu erraten.

Völlige Sicherheit gibt es auch bei komplizierten Passwörtern nicht, denn Internet-Kriminelle kennen noch andere Wege als automatisiertes Raten, z. B. Phishing: scheinbar vertraute, aber gefälschte Websites, die nach Benutzernamen und Passwort fragen. Nicht umsonst setzen heute sensible Internetdienste (z. B. E-Banking) auf sogenannte Mehrfaktorautorisierung, bei der zusätzlich ein Code über ein anderes Gerät (z. B. Mobiltelefon) bestätigt werden muss. Mit Passwörtern wie den oben erwähnten fährt man aber bereits sehr gut. Verwenden sollte man sie , da sie nun schon in diesem Beitrag erwähnt werden, natürlich nicht mehr.

Wie geht Kindererziehung 2.0?

Eltern müssen, auch von Gesetzes wegen, ihren Kindern einen vernünftigen Umgang mit dem Internet beibringen. Verbote und Filter allein helfen kaum, da für viele Jugendliche Facebook und Co. zum erweiterten Lebensraum gehören.

Simone Hofer Frei

Auch die Eltern der heutigen «Netzwerkkinder» buchen ihre Ferien online, schauen ständig aufs Handy, bestellen Weihnachtsgeschenke über Amazon und suchen auf Facebook nach ehemaligen Schulkameraden. Aber: Für sie ist das Internet ein sehr effizientes Hilfsmittel geblieben, und nicht, wie für ihre Kinder, zum erweiterten Lebensraum geworden. Social Media dienen dazu, bei Bedarf auf Berufsbekanntschaften zurückgreifen zu können, in Kontakt zu bleiben, um sich demnächst in einem realen Café zu treffen. Nicht so bei den «Digital Natives»: Man trifft sich im Netz, dabei sein zählt. Chatten ist spannender als Kaffeeklatsch und sie gamen nicht aus Langeweile, weil die Eltern nur einen Ausgang pro Woche erlauben, sondern bleiben aus freien Stücken zuhause und verabreden sich stattdessen im Web. Obwohl (oder gerade weil) der Mutter lieber wäre, die Diskussion drehte sich um die Frage, ob Sohn oder Tochter bereits um elf, oder wie alle anderen erst um zwölf wieder zuhause sein müsse, statt um die Frage, wann das WLAN am Samstagabend auszuschalten sei.

Zahlreiche Ratgeber unterstützen Kinder, Jugendliche und deren Eltern beim Erlernen von Medienkompetenz und im richtigen Umgang mit Facebook und Co. Die meisten dieser Ratschläge sind wichtig und richtig, besonders für jüngere Kinder: Genauso, wie man mit den Kindern das Überqueren der Strasse zuerst auf einer Quartierstrasse und nicht gleich auf einer sechsspurigen Einfallstrasse übt, sollten auch die ersten Schritte im Internet in einem geschützten Rahmen stattfinden.

Gemessen am tatsächlichen Mediennutzungsverhalten von Schweizer Jugendlichen (vgl. James-Studie 2012 und James-focus), muten einige dieser Empfehlungen aber als von der Realität arg strapaziert an. Datensparsamkeit? Facebook ist für viele Jugendliche die zentrale Werbeplattform in eigener Sache. Keine Bilder aufs Web? Das auf Bilder und Videos spezialisierte Instagram ist 2014 nebst Facebook zum beliebtesten sozialen Medium avanciert, vor allem bei jüngeren Nutzern. Das Recht am eigenen Bild? 39% geben an, dass bereits Bilder und Videos von ihnen ungefragt veröffentlicht wurden – nur etwa die Hälfte stört sich daran. Den PC an einem zugänglichen Ort in der Wohnung aufstellen? Auch diese oft empfohlene Massnahme verliert an Bedeutung, da 97% der Jugendlichen ein Smartphone besitzen und täglich damit im Internet surfen (James Studie 2014).

Datensparsamkeit? Facebook ist für viele Jugendliche die zentrale Werbeplattform in eigener Sache.

