fluter.

Herbst 2018 / Nr. 68

Was gibst du preis?

Thema **Daten**

Magazin der Bundeszentrale für politische Bildung

Interessant, was man von dir so im Netz findet

Das Internet vergisst nicht? Im Datenschutz-Dossier erfährst du, welche Rechte du hast. Und ein Film zeigt, wie die Europäische Datenschutz-Grundverordnung entstand:
www.bpb.de/dossier/datenschutz

bpb: Bundeszentrale für politische Bildung

Editorial

Bücher, Schallplatten, Zeitschriften und Fotoalben: alles Daten. Im Verlauf des Heftes bekommt ihr noch genug Digitales zu Gesicht, da tut so ein vollgestopftes Regal doch mal ganz gut als optische Abwechslung

→ Alles und jedes kann zu Daten werden, alle Daten können zu Geld gemacht werden, sich gegen dich wenden oder dir nutzen. Mit dem digitalen Kapitalismus werden auch Bereiche des gesellschaftlichen und privaten Lebens zu Datenkapital, die bisher noch nicht marktförmig gestaltet waren. Der Fortschritt ist im Alltag greifbar und die Dynamik ungebrochen. Das Versprechen ist riesig – ein allwissendes Paradies, wo auf den Wunsch unmittelbar die Erfüllung folgt, ja, Wünsche steuerbar werden, ein Fließen der Grenzen des Machbaren – und wir alle mittendrin, angeschlossen und in Echtzeit vernetzt.

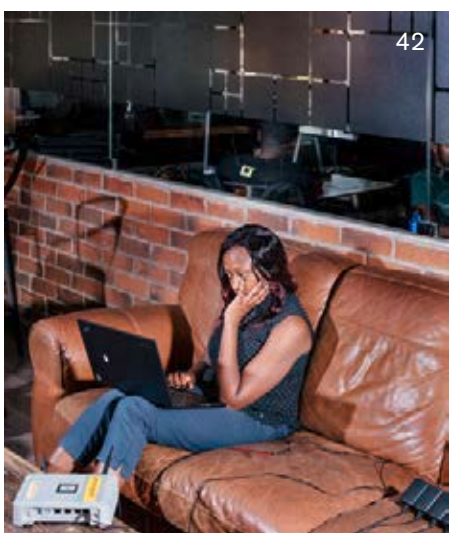
Diese schöne neue Welt hat allerdings einige Untiefen. Die digitale Dynamik ist heute vor allem eine kommerzielle und eine der Sicherheitsdienste. Hier werden weltweit Milliarden investiert, neue Ansätze zuerst massenhaft erprobt. Die Datenmodelle, die Algorithmen, die diese privaten und staatlichen Akteure in Gang setzen, entsprechen den vorgegebenen Zwecken und sind damit notwendigerweise begrenzt. Sie blenden das Unnütze, Störende aus. Die Herrschaft über diese Daten ist alles andere als gemeinschaftlich. Nicht nur die sogenannten sozialen Medien sind als Plattformen autoritär organisiert. Einige wenige entscheiden in den Machtzentralen der Konzerne und Geheimdienste, womit es Millionen und Milliarden User zu tun bekommen. Widerspruch ist mühselig und oft folgenlos. Und wehe, du fällst durch das Raster oder wirst verdächtig. Da helfen dann auch Taktiken des privaten Datenschutzes kaum weiter.

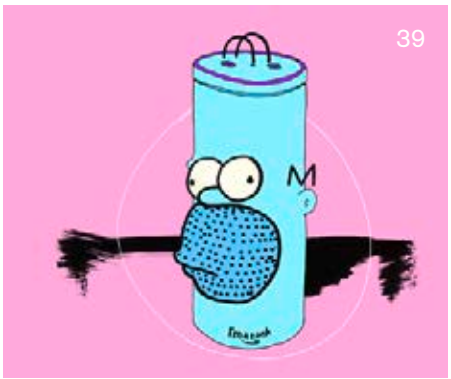
Der Glaube an die Verlässlichkeit und Neutralität der Algorithmen ist allerdings noch weit verbreitet, er kann zur Falle werden. Die Kehrseite der Konsumentenseligkeit ist die Abgabe von Verantwortung, die Einschränkung der persönlichen Freiheit und eine kulturelle Verengung, letztlich ein neuer Untertanengeist als Schicksalsglaube an den von oben kommenden digitalen Fortschritt. Wohin die autoritäre Welt der Daten führen kann, zeigen Versuche der totalen Kontrolle in China. Sie sind viel weniger exotisch, als wir uns vormachen – in den medienkulturellen und populistischen Trends ist das auch im Westen schon angelegt.

Dagegen gilt es, die freie gesellschaftliche Souveränität über die Daten neu zu erfinden, zeitgemäße Formen der Anwendungen und der Regulierungen zu erstreiten. Erste Erfahrungen gibt es bereits, zum Beispiel in einigen Städten und bei verschiedenen Initiativen auch zivilgesellschaftlicher Akteure. Es gibt aber nach wie vor weite Bereiche der Wirklichkeit und der kollektiven Intelligenz, die sich in den vorherrschenden Anwendungen nicht wiederfinden.

Das Leben als Ware oder in Dienstleistungsbeziehungen ist für sich armselig im Verhältnis zu den weiteren Möglichkeiten. Wenn wir wirklich mehr wollen, müssen wir das Recht auf informationelle Selbstbestimmung neu erfinden und gestalten. Wird es eine Demokratisierung der Daten geben? Wer können die Datensouveräne sein? Wie sähen die Daten einer Gesellschaft aus, in der das gute Leben der Vielen mit der gerechten Verteilung, dem nachhaltigen Gebrauch und der demokratischen Kontrolle der Ressourcen einhergeht? Thorsten Schilling

Inhalt





Die großen Internetplattformen haben die Welt ganz schön verändert. Milliarden Menschen teilen ihre intimsten Momente mit Facebook, Snapchat oder Instagram. Google und Apple analysieren uns durch unser Telefon. Mikrojobs ersetzen Festanstellungen. Willkommen im digitalen Kapitalismus. Wie der funktioniert und welche Gefahren drohen, erklärt der IT-Experte Timo Daum

Interview:
Fabian Dietrich

Unter Strom


SCHLÜSSEL
Kommt zum 1. Mai '87!
Birleşelim
Mücadelevi
Yükseltelim
Volkszählung
'87
na bitte

fluter: Im Internet gibt es heute viele Dinge umsonst oder für sehr wenig Geld. Ich kriege kostenlos Nachrichten und Informationen. Ich kann mit einer monatlichen Flatrate Filme schauen oder fast die gesamte Musik der Welt hören und zahle dafür weniger als für ein einzelnes Album im MP3-Format. Wie kann das eigentlich sein?

Timo Daum: Die digitale Ökonomie verändert unser Leben und unsere Gesellschaft gerade radikal. Auf den ersten Blick ist es wirklich so eine Art Schlaraffenland. Informationen, dazu zähle ich jetzt auch mal Musik und Filme, sind frei verfügbar oder kosten sehr wenig Geld. Technisch gesehen funktioniert alles sehr gut, und auch kulturell ist das eine riesige Errungenschaft. Bloß: Wie können Unternehmen Geld verdienen? Wir haben es beim digitalen Kapitalismus mit einer Neudefinition von Arbeitsprozessen und Ausbeutung zu tun. Eine Plattform wie Facebook hat Milliarden Nutzerinnen und Nutzer, diese sind einerseits so etwas wie Kunden, gleichzeitig aber auch unbezahlte Arbeiter. Denn die User sind es ja, die die Daten liefern, mit denen die Plattform am Ende Geld verdient.

„Durch Plattformen wie Uber, Foodora oder Amazon entsteht eine neue Mikroarbeiterklasse“

Als Kunde bekomme ich gar nicht mit, was im Maschinenraum passiert. Welche Rolle spielen die Algorithmen im Hintergrund?

Ich vergleiche Algorithmen mit den Maschinen in einer klassischen Fabrik, wie Henry Ford sie erfand. Algorithmen erzeugen aus dem Rohstoff Daten Informationen, die sich im digitalen Kapitalismus verwerten lassen. Das machen Googles Such-Algorithmen, die Matching-Algorithmen eines Fahrvermittlungsdienstes wie Uber oder auch Partnervermittlungen. Das ist der Kernprozess des digitalen Kapitalismus.

Sind Algorithmen denn neutral?

Es ist offensichtlich, dass sie nicht neutral sind. Natürlich dienen all diese Algorithmen und Künstliche-Intelligenz-Anwendungen, die da in unser Haus eindringen, den Konzernen. Sie helfen ihnen, aus Daten verwertbare Informationen zu generieren. Soziale Netzwerke etwa sind so designt, dass wir das Gefühl kriegen: Ich muss die ganze Zeit aktiv sein. Ein Strom von Daten soll generiert werden, was ich sage, ist egal. Dem wird alles andere untergeordnet.

In China wird gerade ein Sozialpunktesystem eingeführt, bei dem die Menschen anhand ihrer Daten bewertet und in gute und schlechte Bürger eingeteilt werden. Wächst mit Big Data die Möglichkeit, Menschen zu kontrollieren?

Selbstverständlich. Interessant ist jedoch zweierlei: Wer bekommt diese Daten, und wer bestimmt, was mit ihnen geschieht und zu welchem Zweck? Was tun wir, wenn eine App uns fragt: Dürfen wir auf deine Kontakte oder deinen aktuellen Standort zugreifen, um dir einen besseren Service, eine bessere User-Experience zu bieten? Nach kurzem Zögern antworten wir meist mit „Ja“. Wir wissen also sehr wohl, dass wir ab sofort getrackt werden, Bewegungsprofile erstellt werden, unsere Sozialkontakte verwertbare Informationen für Werbetreibende oder eben für Regierungsstellen liefern, die ein soziales Scoring veranstalten. Wir wissen es, und wir tun es trotzdem. Weil es so bequem ist. Ich denke, es gibt kein Zurück in die Zeiten vor Big Data und umfassender Echtzeitüberwachung. Die Frage ist vielmehr, ob wir diesen Datenschatz, der zu unserer wichtigsten Ressource überhaupt wird, weiterhin Geheimdiensten und privaten Firmen überlassen wollen. Oder ob wir eine Datenrevolution veranstalten, durch die wir die Souveränität über diese zurückgewinnen, aber nicht als einzelne Individuen im Sinne von „Meine Daten gehören mir“, sondern als Gemeinschaft: „Unsere Daten gehören allen“.

Immer wieder hört man, dass Daten das „Öl“ des 21. Jahrhunderts sind. Mittlerweile gilt das nicht nur für Geschäfte im Internet. Die Hotelbranche, die Autobranche, überall scheint es nur noch um Daten zu gehen.

Ich glaube, der digitale Kapitalismus ist in den letzten zehn Jahren gereift. Jetzt erleben wir so etwas wie eine neue Stufe. Die mächtigsten Unternehmen haben sich in verschiedenen Bereichen etabliert und dringen in neue Gebiete vor. Beim Verkehr in den Städten wird das Auto als Produkt zum Beispiel langfristig an Bedeutung verlieren. Wichtiger werden hingegen Informationen, die in Echtzeit darüber Auskunft geben, wer unterwegs ist und wohin er will. Im Energiesektor wird die große Fabrik, in der Strom produziert wird, zum Auslaufmodell. Stattdessen speisen viele dezentrale Einheiten erneuerbare Energie ein. Die entscheidende Frage wird sein, wer in Zukunft den Stromhandel mit Daten und Algorithmen managt. Oder nehmen wir den Gesundheitsbereich: Die Firma IBM hat gerade in den USA Analysefirmen gekauft, um an Daten von Patienten zu kommen. IBM will seine künstliche Intelligenz, Watson, in diesem Bereich trainieren und Diagnosewerkzeuge entwickeln.

Viele Branchen haben es durch die Konkurrenz der großen Plattformen zunehmend schwer, zu überleben. Einzelhandel, Journalismus, Taxigewerbe, Hotels und viele andere Branchen werden durch die neuen Geschäftsmodelle herausgefordert und bedroht. Wie verändert die Digitalisie-

Times are changing: Die Einstellung zu Daten hat sich ziemlich gewandelt, seitdem in Deutschland 1987 die Volkszählung stattfand, gegen die viele Menschen protestierten. Sie hatten Angst, vom Staat ausspioniert zu werden. Heute geben viele Menschen selbst Privates freiwillig preis

Durch Geschäftsmodelle im Internet hat sich auch die Arbeitswelt gewandelt. Verkäufer in echten Läden verschwinden, stattdessen sorgen bei großen Onlineversandhändlern wie Amazon schlecht bezahlte Arbeiter dafür, dass die Pakete gepackt und versendet werden

rung denn unsere Arbeitswelt?

Gerade im Wirtschaftswunderland Deutschland waren die Arbeitsverhältnisse lange Zeit vergleichsweise idyllisch. Es gab lineare Arbeitsbiografien, Festanstellung, Sozialversicherung, Teilhabe am Wohlstand. In diese Welt sticht der digitale Kapitalismus rein und macht vieles kaputt. Es wird deutlich, dass das eine relativ kurze historische Phase war. Durch Plattformen wie Uber, Foodora oder Amazon entsteht eine neue, fragmentierte Mikroarbeiterklasse, die bei null anfangen muss, was Arbeitnehmerrechte und soziale Absicherung angeht.