Trotzdem, selbst wenn die Aufgabe keine einfache ist: Eltern stehen in der Pflicht, auch von Gesetzes wegen, ihren Kindern einen vernünftigen Umgang mit dem Internet beizubringen und sie davor zu bewahren, sich selber oder Dritte zu schädigen. Das Thema Medienkompetenz findet sich auch im Lehrplan 21 wieder. Eine einheitlichere Vermittlung des Themas im Unterricht könnte vielleicht dazu beitragen, dass der digitale Graben nicht mehr quer durch die Lehrerzimmer führt, wie das bis anhin der Fall ist. Klar scheint, dass Verbote und Filter allein wenig zu einem vernünftigen Umgang mit dem Internet beitragen. Jugendliche müssen lernen, sich selber zu schützen – im Web und vor dem Web. Zu einem vernünftigen Umgang mit dem Web gehört nämlich auch, das reale Leben nicht zu vernachlässigen. Denn das Web ist und bleibt ein Hilfsmittel. Oder etwa nicht?

Ich wurde gehackt! Was jetzt?

Tanzt nachts der Mauszeiger allein auf dem Bildschirm, so liegt die Vermutung nahe, dass der Computer gehackt wurde. In diesem Fall ist rasches Handeln angezeigt, um weiteren Schaden zu verhindern.

Simone Hofer Frei

«Hallo Gast Visa Europe. Für Ihren Schutz haben wir ihre Kreditkarte sistiert. Klicken Sie hier…» Nicht immer sind Betrugsversuche so offensichtlich zu erkennen, wie bei dieser Phishing-Mail. Laut Schätzungen werden 73 % der Schweizer in ihrem Leben einmal Opfer von Cyberkriminalität. Der Norton Cybercrime Report bezifferte 2011 den direkten finanziellen Schaden auf 374 Mio. Fr., hinzu kämen im Mittel fünf Tage Ärger und zusätzliche Kosten, bis der Computer neu aufgesetzt, die Passwörter gewechselt, die Daten wieder hergestellt und eine neue Kreditkarte bestellt sei. Diese wohl nicht ganz uneigennützige Schätzung von einem Virenschutzhersteller über das Ausmass von Phishing- und Hacking-Angriffen in der Schweiz lässt sich leider nicht anhand offizieller Daten überprüfen. Die Koordinationsstelle zur Bekämpfung der Internetkriminalität KOBIK veröffentlicht zwar einen Jahresbericht, doch sind die bei Kobik gemeldeten Vorfälle wegen der hohen vermuteten Grauziffer wenig aussagekräftig. Die Schweiz kennt keine Meldepflicht für Cyber-Angriffe, auch dürften viele Cybercrime-Opfer auf eine Strafanzeige verzichten, da – anders als bei einem physischen Einbruch – keine Versicherung für den Schaden aufkommt. Die Chance, die meist gut getarnte und grenzüberschreitend agierende Täterschaft zu fassen, ist ohnehin sehr klein.

Laut Schätzungen werden 73 % der Schweizer in ihrem Leben einmal Opfer von Cyberkriminalität.

Im Prinzip gibt es zwei Arten von Hacking: Wenn der Computer durch Schadsoftware (Viren, Trojaner) infiziert wurde, empfehlen Experten die folgenden Schritte:

01_ Computer vollständig vom Netz trennen: Netzwerkkabel ausziehen, WLAN abstellen.

02_ Alle wichtigen Login-Passwörter für externe Dienste wie E-Mail, Apple-ID etc. von einem sauberen PC aus zurücksetzen und ändern.

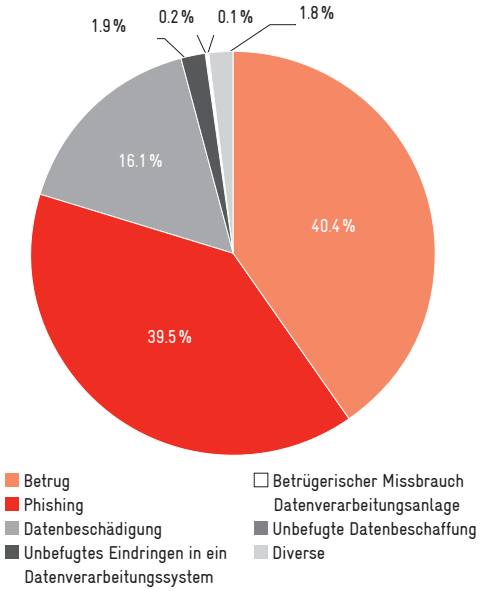
03_ Eine Sicherheitskopie auf einer separaten externen Festplatte erstellen und Malware mit einer aktuellen Antivirensoftware beseitigen. (Achtung: Nicht auf Drittgeräte kopieren, da sonst infizierte Dateien mitkopiert werden.)

04_ Die Festplatte des befallenen Gerätes neu formatieren, aufsetzen und Antiviren-Schutz neu installieren.

05_ Die Daten einzeln wieder übertragen.

Kompliziert kann es auch im zweiten Fall werden, wenn die Identität gehackt wurde und der Zugriff auf die E-Mail- und Social-Media-Konten, Kredit-

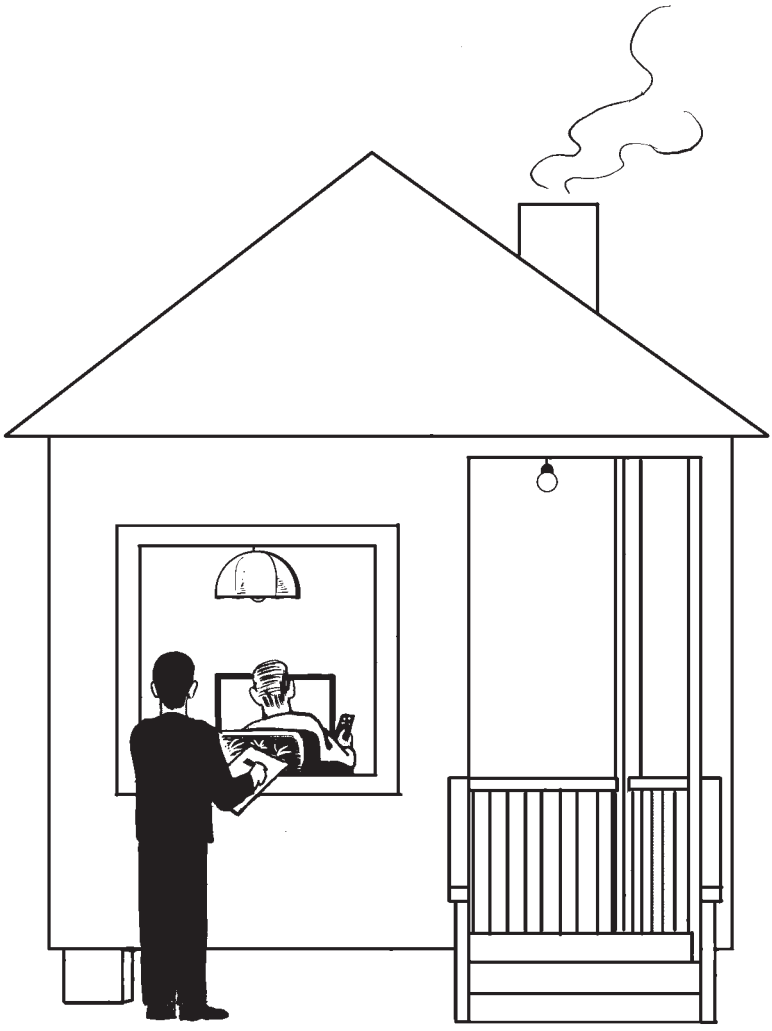
Meldungseingänge über strafbare Handlungen gegen das Vermögen im Internet



Quelle: Kobik Jahresbericht 2013

karte usw. erfolgte. Dass passiert entweder durch Phishing oder durch Social Engineering, indem Passwörter durch das Sammeln von persönlichen Informationen im Internet gehackt werden. In diesem Fall ist das oberste Ziel, möglichst rasch die Kontrolle über die eigenen Konten wiederzuerlangen und zu versuchen, weiteren finanziellen Schaden abzuwehren: Dazu den Dienstanbieter – am besten telefonisch – kontaktieren und das Konto sperren, bzw. die Zugangsdaten erneuern und neu möglichst mit einer 2-Faktor-Authentifizierung schützen. Wurde die gestohlene Identität dazu missbraucht, im Namen des Opfers Inhalte zu verbreiten, stellt sich die Frage, wie diese Falschmeldungen wieder beseitigt werden können: Einträge auf dem eigenen Social-Media-Konto können selber gelöscht werden. Tauchen Kommentare unter dem eigenen Namen auch auf Plattformen Dritter auf, bleibt nur, mit dem Besitzer der Seite oder dem Dienstanbieter Kontakt aufzunehmen und eine Löschung zu beantragen. Eine Anzeige bei der Polizei wegen Persönlichkeitsverletzung hilft selten, den Täter ausfindig zu machen, kann aber dem Antrag auf Löschung einen gewissen Nachdruck verleihen.

Das oberste Ziel ist, möglichst rasch die Kontrolle über die eigenen Konten wiederzuerlangen.