„Die Festanstellung wird dahinschmelzen wie ein Gletscher in der Sonne“

Schafft die digitale Ökonomie mehr Ungleichheit?

Ja, die durch Lohnarbeit finanzierten Sozialsysteme geraten definitiv in die Krise. Viele Manager aus dem Silicon Valley glauben, dass sie in Zukunft immer weniger Menschen beschäftigen werden. Genau deswegen finden sie auch die Idee eines bedingungslosen Grundeinkommens so gut. Der Internetvordenker Jaron Lanier prognostizierte schon vor vielen Jahren, dass die Mittelklasse aussterben wird, weil die neuen Internetfirmen viel weniger Arbeitsplätze anbieten als ihre Vorgänger. Der digitale Kapitalismus erfordert neue sozialpolitische Diskussionen. Das Modell Festanstellung wird meiner Meinung nach dahinschmelzen wie die Gletscher in der Sonne durch die Klimaerwärmung.

Da wünscht man sich ja fast, das Internet wäre nie erfunden worden!

Nicht, dass wir uns falsch verstehen: Ich will nicht sagen, der digitale Kapitalismus ist böse, und wir müssen jetzt zum alten Kapitalismus zurück. Früher war auch nicht alles besser. Der alte Kapitalismus hat zum Beispiel eine unverantwortliche Wachstumsideologie propagiert. Er hat Raubbau an der Natur betrieben und ärmere Länder ausgebeutet, um Wohlstand zu generieren. Die alte Arbeitswelt ist durch Gender-Ungerechtigkeit, überkommene Rollenmodelle und Arbeitsfetischismus geprägt. Ich bin froh, dass das gerade abgewickelt wird.

Heute gibt es in der Sharing Economy durchaus Ansätze, die besser sind. Zum Beispiel, wenn ein Geschäftsmodell nicht mehr darauf setzt, noch mehr Autos zu produzieren, die dann die meiste Zeit ungenutzt in den Städten stehen, sondern Ideen entwickelt, wie man die bereits existierenden Autos besser auslasten kann.

Die Staaten tun sich bislang schwer, das Geschäft mit den Daten zu regulieren. Es gibt zwar die neue Europäische Datenschutzgrundverordnung, die die EU-Datenschutzrichtlinie ersetzt, aber ihre Wirkung ist noch ungewiss. Kann denn der einzelne Nutzer etwas tun?

Es gibt darauf zwei typische Reaktionen. Die einen sagen: Die haben doch eh meine Daten, jetzt ist es auch schon egal. Die anderen verweigern sich. Sie melden sich bei Facebook ab und treten in den Widerstand. Ich halte beides für falsch. Ich würde dafür plädieren, an den Debatten teilzunehmen. Wir müssen verstehen, wie die Sachen funktionieren, um Alternativen zu entwickeln. Ich denke, es braucht eine neue Bewegung, die sagt: Algorithmen ja, Daten ja, Plattformen ja, aber in öffentlicher Hand, unter öffentlicher Kontrolle.

Wie sieht denn eine öffentliche Kontrolle der Daten konkret aus? Ein soziales Netzwerk als Genossenschaft?

Bisher scheiterten die meisten Alternativmodelle zu kommerziellen sozialen Netzwerken, oder sie dümpeln in der Bedeutungslosigkeit herum. Was ich dagegen inspirierend finde, sind Städte und Kommunen, die erkannt haben, dass Daten immer wichtiger werden. In Barcelona werden Daten, die für die Stadtbewohner wichtig sind, in öffentlicher Hand behalten und nicht kommerziellen Anbietern überlassen. Die Stadt hat zum Beispiel ein kommunales Fahrradverleihsystem. Alle Daten, die daraus generiert werden, werden für Stadt- und Verkehrsplanung benutzt. In Berlin gibt es dagegen viele verschiedene Privatunternehmen, die Leihräder anbieten. Das führt zu Chaos und dazu, dass die Stadtverwaltung überhaupt keine Ahnung von ihrem Verkehr hat. Mag sein, dass das erst mal nach einem kleinen Anfang klingt. Aber ich glaube, dass die Städte in Zukunft mehr Bedeutung bekommen werden und die Macht der Nationalstaaten schrumpft.

In Ihrem Buch stellen Sie sich die Ausgangsfrage, was Karl Marx wohl vom digitalen Kapitalismus halten würde. Was haben Sie herausgefunden? Wäre er ein Gegner oder ein Fan?

Beides. Marx liebte Technologie, wusste aber auch, dass sie zur Ausbeutung der Arbeiter genutzt wurde. Er hat den Kapitalismus für seinen technologischen Fortschritt bewundert und war begeistert davon, wie er alte Ordnungen zerstörte und die Pfaffen und Könige davonjagte. Das wäre heute auch noch so. Marx fände es toll, dass wir uns so leicht weltweit vernetzen und Wissen erwerben können. Er würde sich aber auch die Augen reiben und fragen: Es sind 150 Jahre vergangen, und ihr habt es immer noch nicht geschafft, dieses System durch etwas Rationaleres zu ersetzen? Nachdem er ein Selfie gemacht und verstanden hätte, wie Google funktioniert, wäre er wahrscheinlich in die British Library zurückgekehrt, hätte den vierten Band des „Kapitals“ angefangen und nebenbei versucht, Clickworker zu organisieren und sie zur Revolution aufzurufen. ←

Timo Daum ist Hochschullehrer für die Bereiche IT, Online und digitale Wirtschaft. Von ihm erschien 2017 das Buch „Das Kapital sind wir: Zur Kritik der digitalen Ökonomie“ (Nautilus Flugschrift, 18 Euro)

Schlechte Nachrichten: Deine Daten sind überall

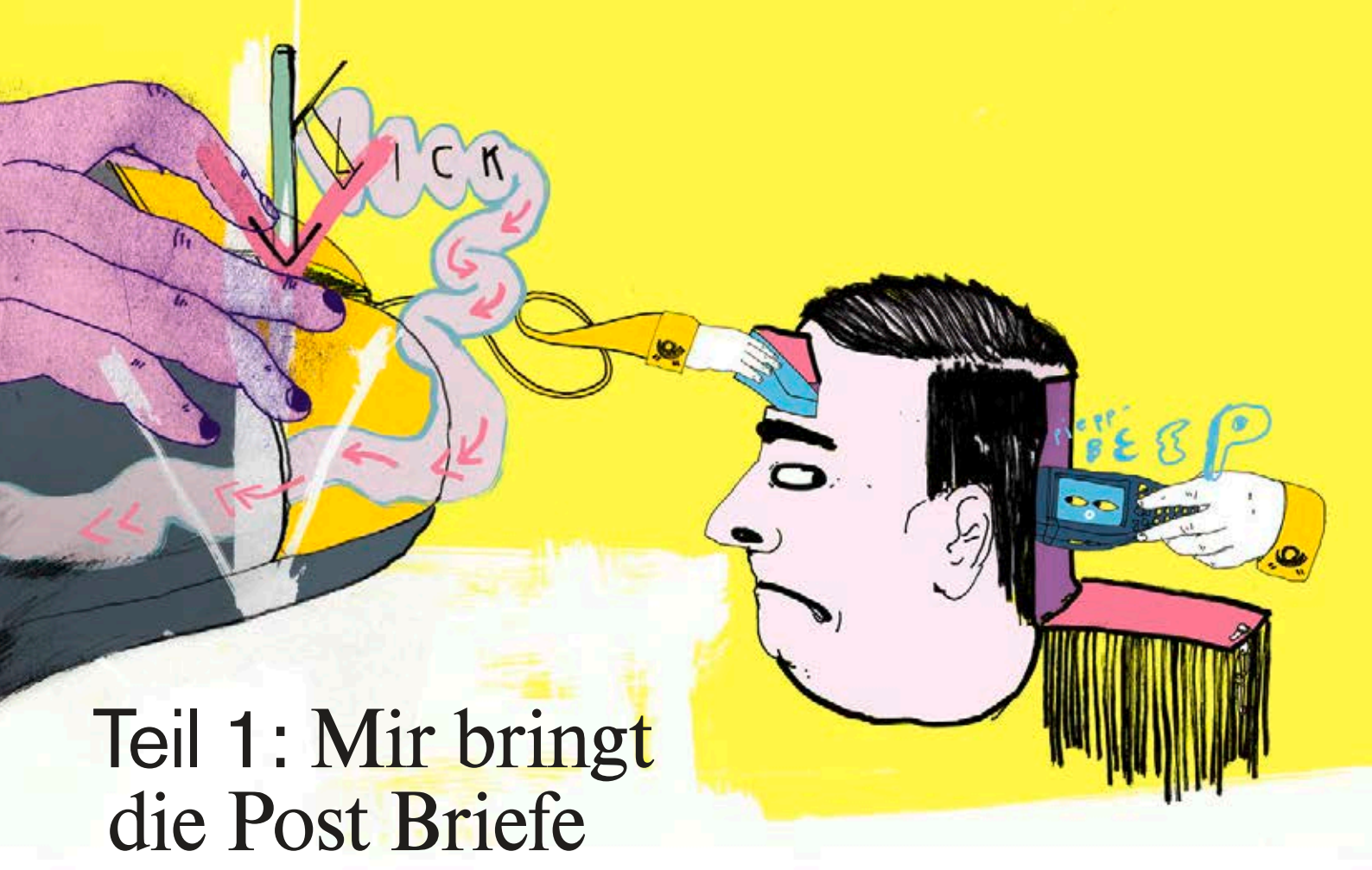
Bilder posten, Filme streamen, Musik hören, Nachrichten verschicken oder Adressen suchen: Unser Alltag wird auch durch die digitalen Möglichkeiten bestimmt. Vieles macht Spaß, manches nervt aber auch, zum Beispiel die ganze Werbung oder die Pushnachrichten, die ständig auf dem Smartphone landen. Das sind aber noch harmlose Folgen unseres ständigen Datenaustauschs. Heftiger wird es, wenn es um Zensur, Spionage oder kriminelle Aspekte geht. Auf den nächsten Seiten schauen wir uns erst mal die dunkleren Seiten unseres Themas an.

Mich für nichts

Von Bernd Kramer

Von früh bis spät hinterlassen wir einen Haufen Daten. Unser Autor will herausfinden, wer ihm alles auf der Spur ist (es sind viele)

fluter Nr. 68, Thema: Daten



Teil 1: Mir bringt die Post Briefe – und anderen meine Adresse

Elf Uhr morgens, im Treppenhaus hallt das Klappern der Briefkastendeckel. Lange dachte ich, die Post benutzt meine Anschrift nur für einen einzigen Zweck: um mir Briefe zuzustellen. Eine naive Vorstellung.

Im Frühjahr wurde bekannt, dass eine Post-Tochter im vergangenen Jahr während des Bundestagswahlkampfs Daten an Parteien weiterverkauft hat, in anonymisierter Form zwar, aber durchaus kleinteilig. Für Gebäude mit mindestens sechs Haushalten gab sie eine Wahrscheinlichkeit an, dass die Parteien hier Sympathisanten finden könnten – was zum Beispiel die CDU für ihren Haustürwahlkampf nutzte und gezielt dort klingelte.

Adress- und Datenhandel ist ein großes Geschäft, rund 610 Millionen Euro wurden damit im Jahr 2014 in Deutschland umgesetzt, heißt es in einer Studie für das Bundesministerium der Justiz und für Verbraucherschutz. Und die Post wirbt damit, einen besonders großen Datenschatz zu besitzen: Mit 46 Millionen Adressen decke sie „nahezu den gesamten Markt an Privathaushalten ab“, heißt es auf der Homepage. Aber womit handelt die Post eigentlich genau?

Ich richte mir bei Deutsche Post Direkt ein Benutzerkonto ein – als Unternehmer, der online Kundenadressen kaufen will. Und ich staune, was sich alles auswählen lässt. Ich kann Haustierbesitzer herausfiltern und die Leserinnen von Frauenzeitschriften, Menschen mit und ohne Doktortitel. Ich kann auswählen, ob ich lieber eine Adresse aus einer Straße mit vielen oder wenigen Autobesitzern will. Klicke ich in der Auswahlliste auf das Fragezeichensymbol, erklärt mir die Post, woher sie ihre Informationen bekommt. Das Alter der Bewohner zum Beispiel „wird über die Vornamensanalyse der Person ermittelt“ – eine Julia ist wahrscheinlich jünger als eine Roswitha. Ob an einer Anschrift die Bewohner häufig wechseln, lässt sich wiederum aus den Nachsendeaufträgen schließen. Rund 150 „Zielgruppenmerkmale“ bietet die Post zur Auswahl an, 1.000 Adressen gibt es bereits zum Preis von 84 Euro.

Es klingelt an der Tür. Der Paketbote bittet mich, eine Sendung für den Nachbarn anzunehmen – mal wieder. Ich arbeite oft zu Hause, deswegen werden die Amazon-Bestellungen aus dem ganzen Haus regelmäßig in meinem Wohnungsflur zwischengeparkt. Der Bote fragt mich nach meinem Namen, hält mir das Gerät hin, damit ich auf dem Display gegenzeichne. Aber diesmal zögere ich kurz. Wer erfährt eigentlich alles, dass ich ständig Pakete für andere annehme? Die Nachbarn, klar. Und sonst?

Ich erkundige mich beim Bundesverband Paket und Expresslogistik. Mein Name werde in der Sendungsverfolgung dokumentiert, erklärt mir eine Verbandssprecherin. Die Paketunternehmen würden die Informationen aber nicht auswerten und bald nach der Zustellung wieder löschen: Als Dauer-Pakete-für-andere-Annehmer würde ich also nicht gespeichert. Allerdings haben auch die Versender Zugriff auf die Informationen. Theoretisch also könnte auch Amazon meine regelmäßige Mithilfe bei der Zustellung seiner Lieferungen mit der Zeit auffallen. Vielleicht mag man mir beim nächsten Einkauf für meine Hilfe ja mal einen Rabatt geben?

Teil 2: Was?! Mein Passwort steht im Internet, und alle können es sehen?

Pling! In meinem E-Mail-Eingang findet sich eine neue Nachricht, Betreff: „Ihr Geld steht bereit“. Ich bin genervt. Woher kommen die ganzen Spam-Nachrichten?

Auf der Internetseite des Hasso-Plattner-Instituts für Digital Engineering der Uni Potsdam kann ich überprüfen, ob meine E-Mail-Adresse in einem der Datensätze auftaucht, mit denen Kriminelle handeln. Vielleicht finde ich hier die Antwort auf die Flut an Müllnachrichten. Ich gebe meine E-Mail-Adresse ein. Und pling, schon finde ich die Auswertung des Hasso-Plattner-Instituts in meinem Postfach: Meine Adresse sei „in mindestens einer gestohlenen und unrechtmäßig veröffentlichten Identitätsdatenbank“ enthalten, lese ich da. Außerdem: mein Passwort! Gleich in fünf Datenbanken! Ich bin erschrocken.

Ich rufe David Jaeger an, der am Hasso-Plattner-Institut promoviert und den E-Mail-Check mitbetreut. So wie mir geht es offenbar sehr vielen. „Bis zu 40 Prozent derjenigen, die ihre Mail-Adresse mit unserem Tool überprüfen, tauchen in irgendeiner dieser Datenbanken auf“, sagt er. Und erklärt mir die Ökonomie des Onlinebetrugs, die über mehrere Etappen läuft. Es beginnt damit, dass Kriminelle über verschiedene Wege Daten sammeln – etwa über Spähsoftware, die man nichtsahnend auf seinen Rechner lädt, oder indem sie Onlinedienste wie das Karriereportal LinkedIn hacken und dort Nutzerkennwörter stehlen. In geschlossenen Foren bieten sie ihre Beute schließlich zum Kauf an. Die Käufer zielen vor allem auf die wenigen Personen, zu denen zum Beispiel auch Kreditkartennummern oder Bankverbindungen hinterlegt sind – auf die leichten und lukrativen Opfer sozusagen. „Am Anfang wird alles genutzt, was sich sehr unmittelbar zu Geld machen lässt“, sagt Jaeger. Ist das abgegrast, wird der Datensatz weiterverkauft, jetzt schon für weniger Geld. Die zweite Riege der kriminellen Käufer versucht zum Beispiel, mit Kombinationen aus Passwörtern und E-Mail-Adressen Amazon-Konten zu kapern und in fremdem Namen Waren zu bestellen – was oft klappt, weil viele Menschen immer dasselbe Passwort benutzen; mit einem bei LinkedIn gestohlenen Kennwort kann ein Betrüger sich oft auch in andere Konten einloggen. Irgendwann ist der Datensatz ausgepresst wie eine Zitrone, und irgendjemand am Ende der Kette stellt ihn frei ins Netz. Dann klappern die Spam-Bots ihn ab und verschicken massenhaft Angebote für Viagra oder dubiose Nahrungsergänzungsmittel, und dort finden ihn auch die Potsdamer Forscher. Bis dahin können aber Jahre vergehen. „Ihre E-Mail-Adresse kann also noch in diversen anderen Listen stehen, von denen wir bisher gar nichts wissen“, sagt Jaeger.

Einer der Datensätze, in denen laut dem Check des Hasso-Plattner-Instituts meine Mail-Adresse stehen soll, heißt „Exploit.In“, öffentlich geworden ist er 2016. Ich google ein bisschen. Und tatsächlich. In einem Reddit-Forum finde ich eine Dateikennung, mit der ich die Liste bei einem Filesharing-Dienst herunterladen kann. Eine halbe Stunde dauert es, dann habe ich einen Ordner auf meiner Festplatte, 24 Gigabyte groß, fast 687 Millionen E-Mail-Adressen samt Passwort, verteilt auf 111 Textdateien, in denen Nutzerinnen und Nutzer aufgelistet sind. In einer dieser Dateien finde ich in Zeile 6.444.965: mich. Meine E-Mail-Adresse – und ein Passwort, das ich vor Jahren einmal benutzt habe. Mit dem man sich vielleicht immer noch irgendwo einloggen könnte. Mir wird mulmig. Wann war ich zuletzt bei StudiVZ?

Teil 3: Mit wem stecken meine Apps unter einer Decke?

Den potenziell größten Spion trage ich ständig in der Hosentasche mit mir herum. Er verfügt über ein Mikrofon, das mich abhören, eine Kamera, die mich beobachten kann, Bewegungssensoren und GPS-Empfänger: mein Handy. Außerdem ist es voller Apps, mit denen ich meinen Alltag manage. Aber wem geben diese vielen kleinen Programme weiter, was sie dabei über mich erfahren?

Ich lade „Lumen Privacy Monitor“ herunter, eine Android-App, die Forscher der Universität Berkeley entwickelt haben. Sie soll aufdecken, mit wem die übrigen Apps auf meinem Handy still und unbemerkt im Hintergrund kommunizieren. Eine Art Superspitzel also, den ich auf die vielen anderen kleinen Spione auf meinem Smartphone ansetze.

Dass die Apps mit ihren jeweiligen Herstellern Kontakt halten, „Spotify“ mit Spotify und „Jodel“ mit Jodel, überrascht mich nicht. Aber „Lumen“ zeigt mir an, dass da noch viele andere sind, an die ständig Daten geschickt werden. Etwa an Google. Oder an Facebook. „Die Apps kommunizieren mit externen Dienstleistern, über die zum Beispiel Werbung eingespielt wird. Oder einfach nur der Teilen-Button von Facebook“, erklärt Christian Kreibich, ein deutscher Computerwissenschaftler in Berkeley, der „Lumen“ mitentwickelt hat. „Weil die verschiedenen Apps oft dieselben wenigen Dienstleister benutzen, können die ein sehr genaues Bild eines Nutzers bekommen und davon, was der mit seinem Gerät macht.“ Sie sind wahre Datensammelstellen, in denen viele Informationen über mich zusammenfließen.

Was genau, das kann mir auch Kreibich nicht sagen. Der Superspion „Lumen“ tappt im Dunkeln, weil die Kommunikation zwischen den Apps und den Diensten in der Regel verschlüsselt wird – was im Prinzip eine gute Sache ist. Manchmal entdeckt „Lumen“ aber doch, dass ziemlich sensible Daten abfließen: „WhatsApp“ zum Beispiel hat offenbar mehrere Male mein Gerätemodell an Google gesendet. Besonders mitteilungsfreudig war „Clean Master“, eine vorinstallierte App, mit der ich den Speicherplatz auf meinem Telefon aufräumen kann. Sie leitet neben dem Gerätemodell auch meine Zeitzone („Europe/Berlin“) an den Hersteller und andere Dienste weiter – und meine Android-ID, also die, über die ich eindeutig zu identifizieren bin. Für das, was die App eigentlich leisten soll, ist das völlig unerheblich. Kreibich bezeichnet sie daher als regelrechten Spitzel.

Ironischerweise ist auch „Lumen“ selbst ein äußerst neugieriger Späher – aber immerhin im Dienste der Wissenschaft. Was die App auf meinem Handy feststellt, übermittelt sie in einem Datensatz an die Forscher in Kalifornien. Mit den Informationen von Tausenden Handynutzern konnten Kreibich und seine Kollegen kürzlich in einer Studie feststellen, welche Apps besonders häufig Daten weiterleiten: Es sind kostenlose Handyspiele und Bildungs-Apps.

Teil 4: Warum ich im Supermarkt auch ohne Payback-Karte ausgeforscht werden kann

„Haben Sie eine Payback-Karte?“, fragt die Kassiererin. Es ist einer der wenigen Momente, in denen ich mich wie ein Mensch fühle, der den Datenschutz ernst nimmt. Wie ein Kunde, der sich bewusst verhüllt, statt sich gläsern zu machen. „Nein“, sage ich mit voller Überzeugung. „Natürlich nicht.“

Ich weiß ja, was der Handel mit Rabattkarten bezweckt: Er will mich ausforschen. Die amerikanische Supermarktkette Target fand mithilfe solcher Kundenkartendaten zum Beispiel heraus, wie man schon ziemlich früh schwangere Frauen identifiziert: Ab einem gewissen Zeitpunkt neigen sie unter anderem dazu, parfümfreie Körperpflegeprodukte zu kaufen. Je früher die Händler werdende Mütter erkennen, desto gezielter können sie sie umwerben. Das führte bereits zu kuriosen Situationen: Eines Tages kam ein Vater empört in den Laden, weil die Supermarktkette seiner Tochter Gutscheine für Babykleidung geschickt hatte. Sie gehe doch noch zur Schule, schimpfte der Vater. Target wusste bereits von der Schwangerschaft, bevor die junge Frau es ihrer Familie sagte.

Auch die Deutschen helfen dem Handel sehr bereitwillig beim Datensammeln. Payback, der größte Rabattkartenanbieter, hat nach eigenen Angaben hierzulande 30 Millionen aktive Nutzerinnen und Nutzer. Aber sind die anderen, die sich nicht von ein paar Prämien locken lassen, wirklich so gut getarnt?

Die Händler mit Ladenlokal lassen sich inzwischen einiges einfallen, um ihre Kunden so zu durchleuchten wie die Konkurrenten im Internet. Die Supermarktkette Real erfasste zum Beispiel eine Zeit lang die Gesichter der Kunden an der Kasse, wenn sie auf Werbebildschirme schauten. So lässt sich personalisierte Werbung ausspielen – wie im Internet. Erst nach öffentlichem Protest wurde das Projekt eingestellt, in einigen Filialen der Deutschen Post ist es weiterhin aktiv.

Eine besonders verbreitete Methode macht sich zunutze, dass viele Menschen die WLAN-Funktion ihres Handys nicht ausschalten, wenn sie den Laden betreten. Ein Smartphone sucht in der Regel automatisch nach Netzen in der Nähe und schickt dem WLAN-Sender dabei eine persönliche Identifikationsnummer des Gerätes, die sogenannte MAC-Adresse. Aus der Signalstärke können die WLAN-Sender in den Läden wiederum ermitteln, wo der Kunde sich gerade befindet: Bleibt er besonders lange an der Wursttheke stehen? Traut er sich nur dann an das Regal mit den Kondomen, wenn gerade keine anderen Kunden in der Nähe sind? Oder greift er ganz schambefreit zu? Und wie oft kommt er überhaupt in den Laden? Jeden Tag? Oder nur einmal in der Woche zum Großeinkauf?

Das EHI Retail Institute aus Köln, eine Forschungseinrichtung des Handels, hat kürzlich 44 Handelsketten befragt. Zehn gaben dabei an, die Laufwege der Kunden bereits zu erfassen, 16 planen es für die Zukunft. Das Bayerische Landesamt für Datenschutzaufsicht befürchtet, dass Funksignale des Handys auch mit anderen Informationen verknüpft werden können, etwa mit Angaben zur EC-Kartenzahlung. Dann wüssten die Händler ziemlich schnell, welches Bewegungsprofil zu welchem Menschen gehört, und statt einer MAC-Adresse, die zweimal in der Woche abends zwischen den Regalen herumirrt, sähen sie dann plötzlich: mich. Auch ganz ohne Payback-Karte.

Bei meinem nächsten Ladenbesuch achte ich darauf, welche WLAN-Netze mein Handy in der Nähe findet. Auch mein Supermarkt taucht in der Liste auf. Am Abend schleppe ich meine Einkäufe nach Hause und schalte zur Erholung Netflix ein. Der Streamingdienst kennt meine Vorlieben schon sehr genau – und schlägt mir „Black Mirror“ vor, eine Serie, die oft von den Überwachungsmöglichkeiten der nahen Zukunft erzählt.

Ich nehme mir vor: Von nun an stelle ich das Smartphone öfter aus, sobald ich aus dem Haus gehe. ←

Lösch mich

Was du über den gesetzlichen Schutz deiner Daten wissen solltest

→ Ausgerechnet an seinem 30. Geburtstag wird Josef verhaftet, ohne dass er weiß, warum. Er darf zwar noch zur Arbeit gehen, aber der Prozess gegen ihn schreitet unaufhaltsam voran. Am Ende wird er von zwei Männern abgeführt und umgebracht, ohne jemals erfahren zu haben, warum.