Haben Sie heute schon ein Gesetz gebrochen?

Punkto Datenschutz bewegen wir uns auch als normale Bürger auf dünnem Eis. Der Datenschutzspezialist David Rosenthal, Co-Leiter der IT-Rechtsberatung der Wirtschaftskanzlei Homburger, sagt, worauf man als Privatperson achten sollte.

David Rosenthal im Interview mit Verena Parzer Epp

Herr Rosenthal, wie gross ist das Risiko, dass ich wegen eines unbeabsichtigten Fehltritts im Netz angeklagt werde?

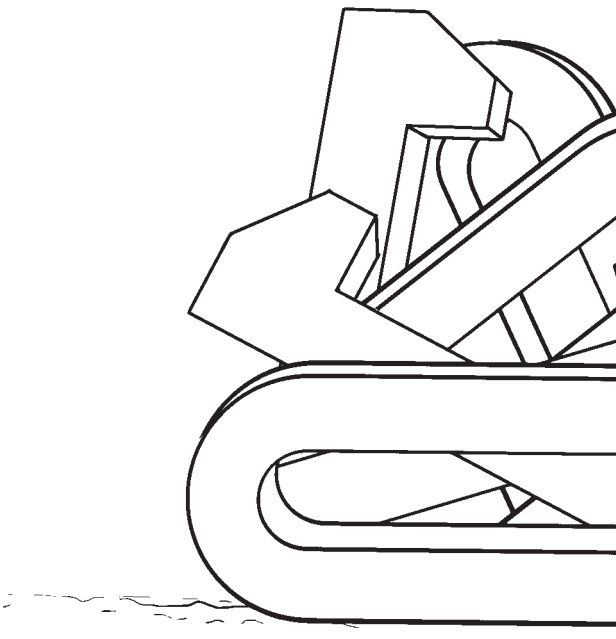
So schweres Geschütz fahren wir beim Datenschutz in der Schweiz nicht auf! Zum Glück nicht, denn jeder von uns verletzt laufend den Datenschutz. Klatsch und Tratsch über andere ist zum Beispiel streng genommen meist eine Persönlichkeitsverletzung. Grösser ist aus meiner Sicht aber das Risiko, im Netz die Kontrolle über eigene Daten zu verlieren: Eine coole App ist rasch mal installiert und Schwupps sind persönliche Daten aus dem Handy abgesaugt und auf irgendeinem fremden Rechner. Ist das unbeabsichtigt? Jein. Viele Handys weisen sogar ausdrücklich darauf hin, worauf eine App zugreift. Aber die meisten Leute interessieren sich nicht dafür, vermutlich weil sie abgestumpft sind. Sie wollen Technik einfach nutzen und sich über mögliche Datenfolgen keine Gedanken machen, so nach dem Motto «Kann ja nicht so schlimm sein».

«Sie selbst sollten auf Ihren Bauch hören: Wie fänden Sie es, wenn ein anderer das mit Daten über Sie macht?»

Welche Mindeststandards sollten Privatpersonen punkto Datenschutz einhalten? Inwiefern sind sie für ihre eigene Sicherheit verantwortlich?

Geht es nur um eigene Daten, muss jeder seine Komfortzone selbst finden. Bevor ich eigene Daten weitergebe, frage ich meinen Bauch nach dem Risiko, dass damit Unfug getrieben wird. Er ist dank meiner Datenschutzerfahrung natürlich gut geschult. Ab und zu lese ich sogar eine Datenschutzerklärung. Aber selbst wenn ich verstehe und mir passt, was mir da versprochen wird, ist es am Schluss eine Vertrauensfrage, denn kontrollieren oder erzwingen kann ich das nicht wirklich. Das macht die Sache so schwierig. Aber es führt immer wieder dazu, dass ich gewisse Angebote im Netz nicht nutze, oder gewisse Informationen wie etwa meine normale E-Mail-Adresse nicht angebe, weil ich den Empfänger nicht gut genug einschätzen kann.