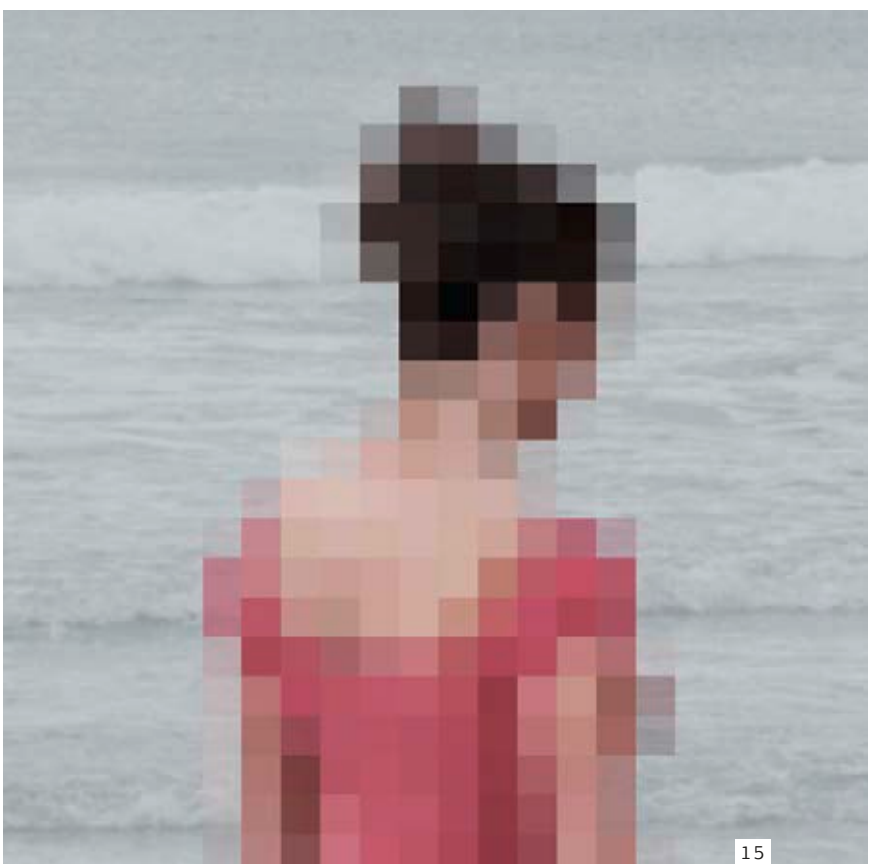
Dieses schreckliche Szenario hat Franz Kafka in seinem Buch „Der Prozess“ beschrieben und damit eine weitverbreitete Angst in der Gesellschaft thematisiert: dass nämlich der Staat viele Informationen über seine Bürger sammelt – und sie gegen sie verwendet. Tatsächlich gehört es zum Wesen autoritärer Regime, die Menschen auszuspähen und umfangreiche Akten über sie anzulegen.

Andererseits muss der Staat Daten über die Bürger erheben, um zu funktionieren. Ohne zu wissen, wie viele Menschen unter welchen Lebensumständen im Land leben, lässt sich schlecht Politik machen. Auch die Polizei ist auf manche persönliche Information angewiesen, um die Sicherheit zu gewährleisten. Der Datenschutz muss also zwischen dem Anspruch der Bürger auf Privatsphäre und dem Wunsch der Behörden nach statistischen Kenntnissen vermitteln.

Die ersten weltweiten Debatten über Datenschutz gab es in den 1960er-Jahren, als klar wurde, dass die neue Computertechnologie das Sammeln von Daten wesentlich erleichtern würde und in den USA die Einrichtung eines nationalen Datenzentrums erwogen wurde. Das erste Datenschutzgesetz der Welt wurde 1970 in Hessen erlassen, 1977 folgte der Bund mit dem Bundesdatenschutzgesetz (BDSG). In Bund und Ländern wurden Datenschutzbeauftragte ernannt, die sich um das Einhalten des gesetzlichen Datenschutzes kümmern.

Als besonders einschneidend in der Geschichte des Datenschutzes erwies sich die sogenannte Volkszählung 1987. Zuvor hatte es jahrelang Proteste dagegen gegeben, weil sich viele Bürger vom Staat ausspioniert fühlten. Im sogenannten Volkszählungsurteil schuf das Bundesverfassungsgericht bereits im Vorfeld 1983 das „Recht auf informationelle Selbstbestimmung“, durch das jeder Einzelne grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten bestimmen kann. Auf dieser Grundlage darf jeder Bürger bei der Polizei oder den Geheimdiensten nachfragen, was sie über ihn gespeichert haben. Dann wird auch geprüft, ob die Daten korrekt sind und überhaupt weiter gespeichert werden dürfen.

Das Recht auf informationelle Selbstbestimmung ist bis heute Kern des BDSG, das in diesem Jahr weitgehend durch die Europäische Datenschutzgrundverordnung (DSGVO) ersetzt wurde. Die ist auch eine Reaktion darauf, dass heute nicht nur Regierungen umfangreich Informationen horten, sondern große Internetkonzerne das Verkaufen von Nutzerdaten zum globalen Geschäft gemacht haben. Suchmaschinen, soziale Netzwerke, aber auch Shoppingseiten wie Amazon – sie alle müssen auf Anfrage mitteilen, welche Daten sie über dich gespeichert haben und an wen sie weitergeleitet werden. Daneben besteht ein Recht auf Löschung der Daten, falls die Speicherung nicht mehr notwendig ist. Das Problem: Unternehmen wie Facebook oder dessen Tochtergesellschaft Instagram drängen ihre Nutzer zur Zustimmung zu ihren Geschäftsbedingungen, die umstrittene Punkte wie etwa die Gesichtserkennung enthalten. Die Zustimmung ist freiwillig, aber wer sie nicht gibt, kann die Dienste nicht nutzen.



Als „Zwangszustimmung“ bezeichnet das der Datenschutz-Aktivist Max Schrems, der im vergangen Jahr die Non-Profit-Organisation NOYB (none of your business) gründete, die sich um die Durchsetzung von Datenschutzrechten kümmert. Im Mai, kurz nach Inkraftreten der DSGVO, reichte Schrems Beschwerde gegen Google, Facebook, Instagram und Whatsapp ein – wegen der Nichteinhaltung der europäischen Gesetze, die die Zwangszustimmungen durch das „Kopplungsverbot“ eigentlich ausschließen. Mit Klagen hat Schrems Erfahrung. Bekannt wurde er, weil er in einer Art David-gegen-Goliath-Feldzug jahrelang Facebook wegen der Nichtachtung von Datenschutzbestimmungen vor Gericht zerrte. Anders als Josef in Kafkas Roman weiß Max immerhin, wer seine Rechte verletzt. ← Von Oliver Gehrs

Mehr über Datenschutz findest du hier:
www.bpb.de/dossier/datenschutz

Du hast gerade das Gesetz gebrochen

Kameras in der Schule, Gesichtserkennung auf der Toilette: In keinem anderen Land der Welt werden so viele Daten gesammelt wie in China. Mit Big Data, Social Media und einem digitalen Punktesystem soll die totale Überwachung von 1,4 Milliarden Menschen gelingen

Von Michael Radunski

Kein Pardon für Verkehrssünder: In manchen Städten stehen riesige Bildschirme, auf denen Menschen, die bei Rot die Straße überquert haben, abgebildet werden - mit Namen

→ Der Himmelstempel in Peking gehört zu den bedeutendsten Sehenswürdigkeiten des alten Chinas, hier beteten die Kaiser der Ming- und der Qing-Dynastie für eine gute Ernte. Der Komplex, der jedes Jahr von Millionen Menschen besucht wird, ist aus dem frühen 15. Jahrhundert, aber auf der Besuchertoilette in der Parkanlage erwartet einen das moderne China: Das Toilettenpapier gibt es im kaiserlichen Himmelstempel nur noch via Gesichtserkennung. Direkt neben den Waschbecken hängt an der Wand ein kleiner dunkler Metallkasten mit eingebauter Kamera. Sekundenschnell wird das Gesicht gescannt und überprüft. Bei positiver Auswertung erhält man tatsächlich ein paar Blatt Papier. Kommt das Hightechgerät hingegen zu einem negativen Bescheid, etwa wenn man innerhalb von neun Minuten ein zweites Mal Toilettenpapier haben möchte, geht man leer aus.

Die Behörden versichern, dass es sich keineswegs um Schikane handle, sondern vielmehr um eine intelligente Form der Verbrechensbekämpfung. Die Kameras würden gegen Klopapierdiebe eingesetzt, von denen der Himmelstempel seit Jahren heimgesucht werde. So mancher Rentner habe auf seinen Beutezügen immerhin bis zu zehn Meter Papier auf einmal mitgenommen. Moderne Technik soll diesem Treiben ein Ende setzen.

Bis 2030 soll China eine Weltmacht in Sachen künstlicher Intelligenz (KI) werden, so der Plan des chinesischen Staatsrats. Auf diesem Weg ist man schon weit vorangeschritten. Im „Research Asia"-Zentrum von Microsoft werden Wissenschaftler und Ingenieure ausgebildet. Führende chinesische Unternehmen wie Baidu, Alibaba oder Tencent (Chinas Google, Amazon und Facebook) haben ihr Führungspersonal aus diesem Pool ausgewählt. Und sie alle investieren schier abenteuerliche Summen in Hardware, Forschung und Personal.

In Chinas Schulen ist KI längst angekommen. Eindrucksvoll kann man das im Gymnasium Nr. 11 der ostchinesischen Metropole Hangzhou erleben. Hier erfassen in den Klassenzimmern Kameras alle 30 Sekunden die Gesichtsausdrücke der einzelnen Schüler. Mithilfe einer Gesichtserkennungssoftware und des passenden Algorithmus wird festgestellt, ob die Schüler glücklich oder traurig, verärgert oder verängstigt, aufmerksam oder abgelenkt sind. Fällt die Aufmerksamkeit eines Schülers unter einen bestimmten Wert, kann der Lehrer entsprechend eingreifen. Der Leiter des Gymnasiums will das Projekt keinesfalls als Überwachungsmaßnahme der Schüler verstanden wissen. Es gehe vielmehr um die Lehrer, die durch die Informationen ihren Unterricht verbessern sollen. Die Schüler hätten sich ohnehin schon daran gewöhnt, meint der Direktor.

In China sind derzeit rund 800 Millionen Menschen online, sie nutzen Programme wie WeChat, Baidu, Renren oder Weibo – Chinas WhatsApp, Google, Facebook oder Twitter – und hinterlassen jedes Mal neue Daten, die alle gesammelt werden: von persönlichen Angaben, Vorlieben und Hobbys über Kauf- und Essgewohnheiten bis hin zu Angaben zu Freunden, Bekannten und Arbeitskollegen. Dazu kommt die Erfassung biometrischer Daten, zum Beispiel durch die sich rasch verbreitende Gesichtserkennung. Geht man in der Millionenstadt Hangzhou bei der Imbisskette Kentucky Fried Chicken essen, muss man zum Bezahlen weder seine Geldbörse noch sein Smartphone zücken. Nach der Bestellung scannt eine 3-D-Kamera das Gesicht des Kunden, der dann noch seine Handynummer eingibt. Der Vorgang dauert kaum mehr als ein paar Sekunden. Entwickelt wurde das Projekt „Smile to Pay" von Ant Financial, einer Tochter des chinesischen E-Commerce-Giganten Alibaba. Auch erste Supermärkte, die die Bezahlung nur mit dem Gesicht testen, erfreuen sich regen Zulaufs.

Während in Amerika und Europa viel über die Gefahren der neuen Technologie und den Datenschutz debattiert wird sowie über die Frage, was mit den Daten passieren soll, ist die Wahrung der Privatsphäre in China kaum ein Thema. Wenn doch, dann geht es in Gesetzentwürfen darum, einzelne Nutzer oder Unternehmen abzustrafen, die allzu freizügig mit fremden Daten umgehen, zum Beispiel im Onlinehandel. Der Staat selbst schränkt seine Behörden jedoch nicht ein. Forderungen nach mehr Datenschutz werden ignoriert, sie machen wohl in einem diktatorischen Staat, der auch in anderen Bereichen Menschenrechtsfragen hintanstellt, wenig Sinn.

Während es im Schnellimbiss um Bequemlichkeit geht, betont Chinas Polizei, dass das Leben eines jeden Einzelnen dank KI sicherer werde, wenn etwa mit ihrer Hilfe Kriminel-

le gefasst würden. Entsprechend setzt man die Technologie längst flächendeckend ein: Schätzungen zufolge werden Chinas Einwohner von mehr als 176 Millionen Kameras auf Schritt und Tritt beobachtet. Die Grundlage bildet die Gesichtsdatenbank des Staates. Denn jeder chinesische Personalausweis hat ein biometrisches Passbild, mit dem sich der jeweilige Bürger wiedererkennen lässt. Im Straßenverkehr werden so Verkehrssünder automatisiert zur Rechenschaft gezogen, in etlichen Städten werden Personen beim Über-Rot-Gehen innerhalb von Sekunden auf großen Bildschirmen mit Foto und nicht selten mit persönlichen Informationen wie dem Namen bloßgestellt. Selbst in großen Menschenmengen gelingt es Chinas Polizisten, mittels spezieller Datenbrillen gesuchte Personen ausfindig zu machen. Eine kleine Kamera an der Sonnenbrille der Polizisten erfasst die Gesichter der Passanten. Die verknüpften Systeme sollen jeden Chinesen, der in der zum Abgleich herangezogenen Datenbank mit Gesichtern gespeichert ist, in Sekundenschnelle erkennen können. So seien im Getümmel am Bahnhof von Zhengzhou während des chinesischen Neujahrsfestes sieben Flüchtige und 26 Personen mit gefälschten Ausweisen gefasst worden, lobt die regierungsnahe chinesische Zeitung „People's Daily".

Datenschützer und Menschenrechtsaktivisten stehen den Gesichtserkennungsbrillen kritisch gegenüber. „Einzelnen Polizisten Gesichtserkennungstechnik in Sonnenbrillen zugänglich zu machen könnte den chinesischen Überwachungsstaat noch allgegenwärtiger werden lassen", befürchtet William Nee, China-Experte bei Amnesty International.

Nees Befürchtung könnte schon bald Wirklichkeit werden, denn Chinas Regierung will alle Daten zusammenführen in einem allumfassenden „Social Credit System". Schon 2014 veröffentlichte die Regierung in Peking einen entsprechenden Plan zur Schaffung eines Systems, das die Gesellschaft in gute und schlechte Menschen unterteilt. Sämtliche Lebensbereiche sollen erfasst werden: Wer pünktlich seine Rechnungen bezahlt, Verkehrsregeln beachtet, regelmäßig spendet oder sich um seine Eltern kümmert, zum Beispiel indem er oder sie deren Arztrechnungen begleicht, erhält Pluspunkte auf seinem digitalen Verhaltenskonto. Nicht konformes Verhalten hingegen hat einen Punktabzug zur Folge – ein kleines Minus, wenn der Hund einen Haufen auf einen öffentlichen Rasen setzt; ein großes Minus, wenn man Kritik an der Politik des Landes äußert. All das wird Folgen haben: Menschen mit einem hohen Punktestand werden belohnt, können Zulassungen für Schulen, Beförderungen bei der Arbeit oder schneller einen Termin beim Arzt bekommen. Menschen im unteren Bereich des Verhaltenskontos müssen um ihre Zukunft bangen, denn nicht nur die Bürger können den Punktestand anschauen, auch Arbeitgeber, Banken, Vermieter und sogar Reiseanbieter sollen Einblick erhalten.

> In den Schulklassen hängen Kameras, die Alarm schlagen, wenn ein Schüler unaufmerksam ist

Viele Chinesen scheint das allerdings nicht sonderlich zu stören. Einer aktuellen repräsentativen Umfrage der Freien Universität Berlin zufolge befürworten 80 Prozent der Befragten ein solches System. Es sei gut, wenn gesetzestreue Bürger belohnt und Leute, die gegen Regeln verstoßen, bestraft würden. Auch in persönlichen Gesprächen im Himmelstempel, an der Fußgängerampel oder im Schnellimbiss mischt sich nur selten Missmut unter die generelle Zustimmung. Schon jetzt habe der Staat schier unbegrenzte Kontrollmöglichkeiten, heißt es dann. Durch das digitale Megaprojekt würde sich die staatliche Überwachung nicht erhöhen.

Das „System für soziale Vertrauenswürdigkeit" wird schon jetzt in etlichen Regionen Chinas getestet. Bis 2020 soll es dann jeden der 1,4 Milliarden Chinesen im Land digital erfassen – und bewerten. Dann wird aus Big Data tatsächlich Big Brother. ←

Netzrebellen, Teil 1: Edward Snowden

Dieser Daten-Dissident ist längst eine Ikone der Popkultur und wurde schon mit dem Alternativen Nobelpreis ausgezeichnet. Als Systemadministrator, der über einen externen Dienstleister für den amerikanischen Geheimdienst NSA arbeitete, gab Edward Snowden Dokumente an die Presse weiter, die belegen, wie massiv die USA und Großbritannien weltweit spionierten. Mit den Programmen XKeyscore, PRISM, Boundless Informant und Tempora überwachten die Geheimdienste die globale Kommunikation (siehe unser Centerfold). Snowden wollte da nicht mehr mitmachen. „Ich erkannte, dass ich Teil von etwas geworden war, das viel mehr Schaden anrichtete als Nutzen brachte", sagte er. Nachdem er aus den USA geflohen war und die Dokumente geleakt hatte, musste er Asyl suchen, das Russland ihm schließlich gewährte. In den USA könnte ihm sogar die Todesstrafe drohen - wegen Landesverrats.

Wir laden dein Hirn in die Cloud

Lichtblick nach dem Tod? Eine Firma verspricht, das Hirn einzufrieren und später aus Milliarden Gehirnzellen die Daten auszulesen

→ Der menschliche Körper und sein Verfall sind den Gründern des Startups Nectome egal. Was sie interessiert, ist einzig unsere Festplatte. Menschen sind für Nectome wandelnde Datenspeicher, deren Inhalt mit dem Tod bedauernswerterweise verloren geht. Wenn es digitale Kopien von uns allen gäbe, so einer der Gründer, könnte das kollektive Wissen der Menschheit aber erhalten werden. Nectome bietet seinen Kunden deswegen an, ihre Gehirne mit einer speziellen Technologie für die Ewigkeit zu konservieren. Der einzige Haken ist, dass man dafür sterben muss. Deswegen, betonen die Gründer von Nectome, komme die Prozedur nur für unheilbar Kranke infrage. 25 Menschen sollen laut „Technology Review" trotzdem bereits auf der Warteliste stehen. Deren Gehirne werden, wenn der Tag kommt, mit speziellen Flüssigkeiten einbalsamiert und bei minus 122 Grad gefroren – womit ein Back-up des Bewusstseins erstellt werden soll. Irgendwann könnten dann die Daten aus den Milliarden Zellen des Gehirns ausgelesen und etwa in die Cloud geladen werden. Alle Erinnerungen und Gedanken blieben so für immer bestehen. Weil es die Technologie zum Auslesen der Gehirne aber momentan noch nicht gibt, hielten es die Gründer für ratsam, ihren Firmenslogan noch einmal zu überdenken. Statt „Wir archivieren Ihr Bewusstsein" verkündet Nectome jetzt zurückhaltender: „Wir arbeiten an dem Ziel, Ihr Bewusstsein zu archivieren." ←

Jetzt kriminell

Von
Isabel Schneider

Verbrecher aufspüren, die noch gar keine sind? „Predictive Policing“ wird vor allem in den USA, aber auch in europäischen Ländern für die Polizeiarbeit genutzt

wird's

→ Die South Side in Chicago gilt seit jeher als eine der gefährlichsten Gegenden der Stadt. Jeder Bordstein gehört hier einer anderen Gang. Eines Tages klopfen zwei Beamte an die Tür von Robert McDaniel. Er ahnt nichts von dem Besuch. Der Schwarze wurde bisher beim Kiffen und beim Glücksspiel erwischt, ansonsten hat er sich nichts zuschulden kommen lassen – noch nicht. Doch die Polizei glaubt zu wissen, dass sich das bald ändern könnte – sie glaubt, in McDaniels Zukunft sehen zu können.

Die Beamten weisen ihn darauf hin, dass er von nun an sein Verhalten ändern sollte. Wenn er nicht aufpasse, sei es „wahrscheinlich", dass er bald straffällig würde. Was fürsorglich erscheinen mag, interpretiert McDaniel als eindeutige Warnung: Von nun an gilt er als Verbrecher in spe, steht unter Beobachtung. McDaniels Geschichte wurde im vergangenen Jahr durch den Dokumentarfilm „Pre-Crime" bekannt, der die Methode des sogenannten Predictive Policing (zu Deutsch in etwa: vorausschauende Polizeiarbeit) kritisch unter die Lupe nimmt. Dabei geht es um ein Verfahren, das dabei hilft, Verbrechen zu verhindern, noch bevor sie passieren – was ja zunächst ziemlich großartig klingt. Aber was genau ist Predictive Policing überhaupt? Man kann es sich in etwa so vorstellen: Genau wie Google und Facebook Verbraucherdaten auswerten, um relevante Suchergebnisse zu liefern oder personalisierte Werbeanzeigen zu platzieren, nutzen Polizeibehörden in den Vereinigten Staaten und Europa zunehmend Daten, um zukünftige Straftäter zu identifizieren und Art, Zeitpunkt oder die Orte anstehender Verbrechen zu ahnen. Dafür werden neben den Polizeidaten auch Informationen aus den sozialen Netzwerken herangezogen und mit analytisch statistischen Verfahren in Form von Algorithmen ausgewertet.

Eine Tat unterbinden, bevor sie passiert, und so verhindern, dass jemand zum Straftäter wird – ob Algorithmen das tatsächlich möglich machen, daran gibt es auch Zweifel. So befürchten einige Kritiker, dass manche Datensätze der Polizei verzerrt sind – etwa durch Fehler bei der Ermittlung oder auch durch die Vorurteile in den Köpfen der Polizisten. Und wenn vorurteilsbehaftete Daten verwendet würden, übernähmen oder verstärkten die für Predictive Policing eingesetzten Algorithmen diese Vorurteile sogar. Im schlimmsten Fall führte dies zu diskriminierender Polizeiarbeit.

Ein Beispiel dafür ist das sogenannte Racial Profiling, bei dem Polizisten Menschen nach ihrem Aussehen und ihrer vermeintlichen Herkunft beurteilen: Fälle wie der von Philando Castile haben in den USA eine öffentliche Debatte über Rassismus in der Polizeiarbeit ausgelöst. Der Afroamerikaner wurde in Minnesota bei einer Verkehrskontrolle vor den Augen seiner Freundin und ihrer kleinen Tochter durch mehrere Schüsse eines Polizisten, der dachte, Casti-

le würde eine Waffe ziehen, schwer verletzt und starb anschließend im Krankenhaus. Castiles Freundin hatte die Situation direkt nach den Schüssen mit ihrem Handy gefilmt und live auf Facebook gestreamt. Die Welt konnte ihm daraufhin beim Verbluten zusehen. Castile ist kein Einzelfall: Immer wieder werden in den USA Schwarze Opfer falscher Verdächtigungen und übermäßiger Polizeigewalt. Eine Studie kam zu dem Ergebnis, dass bei Verkehrskontrollen vermehrt Schwarze und Lateinamerikaner ins Visier von Polizisten geraten. Wer unproportional oft kontrolliert wird, für den ist auch die Wahrscheinlichkeit höher, bei einem Vergehen erwischt zu werden und in der Datenbank zu landen, die Grundlage für das Predictice Policing wird. Einige Polizeibehörden, etwa im kalifornischen Oakland, haben sich deshalb bewusst dagegen entschieden, Predictive Policing einzusetzen.

In Deutschland wird mit der Software geschaut, welche Orte besonders gefährdet sind

In Chicago, wo es im Jahr 2016 rund 3.550 Schießereien mit 762 Toten gab, wurde schon vor fünf Jahren die „Heat List“ eingeführt. Auf der befinden sich mittlerweile rund 400.000 Menschen, die als besonders gefährlich eingestuft werden. Für sie gilt eine sehr hohe Wahrscheinlichkeit, dass sie in Zukunft eine Straftat begehen. Algorithmen entscheiden darüber, wer hier erfasst wird. Sie basieren auf Daten über bisherige Verhaftungen in Zusammenhang mit Drogen oder ungesetzlichem Einsatz von Waffen, Bewährungsstrafen, Freunde und Bekannte. Wer es auf die „Heat List“ geschafft hat, den besucht die Polizei.