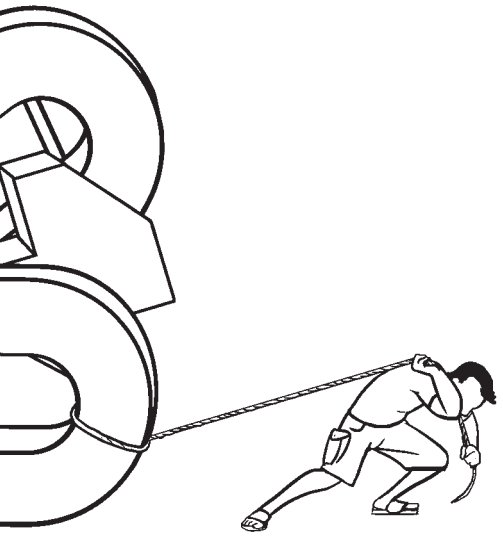
Ist es illegal, wenn ich mit meinen Handy-Kontaktdaten auf Facebook nach Bekannten suche? Inwiefern habe ich Verantwortung für die Daten von Freunden und Bekannten?



Nein, das ist erlaubt. Das Problem dabei ist, dass Firmen wie Facebook diese Daten gern auch für sich nutzen würden. Ob Sie selbst damit ein Problem haben, spielt dabei gar nicht einmal so sehr eine Rolle; ihnen selbst ist der Datenstrip erlaubt, denn die «informationelle Selbstbestimmung», das Kernanliegen des Datenschutzes, geht in alle Richtungen. Aber können Sie auch für Ihre Freunde und Bekannten entscheiden? Nein, und daher darf Facebook mit deren Daten nichts anderes tun, als was Sie dürfen. Entscheidend ist daher, ob Sie Facebook vertrauen können, dass sie sich daran halten. Rechtlich sind Sie mindestens mitverantwortlich, wenn Unfug geschieht.

«Ihnen selbst ist der Datenstrip erlaubt, denn die ‹informationelle Selbstbestimmung› geht in alle Richtungen.»

Ich glaube aber, das sind Dinge, die vor allem die Aufsichtsbehörden kontrollieren sollten, nicht Verbraucher wie Sie. Denn die Behörden können das viel besser. Sie selbst sollten auf Ihren Bauch hören: Wie fänden Sie es, wenn ein anderer das mit Daten über Sie macht?



Dank

Die in dieser Broschüre enthaltenen Texte wurden erstmals im Avenir-Suisse-Adventskalender 2014 «Über die Privatsphäre, den Datenschutz und das Netz» publiziert (www.avenir-suisse.ch/42160).
Bei der Erarbeitung der Inhalte durften wir auf die Unterstützung von zahlreichen Experten in den Bereichen IT, Datenschutz und Datensicherheit zählen. Ihnen allen gilt unser herzlicher Dank:
Bruno Baeriswyl (Datenschutzbeauftragter des Kantons Zürich), Prodosh Banerjee (CEO Safe Swiss Cloud), Raphael Bienz (CEO Blueglass Interactive), Volker Birk (Mitglied des Chaos Computer Clubs Schweiz), Markus Brönnimann (IT-Experte beim Datenschutzbeauftragten des Kantons Basel Stadt), Nicolas Gisin (Professor Universität Genf), Oliver Hirschi (Dozent für Wirtschaftsinformatik, Hochschule Luzern), Jovan Kurbalija (Direktor der Geneva Internet Platform und der Diplofoundation), Elisabeth Floh Müller (Alpine Rettung Schweiz), Lars Raffelt (Leiter IT-Servicezentrum der Bayerischen Staatlichen Museen und Sammlungen), David Rosenthal (Co-Leiter der IT-Rechtsberatung von Homburger), Hanspeter Thür (Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter)

Für den Inhalt ist allein Avenir Suisse verantwortlich.

Publikationen

3. Auflage

2. Auflage

Verantwortlich für diese Ausgabe Gerhard Schwarz, Verena Parzer Epp und Simone Hofer Frei, Avenir Suisse, Zürich Mitarbeitende Tibère Adler, Alois Bischofberger, Alexandra Christen, Jérôme Cosandey, Simon Hurst, Michael Mandl, Urs Meister, Jörg Naumann, Nicole Pomezny, Marco Salvi, Patrik Schellenbauer, Rudolf Walser, Claudia Wirz, Dominique Zaugg Redaktion Rotbuchstrasse 46, 8037 Zürich Telefon 044 445 90 00 E-Mail redaktion@avenir-suisse.ch Gestaltung arnold.kircher-burkhardt.ch, atelier4m.ch Zeichnungen Sergo Mikirtumov, s.mikirtumov@gmail.com Druckauflage 7200 Exemplare Druck Neidhart + Schön AG, www.nsgroup.ch Download Nachdruck, auch auszugsweise, mit Quellenangabe («avenir spezial») gestattet; abrufbar als PDF auf www.avenir-suisse.ch.