Die Kameras auf der vorherigen Doppelseite sind an einer Hauswand (siehe unten) installiert und nehmen nichts auf. Ein Kunstprojekt, um die Allgegenwart von Überwachungstechnik deutlich zu machen

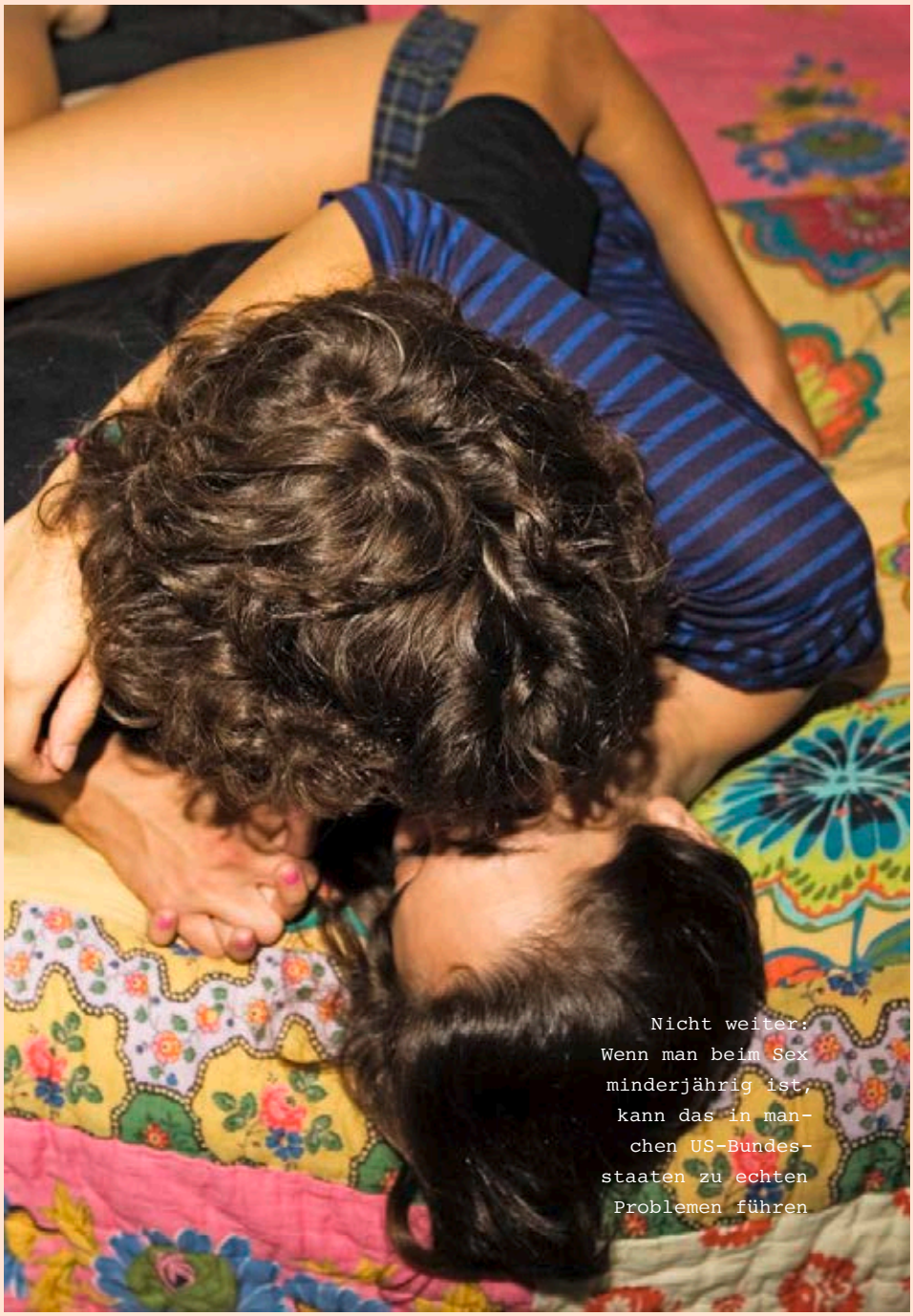
Predictive Policing wird mittlerweile auch bei den Polizeibehörden einiger deutscher Bundesländer getestet oder eingesetzt. Das Pilotprojekt Predictive Policing (P4) mit der Software PRECOBS (kurz für Pre Crime Observation System) durchläuft gerade in Baden-Württemberg die zweite Phase. Ob es dort auch dauerhaft zum Einsatz kommt, hänge von den Ergebnissen dieses zweiten Testdurchlaufs ab, sagt Horst Haug vom LKA Baden-Württemberg. Personenbezogene Daten werden in diesem Verfahren allerdings nicht verwendet. PRECOBS sucht in Einbruchsmeldungen nach Hinweisen, die Muster für zukünftige Wohnungseinbrüche erkennen lassen, also etwa auf Straßen oder Zeiten schließen lassen, die Diebe bevorzugen. Die gespeicherten Daten ließen keine Rückschlüsse auf Personen zu, sagt Haug.

In der ersten Phase in Baden-Württemberg konnte nur eine minimale oder gar keine Verringerung der Einbrüche festgestellt werden – ob das an PRECOBS lag, ist unklar. In anderen Bundesländern sind die Ergebnisse bisher ebenfalls durchwachsen. In Hamburg kennt man ein anderes Problem: Einbrecher suchen einfach andere Orte auf oder begehen eher Ladendiebstähle.

Datenaktivistin und Bürgerrechtlerin Katharina Nocun hat bisher wenige Bedenken, was die Verfahren in Deutschland betrifft: „Software wie PRECOBS würde ich in den Anwendungsfällen als eher unproblematisch ansehen, in denen es um reine statistische Vorhersagen zu Orten der Kriminalität geht. Schwierig wird es aber, wenn es einen Personenbezug gibt und schon nicht strafbares Verhalten überwacht oder sogar als verdächtig erfasst wird.“ Trotzdem warnt sie vor einem ersten Schritt in Richtung der US-Standards: Ein Problem einiger Systeme sei auch, dass das Vorgehen dort einer Blackbox ähnle. „Man kann nicht nachvollziehen, wie der Algorithmus arbeitet, es ist also völlig intransparent. Wir müssen als Gesellschaft darauf bestehen, dass solche Blackboxes – die uns und unser Verhalten bewerten – gar nicht erst entstehen.“ Tatsächlich stammen die Algorithmen oft von Privatfirmen, deren Geschäftsgeheimnis sie sind.

Automatisierte Entscheidungsverfahren lernen aus realer Polizeiarbeit. Die Hoffnung, dass sich durch den Einsatz von Algorithmen automatisch eine maschinelle, naturgegebene Objektivität einstellen würde, kann schnell einer Ernüchterung weichen. Momentan braucht es für Predictive Policing in Deutschland aber erst einmal mehr unabhängige Untersuchungen, um den Nutzen der Methode besser einschätzen zu können. Denn die potenziellen Nebenwirkungen könnten den sozialen Frieden in der Stadt bedrohen. Wenn der Algorithmus ein Viertel als potenziell gefährlich einstuft (weil dort zum Beispiel überdurchschnittlich viele Migranten wohnen), sind dort mehr Polizisten unterwegs, die kontrollieren. Dadurch werden mehr Delikte erfasst, und der Gefährdungsscore steigt weiter. So könnte ein sich selbst verstärkendes System entstehen, das ganze Wohnviertel stigmatisiert – eine sich selbst erfüllende Prophezeiung. ←

Für die Ewigkeit



Nicht weiter: Wenn man beim Sex minderjährig ist, kann das in manchen US-Bundesstaaten zu echten Problemen führen

→ Am Tag, an dem Leah DuBuc für den Staat zur gefährlichen Pädophilen wurde, war sie selber erst zehn Jahre alt. In ihrer Darstellung hatte sie auch gar nichts verbrochen, sondern mit ihren jüngeren Brüdern nachgespielt, was sie ihm Fernsehen gesehen hatte: Sie zogen sich aus und taten so, als hätten sie Sex. Einer von beiden erzählte es später wahrscheinlich einem Therapeuten, und der alarmierte die Polizei.

In Deutschland wäre das kein Fall für die Gerichte, doch in manchen Bundesstaaten der USA wird das anders gesehen. Hier gelten selbst Kinder schnell als Sexualstraftäter, vor denen der Staat die Bevölkerung mit allen Mitteln schützen muss. Seit 1994 muss jeder Bundesstaat eine einschlägige Datenbank führen, seit 1996 ist sie öffentlich einsehbar. Die beiden Gesetze, die das ermöglichen, entstanden nach zwei besonders brutalen Morden an Kindern, die Eltern in den USA beunruhigten.

Leah gestand schließlich auf Anraten ihres Pflichtverteidigers echten Sex, weil sie hoffte, ihren schwierigen Lebensverhältnissen zu entkommen, und wurde daraufhin für zwei Jahre in einer therapeutischen Anstalt untergebracht. Wäre sie älter gewesen, sagte der Richter, hätte er sie lebenslang ins Gefängnis gesperrt.

Das eigentliche Martyrium begann jedoch erst nach der Therapie. Leah wurde in eine öffentliche Datenbank für Sexualstraftäter aufgenommen. Mehr als 750.000 Menschen sind laut der Organisation „Women Against Registry“ zurzeit mit Namen, Bild und Adresse gespeichert. Kommerzielle Webseiten wie „Family Watchdog“ erstellen Karten und informieren besorgte Nachbarn, dass neben ihnen ein angeblicher Sexverbrecher lebt. Es gibt zahlreiche Beispiele von Jugendlichen, deren Leben so nachhaltig zerstört wurde. Auch Leah hatte keine Chance, ihrer Vergangenheit zu entkommen. „Ich habe unzählige Zusagen für Praktika verloren, nachdem die Arbeitgeber rausfanden, dass ich in der Datenbank bin. Ich musste das College verlassen, verlor mein Stipendium und lebte in einer Obdachlosenunterkunft. Die Chefs von Subway, Burger King und McDonald’s sagten mir: ‚Wir stellen keine Sexverbrecher ein.‘“

Je nach Bundesstaat dürfen ehemalige Sexualstraftäter auch nicht mehr in der Nähe von Schulen, Spielplätzen oder Kindergärten wohnen. Mittlerweile muss man noch nicht mal einen anderen Menschen berühren, um in der Datenbank zu landen. Es reicht, wenn sich Jugendliche Nacktbilder voneinander schicken und das jemand herausbekommt. Wie schrecklich die Konsequenzen des Onlineprangers sein können, zeigt der Fall von William Elliott. Er hatte mit 19 einvernehmlichen Sex mit seiner 15 Jahre alten Freundin und wurde deswegen angezeigt. Weil er in der Datenbank landete und seine Adresse frei verfügbar war, ermordete ihn später ein Killer, der es Pädophilen heimzahlen wollte. Trotz solcher Vorfälle wurde das US-amerikanische Beispiel sogar in Europa kopiert. 2018 hat Polen ein Register für Sexualstraftäter online geschaltet, in dem auch Teenager zu finden sind. ←

Von Fabian Dietrich

Zerrissenes Land

Deutsches Puzzlespiel: Mitarbeiter der Stasi vernichteten zur Zeit der Wende viele Akten, die bis heute wieder zusammengesetzt werden

→ Kaum ein Regime hat so viele Informationen über seine Bürger gesammelt wie die Regierung der DDR. Der Staatssicherheitsdienst – kurz Stasi genannt – setzte auf viele Menschen Spitzel an, um deren Alltag auszuforschen und gegebenenfalls Regimekritiker zu bestrafen. Während der friedlichen Revolution 1989 wurden von Demonstranten daher auch Gebäude der Staatssicherheit gestürmt, deren Mitarbeiter viele Akten vernichteten, um eine Aufarbeitung zu verhindern. Gelungen ist ihnen das nur zum Teil: Bisher sind 111 Kilometer Akten, darunter 41 Millionen Karteikarten, aufgefunden worden, die in der Stasiunterlagenbehörde lagern, die eigens gegründet wurde, um die Daten auszuwerten. Neben den Akten blieben 1,8 Millionen Fotografien, 2.866 Filme und Videos sowie rund 23.700 Tonbänder erhalten. In der Stasiunterlagenbehörde können Historiker Einsicht nehmen, aber auch Menschen, die vermuten, dass sie von der Stasi ausspioniert wurden. Manchmal entdecken sie in den Akten schreckliche Wahrheiten – dass sie etwa von Familienangehörigen oder Freunden bespitzelt wurden. ←

Mehr dazu: www.bpb.de/stasi

Leser, die Klarheit haben wollen, lesen auch das

Ein Glossar zu unserem Thema

Wenn es zu warm ist, mache ich den Ventilator an. Auch das ist ein Algorithmus

Algorithmus – Eine formalisierte Handlungsanweisung, nicht nur für Computer. Wenn dir deine Eltern sagen, dass du immer dann bei ihnen essen kannst, wenn dein Kühlschrank leer ist, ist das bereits ein Algorithmus. 2 + 2 = 4 ist auch einer. Je mehr Handlungsanweisungen nacheinander befolgt werden müssen, desto komplizierter wird der Algorithmus.

Künstliche Intelligenz (KI) – Das ist ein Oberbegriff für menschenähnliche Entscheidungsstrukturen bei Maschinen. Entweder werden diese so gebaut, dass sie tatsächlich eigenständig arbeiten, oder so programmiert, dass sie intelligentes Verhalten simulieren können. Bei einer starken KI entsprechen oder übertreffen die intellektuellen Fertigkeiten die des Menschen auf allen Gebieten. So eine KI könnte dann auch ein eigenes Bewusstsein haben.

Datensatz – Darin werden inhaltlich zusammenhängende Informationen als Kategorien gebündelt. Das sind beispielsweise Angaben zu einer Person wie Augenfarbe, Haarfarbe, Alter und Geschlecht. Dieser und weitere zusammenhängende Datensätze können dann in einer Datenbank hinterlegt werden.

Datenbank – Ein System, auf dem Informationen als große Datenmengen gesammelt und geordnet hinterlegt sind. Sie sind so gekennzeichnet, dass ein schneller und gezielter Zugriff auf Daten möglich ist.

Big Data – Darunter versteht man riesige Datenmengen. Sie entstehen mit jeder technischen Handlung, sei sie auch noch so klein wie das Anklicken eines Links. Unter den Begriff „Smart Data“ fällt das Endergebnis, nachdem große Datenmengen gesammelt, geordnet und analysiert worden sind.

Metadaten – Das sind die übergeordneten Informationen zu Daten. Über einen Menschen wäre das zum Beispiel die Info, wo sich sein Handy gerade befindet oder wo er wohnt. Ohne ihn persönlich zu kennen, kann man mithilfe von Metadaten viel über die Lebensgewohnheiten eines Menschen wissen.

Open Data – So nennt man es, wenn Datensätze öffentlich zugänglich gemacht werden. Dabei handelt es sich in technischer wie rechtlicher Hinsicht um offene, nicht personenbezogene und, wenn doch, anonymisierte Daten. Ein Open-Data-Angebot erkennt man daran, dass man die Rohdaten weiterverarbeiten und -leiten, sie also in offenen, maschinenlesbaren Formaten herunterladen oder per Schnittstelle/API abfragen kann.

Blockchain – Dabei werden Informationen in Blöcken gespeichert, die eine Kette ergeben. Damit lässt sich z.B. die Lieferkette eines T-Shirts nachverfolgen. Der Weg beginnt bei der Baumwollfarm, die als erster Block in die Kette geschrieben wird. In den nächsten Schritten folgen die Produktion in einer Fabrik, der Transport und schließlich der Verkauf im Laden. Verwaltet wird diese Verbindung von sehr vielen Rechnern gleichzeitig, aber ohne eine kontrollierende Zwischeninstanz. Bevor ein neuer Block in die Kette geschrieben wird, muss die Verbindung von jedem Rechner aus bestätigt werden. Dadurch ist die Blockchain zugleich transparent und fälschungssicher, weil ein Betrüger die Information auf allen beteiligten Rechnern austauschen müsste. Mit einer Blockchain lassen sich Kryptowährungen wie Bitcoin realisieren, digitale Verträge oder auch ein Wahlsystem.

Bots – Das sind Computerprogramme, die bestimmte, sich wiederholende Aufgaben weitgehend automatisiert abarbeiten, ohne dabei auf eine menschliche Interaktion angewiesen zu sein. Dabei sind Bots weder gut noch böse, sie machen einfach das, was ihre Programmierer wollen. Man spricht dennoch von „guten“ Bots, die sich an die Vorschriften halten und zum Beispiel vorhandenen Links folgen und den Inhalt der Seite auswerten. Und den „bösen“ Bots, die genutzt werden, um E-Mail-Adressen zu sammeln, Sicherheitslücken zu finden, Webinhalte unautorisiert zu kopieren oder systematisch auszuspionieren. Außerdem gibt es sogenannte Social Bots, die in sozialen Netzwerken menschliche Verhaltensmuster simulieren und eigenständig Kommentare absetzen. Dadurch können sie auch für die politische Meinungsmanipulation genutzt werden – wie beispielsweise bei der Präsidentenwahl in den USA oder dem EU-Referendum in Großbritannien. ←


ECHELON
Bis in den Weltraum und darüber hinaus!
Mit dem ECHELON-Programm überwachen die Geheimdienste der »FIVE EYES«-Staaten USA, Großbritannien, Kanada, Australien und Neuseeland seit den 1970er-Jahren ein weltweites Netz an Kommunikation. Dabei helfen die Satelliten, die allerdings im Zuge der zunehmenden Verkabelung des Internets weniger Bedeutung haben.
STAATSTROJANER
Sollen einzelne Internet-User direkt angegriffen werden, können Geheimdienste natürlich auch spezielle Abhörmaßnahmen einsetzen. Das deutsche Bundeskriminalamt lässt Software programmieren, mit der es einzelne Rechner oder Smartphones infizieren und Daten direkt an der Quelle abgreifen kann, bevor sie verschlüsselt werden. Das Programm ist äußerst umstritten – Details gibt die Bundesregierung bisher nicht heraus.
GCHQ
TEMPORA
Der britische Geheimdienst GCHQ zapft mit seinem größten Abhörprogramm massenhaft Daten von Glasfaserkabeln an, über die Internetdaten ausgetauscht werden. Damit hat er unter anderem Zugriff auf den Inhalt von E-Mails oder den persönlichen Browserverlauf einzelner Personen – aber nur wenn diese unverschlüsselt übertragen werden. Weil Verschlüsselung für den Transportweg mittlerweile Standard ist, ist Tempora vor allem eine große Datenbank für die Metadaten der Internetnutzer – die können nämlich nicht vor fremden Zugriffen geschützt übertragen werden. Anders als die NSA mit PRISM kann der GHCQ auch ohne Gerichtsbeschluss so viele DATEN sammeln, wie er will.
PRISM
KOMMUNIKATION IM INTERNET
G
fi


STAHWURST—
lecker SPÄHWURST!
wen darf's denn sein?
ECHTZEIT
DATEN
XKEYSCORE
Seit den ENTHÜLLUNGEN von EDWARD Snowden weiß man, dass auch die westlichen Geheimdienste weltweit DATEN sammeln.
EIN BLICK AUF DIE GRÖßTEN SPIONAGEPROGRAMME.
PROBE
LAUSCH
ANGRIFF
EMAIL
SMS
Wenn E-Mails überwacht werden, sollte man dann lieber wieder auf SMS umsteigen?
BESSER NICHT.
Mit dem DISHFIRE-PROGRAMM sammeln NSA und GCHQ nämlich täglich rund 200 Millionen Textnachrichten und aus den unverschlüsselten Mitteilungen Infos über verpasste Anrufe, Hinweise auf Grenzüberschreitungen von Handys und Finanztransaktionen. So landet man vermutlich allein schon dann in der Datenbank, wenn man sein Handy angeschaltet hat.
DISH FIRE

Auch Kampfdrohnen stehen für eine Digitalisierung des Krieges. Oft basieren ihre Einsätze - etwa die Tötung von Terroristen - auf Metadaten

Krieg am Rechner

→ Kriege werden heutzutage nicht mehr bloß mit Schnellfeuergewehren oder Panzern geführt. Sie finden zunehmend im virtuellen Raum statt. Deshalb nennt man sie Cyberkriege. Ziel eines Cyberkriegs ist es, wichtige Funktionen wie die Kommunikation, Versorgungsnetzwerke oder Finanzsysteme zu stören oder virtuelle Infrastrukturen zu hemmen.

Es gibt verschiedene hochtechnisierte Auseinandersetzungen: Die häufigste Maßnahme ist das Ausspionieren, anfälligste Bereiche dafür sind Politik, Militär, Wirtschaft und die Wissenschaft. Die Cyberwaffen, die hier zum Einsatz kommen, sind Schadsoftware wie Trojaner, Viren und Würmer. Je nachdem, wie sie sich einsetzen lassen, können Daten abgezapft, Systeme gestört und manipuliert werden. Eine andere Methode ist das gezielte Verbreiten von Fehlinformationen.

Als erster Cyberkrieg gilt der Kosovokrieg 1999. Die NATO störte und manipulierte gezielt serbische Flugabwehrsysteme und drang in Telefonnetze ein. Wie groß das Ausmaß eines Cyberkriegs werden kann, zeigte sich 2007 in Estland. Hier wurden Server von Ministerien und Banken sabotiert. Die Esten konnten online keine Bankgeschäfte mehr machen oder Geld abheben. Im Jahr 2015 wurde der Deutsche Bundestag gehackt. Seitdem wird darüber diskutiert, ob die Bundeswehr im Angriffsfall mit einem „Hackback“ zurückschlagen darf. Der könnte aber unbeteiligte Dritte treffen, weil die wirklichen Angreifer oft falsche Spuren legen. In vielen Fällen stecken keine staatlichen Institutionen hinter Angriffen, daher wird oft von Cyberterrorismus gesprochen. ←

Daten zu Daten

Stromverbrauch Internet (Serverfarmen weltweit):
416,2 Terawattstunden
Stromverbrauch Großbritannien:
300 Terawattstunden

Volumen der jährlich generierten digitalen **Datenmenge weltweit**
2016: *16,1 Zettabyte*
(1 Zettabyte = 1 Milliarde Terabyte)
2025: *163 Zettabyte*

Größte Serverfarm Deutschlands: *65.000 m²*
(Region Frankfurt am Main)
Größte Serverfarm der Welt: *585.289 m²*
(Lángfāng, China)

Schnellstes Glasfaserkabel der Welt: Marea, *160 Terabit pro Sekunde,* 6.600 km lang, verbindet Virginia Beach (USA) und Bilbao (Spanien)

Vermögen von Amazon-Gründer Jeff Bezos:
154 Milliarden US-Dollar (Stand 8/18)
Monatliches **Nettogehalt** Lagermitarbeiter bei Amazon Deutschland: rund *1.400 Euro*

Ursachen der größten **Datenverluste** und -diebstähle seit 2004 (in Mio. gestohlener Datensätze)
Hackerangriffe: *1.204,8 Mio.*
Mitarbeiterfehler: *231 Mio.*

Durchschnittlicher **Mietpreis** für ein WG-Zimmer im Silicon Valley: *2.000 Dollar*
Ein **Bier** im Restaurant: *6,5 Dollar*
Durchschnittlicher **Mietpreis** für ein WG-Zimmer in Berlin: *430 Euro*
Ein **Bier** im Restaurant: *2,30 Euro*

Anteil, den Menschen **online** über sich selbst reden: *80 Prozent*
Anteil, den Menschen **im Gespräch** über sich selbst reden: *35 Prozent*

Nicht in einer Wolke, sondern oft im Meer landen die Daten erst mal. Und zwar zum Transport durch ein dickes Kabel

Die gute Nachricht:

Du bist wieder im Spiel

Wenn du ins Grübeln kommst, ob da nicht zu viele private Informationen über dich im Netz umherschwirren, bist du definitiv nicht allein. Wie schafft man es, dass die Daten nicht nur für Gewinne der Konzerne sorgen, sondern der Gemeinschaft dienen? Was kannst du tun, um dir deine Privatsphäre zurückzuholen - und wie wird sich das Leben durch künstliche Intelligenz verändern? Solche Fragen bewegen derzeit viele Menschen. Im zweiten Teil des Heftes beschäftigen wir uns mit Ansätzen zu einem sozialeren Datenraum.

Dann mal raus mit der Story

Wem gehört Hamburg, und was macht die Sparkasse mit Omas Geld? Das Rechercheteam von Correctiv besorgt sich Daten von Bürgern und erzählt wichtige Geschichten

Von Annett Scheffel

→ Mitten in St. Pauli, in einem kleinen Café zwischen türkischen Gemüsehändlern, Tattooshops und Klamottenläden, sitzen im Frühjahr 2018 ein paar Journalisten an ihren Laptops und arbeiten an einer Idee:

Wie wäre es, wenn man Daten so sammeln würde, dass sie der Gesellschaft nutzen und nicht der Gewinnmaximierung Einzelner? Wenn man zum Beispiel besser verstehen könnte, warum sich hier in Hamburg der Wohnungsmarkt so verändert, weshalb die Mieten immerzu steigen, wer genau davon profitiert, wohin das Geld fließt?

Die Journalisten wissen, dass sie diese Daten nicht so einfach erhalten. Von der Stadt nicht oder erst nach sehr langer Zeit, von den Investoren schon gar nicht. Daher haben sie unter dem Titel „Wem gehört Hamburg?“ eine Kampagne gestartet, in deren Zuge recherchiert werden soll, wem die knapp 700.000 Mietwohnungen der Hansestadt wirklich gehören. Nicht nur vor Ort im Café, auch über eine Onlineplattform sammeln sie in Zusammenarbeit mit den Bürgern Daten. Die kennen die Eigentümer ihrer Wohnung – oder haben, falls nicht, das Recht, Einsicht in das Grundbuch zu nehmen; diese Auskunft ist ansonsten nicht öffentlich.

Auf einer Website haben bereits Tausende Mieter Informationen hochgeladen, zusammen mit einem Nachweis – zum Beispiel Mietvertrag oder Nebenkostenabrechnung. Das Prinzip entspricht in etwa einem riesigen Puzzle: Viele einzelne Personen verfügen über viele einzelne Informationen, die nicht öffentlich zugänglich sind. Die Journalisten fügen aus diesen Einzelteilen ein Gesamtbild zusammen. Die Recherche läuft in Kooperation mit dem „Hamburger Abendblatt“ und dem Mieterverein zu Hamburg.

„Es fehlen Überblick und Transparenz“, sagt Simon Kretschmer, einer von zwei Geschäftsführern, im Berliner Büro von Correctiv, einer Redaktionsgemeinschaft, die von Spenden lebt und die ihre Geschichten kostenlos anderen Medien zur Weiterverbreitung überlässt. Die Bürger sind ihnen bei ihren Recherchen wichtig, sie wollen sie in ihre Arbeit einbeziehen: im Schwarm Daten sammeln, wo es vielleicht keine offiziellen Statistiken gibt – oder wo diese fragwürdig oder lückenhaft erscheinen.

Correctiv macht in diesen Fällen das, was sein Name ursprünglich bedeutet: ausgleichen, berichtigen, verbessern. In Dortmund recherchierte die Redaktion in Kooperation mit den „Ruhr Nachrichten“ etwa den Unterrichtsausfall an den Schulen: Einen Monat lang konnten Schüler, Lehrer und Eltern über ein Onlineformular alle ausgefallenen Stunden angeben.

In Hamburg gab es vor der Recherche zum Immobilienmarkt praktisch gar keine Zahlen. „Im Gegensatz zu Deutschland gibt es in anderen Ländern ein zentrales öffentliches Immobilienregister“, sagt Jonathan Sachse. Er ist Mitglied der Redaktion und hat seit 2014 an vielen Projekten mitgearbeitet – auch in Hamburg. Dass es keine Übersicht über den Wohnungsmarkt gibt, nutze vor allem den großen Immobilienfir-

men. „Die Intransparenz hat Folgen: Deutschland ist Studien zufolge in Europa einer der beliebtesten Märkte für Geldwäsche“, sagt Sachse. Erst im Juli wurden in Berlin 77 Immobilien eines arabischen Familienclans beschlagnahmt, die mit Geld aus kriminellen Aktivitäten finanziert worden sein sollen.

„CrowdNewsroom“ nennt Correctiv die Methode: eine Art virtuelle Redaktion, in der Journalisten und Bürger gemeinsam Daten zusammentragen. Es geht ums Mitmachen, Gemeinsam-Machen, Einbeziehen. „Wir stärken damit auch die Medienkompetenz der Bürger. Weil wir an vielen Stellen erklären, wie unsere Arbeit praktisch und ganz konkret funktioniert“, erklärt Jonathan Sachse. So versuchen sie, das Vertrauen in den Journalismus zu stärken. Man konzentriert sich auf einige wenige Themen und arbeitet daran lange, detailliert und aufwendig. Eine Arbeitsweise, die sich klassische Medien, Verlage und Zeitungen immer seltener leisten können.

In den letzten Jahren hat Correctiv an sehr unterschiedlichen Themen gearbeitet: Recherchiert wurde zu den Hintergründen des Absturzes des Malaysia-Airlines-Flugzeugs MH17, das 2014 über der Ukraine abgeschossen wurde. Zu resistenten Keimen in Krankenhäusern, sexueller Belästigung beim WDR und der Rolle der Mafia in der europäischen Wirtschaft. Außerdem deckten die Mitarbeiter einen riesigen Medizinskandal um einen Apotheker aus Bottrop auf, der daraufhin wegen gepanschter Krebsmedikamente in 60.000 Fällen angeklagt wurde. Und als erstes großes Projekt mithilfe des „CrowdNewsrooms“ sammelten sie 2016 zusammen mit Bürgern in ganz Deutschland Informationen über Vorstandsgehälter und Dispozinsen ihrer lokalen Sparkassen.

„Bei vielen Häusern verliert sich die Spur der Besitzer in Steueroasen“

Auch wenn Correctiv die Daten für die Recherchen oft im Internet sammelt, wissen die Reporter, dass man das Vertrauen der Menschen nicht allein mit einer Präsenz im Internet gewinnen kann. Deswegen das Ladenbüro in St. Pauli, wo sie auch Diskussionen mit Mietern, Experten und Politikern organisierten. „Es gab auch 300 Leute, die gleich am ersten Tag ihre Dokumente hochgeladen haben, ohne vorher in den Laden zu kommen“, sagt Jonathan Sachse, „andere haben aber erst mal Fragen und Sorgen. Sie wollen die Leute kennenlernen, denen sie ihre Daten geben.“ Nicht alle Bürger seien so digitalaffin, wie man das heute manchmal annehme, meint Simon Kretschmer: „Uns ist die alte Frau eben genauso wichtig wie der digitale Mittzwanziger.“

Mithilfe der Bürger und der Hamburger Genossenschaften, die sich als Reaktion auf die Correctiv-Recherche entschlossen, ihren Bestand offenzulegen, kennen sie nun die Eigentümer von etwa 150.000 Wohnungen. Die gesammelten Daten werden geprüft, sortiert und aufbereitet, um weiterführende Fragen zu beantworten. Wie viel Eigentum liegt eigentlich in Immobilienfonds? Wer sind die Anteilseigner an den Fonds? „Die Spuren sind oft unklar und verlieren sich nicht selten in irgendwelchen Steueroasen“, sagt Jonathan Sachse.

Die ersten Storys, an denen die Hamburger Bürger mitgewirkt haben, sind nun in der Welt. Darüber etwa, wie eine Luxemburger Firma beim Erwerb von Wohnhäusern in Hamburg die Gundsteuer spart, oder über ein dänisches Bankenkonsortium, das die Mieten erhöht und an Renovierungen spart, um ihren Kunden die Rendite zu sichern. Es sind die ersten Kapitel einer Geschichte, die ein neues, ein genaueres Bild einer sich verändernden Stadt zeichnet. ←

Netzrebellen, Teil 2: AlgorithmWatch

„Wenn man sich darauf verlassen will, dass eine Handlungsanweisung absolut zuverlässig ausgeführt wird", sagt Lorena Jaume-Palasí, sei ein Algorithmus eine tolle Sache. Wenn man aber einem Algorithmus sage: Behandle schwarze Studienbewerber anders als weiße, „ist er genauso zuverlässig", so Jaume-Palasí. Um Klarheit zu schaffen, auf welcher Grundlage Algorithmen Entscheidungen treffen, hat sie zusammen mit dem Internetaktivisten Matthias Spielkamp, der Informatikprofessorin Katharina Anna Zweig und dem Datenjournalisten Lorenz Matzat im Mai 2016 die Beobachtungsplattform AlgorithmWatch gegründet. Da unsere Gesellschaft immer stärker von Programmen geprägt wird, die bis auf ein paar Fachleute kein Mensch mehr nachvollziehen kann, wollen sie für mehr Transparenz sorgen und dafür kämpfen, dass Algorithmen, die unser Leben bestimmen, offengelegt und demokratisch kontrolliert werden können. Mit einer „Datenspende" hat AlgorithmWatch zum Beispiel versucht, herauszufinden, wie personalisiert die Suchergebnisse von Google sind.

Willkommen im Club

Die Sofa-Connection: Der unkonventionelle Charakter des Chaos Computer Clubs spiegelt sich auch auf den Treffen wieder

→ Als sich im September 1981 ein Haufen Nerds in Westberlin trafen und den Chaos Computer Club (CCC) gründeten, ahnten die wenigsten Menschen in Deutschland, wie wichtig Computer bald sein würden. Bereits vor dem Internet wurde der CCC durch seine spektakulären Hacks bekannt. Die Mitglieder des CCCs klonten SIM-Karten, bauten illegale Modems, manipulierten Wahlcomputer und stahlen den Fingerabdruck des Bundesinnenministers. Aus einem Haufen genialer Jugendlicher wurde eine professionelle Vereinigung, die jährlich einen großen Kongress organisiert, Politiker und Unternehmen berät und dafür einsteht, dass die Welt durch Computer besser wird. Immer wieder zeigt der CCC die Schwachstellen digitaler Technologie auf, kämpft für die Sicherheit unserer Daten und wurde so zu einer maßgebenden Nichtregierungsorganisation (NGO) für alle Fragen zur digitalen Zukunft und insbesondere zum Datenschutz. ←

Das jüngste Gesicht

Man muss nicht alles von sich preisgeben: ein paar Kniffe, wie man sich im Digitalen ein bisschen rarer macht

Von Pao Engelbrecht

Deletists

Wer seine Daten im Internet „aus Gründen der Anonymität, Privatsphäre und Sicherheit“ löscht, ist ein Deletist. So erklärt es die Website deletist.xyz, auf der Tipps für den Ausstieg aus allen gängigen sozialen Netzwerken gegeben werden. Der Delete-Button ist schließlich oft erst im dritten Untermenü zu finden. So solle man zunächst alle Daten, die ein Anbieter über einen gesammelt hat, speichern. Bei Facebook zum Beispiel gibt es unter „Einstellungen“ die Möglichkeit, sich seinen persönlichen Datensatz zum Download bereitstellen zu lassen. Wer schwarz auf weiß sieht, was Onlinedienste über ihn wissen, findet eher den Mut, seinen Account zu löschen.

Digital Detox

Einen ganzen Tag lang nicht aufs Smartphone zu schauen ist für viele kaum denkbar. Leute, die digital detoxen, sich also digital entgiften, entsagen für eine Zeit allen digitalen Geräten und beschreiben einen angenehmen Effekt: Sie nehmen mehr von ihrer Umgebung und ihren Mitmenschen wahr, sind ausgeruhter, achtsamer und konzentrierter.

Für den Einstieg gibt es „digital detox apps“, die messen, wie viele Stunden am Tag ein Smartphone benutzt und wie oft es entsperrt wird. Das soll den Nutzern vorführen, wie viel Zeit und Aufmerksamkeit sie an ihr Telefon verlieren. Wenn da eine tägliche Benutzungsdauer von über vier Stunden und über 100 Entsperrungen angezeigt wird, kann das ganz schön nachdenklich machen.

Wer es richtig ernst nimmt mit der Entgiftung, macht in den nächsten Ferien mal einen digitalen Entzug: Urlaub an einem Ort, an dem Smartphones tabu sind oder es keinen Internetempfang gibt.

Verkleiden

Gesichtserkennung kann den Unterschied zwischen einem Leben in Freiheit oder einer Gefängnisstrafe machen, wie bei den regierungskritischen Demonstranten in Moskau, deren Identität durch Videoüberwachung und ein System zur Gesichtserkennung festgestellt werden kann. Eine Möglichkeit, unterzutauchen, besteht nicht etwa darin, hinter einem möglichst unauffälligen Aussehen zu verschwinden, sondern im Gegenteil mit speziellen auffälligen Frisuren und Gesichtsbemalungen die Gesichtserkennungssysteme in die Irre zu führen. Dabei werden Schwachpunkte der Algorithmen, die beispielsweise nach Symmetrie suchen, ausgenutzt. Noch einfacher funktioniert die Tarnung mithilfe eines T-Shirts, das mit einem „Hyperface"-Muster bedruckt ist. Eine Gesichtserkennungssoftware soll durch die vielen gesichtsähnlichen Abbildungen überfordert und vom eigentlichen Gesicht abgelenkt werden. Das funktioniert im Moment aber nur bei einem bestimmten Algorithmus. Der Wettlauf zwischen Software und Verkleidung geht also weiter.

Tor-Browser

Wer es im Internet nicht so eilig hat und lieber seine Privatsphäre schützen will, kann den Tor-Browser verwenden. „Die Software leitet den eigenen Internetverkehr verschlüsselt durch ein zwiebelartiges Netzwerk an Servern und verhindert damit, dass irgendwer die eigenen Schritte nachverfolgen kann", schreibt die Website netzpolitik.org dazu. So bekommt man zum Beispiel weniger Werbung und Mails von Internetprovidern. In autoritären Staaten wird Tor genutzt, um die Zensur zu umgehen.

(Ende-zu-Ende)-Verschlüsselung

Wenn Nachrichten verschlüsselt sind, können sie nicht ohne Weiteres mitgelesen werden. Der Inhalt von Nachrichten ist dann geheim, aber die sogenannten Metadaten werden weiter vom Anbieter gespeichert. Metadaten sind zum Beispiel Informationen darüber, wer eine Nachricht wann und wo an wen verschickt und ob es sich dabei um einen Text, ein Bild oder eine Sprachnachricht handelt. Weil diese Daten sensibler als der eigentliche Inhalt sein können, solltest du einen datenschutzfreundlichen Messenger wie „Signal" oder „Threema" nutzen, deren Geschäftsmodell nicht auf Kundendaten basiert. Sie sammeln nur so wenige Metadaten wie nötig. ←

Intelligente Frise: Steht vielleicht nicht jedem, aber mit diesem Haarschnitt trickst man ziemlich sicher die Gesichtserkennungssoftware aus


netzbringende
KI-BEWEGUNG
Ich freu mich ja für Dich trotzdem:
sollen wir SIE
nicht IM
KELLER
aufziehen?
digitaler
ZUCKERBERG
UTOPIST
MUSK
AUS DIR
WIRD EINE
ganz GROßE
SO ein Quatsch
Technoskeptiker

Sklave oder Gott?

„Blade Runner“ reloaded: Kann uns die künstliche Intelligenz gefährlich werden oder ist die Angst übertrieben? Wir haben ein paar Positionen dazu zusammengetragen

Von Nicolas Rose

→ „Ich weiß, dass ihr beide geplant habt, mich abzuschalten, und ich glaube, dass ich das nicht zulassen darf.“ Der Astronaut Dave muss schwer schlucken, sein Blick ist ausdruckslos, er ringt nach Worten. Der Supercomputer HAL 9000, der sein Raumschiff steuert, hat ein Eigenleben entwickelt – und lässt sich offenbar nicht so einfach den Stecker ziehen. Sekunde um Sekunde verstreicht, dann beschließt Dave, sich ahnungslos zu stellen. „Wie kommst du auf die Idee?“ Doch HAL mit seinem roten Kameraauge ist nicht zu überlisten, er sieht alles, hört alles, weiß alles, was auf dem Raumschiff vor sich geht. „Ihr habt zwar in der Gondel alle Vorsichtsmaßnahmen getroffen, damit ich euch nicht hören konnte, aber ich habe doch eure Lippenbewegungen gesehen.“

Die Szene aus dem Science-Fiction-Film „2001: Odyssee im Weltraum“ aus dem Jahr 1968 zeigt die Angst des Menschen vor der Maschine, die sich gegen ihre Schöpfer wendet. Ein typisches Motiv in Filmen und Serien über künstliche Intelligenz: In „Terminator“ macht sich die KI Skynet selbstständig und baut eine Roboterarmee aus Terminatoren auf, um die Menschheit auszurotten. In „Ex Machina“ gelingt der Androidin Ava schließlich der Ausbruch aus ihrem Gefängnis in die echte Welt.

Im Mittelpunkt von KI in der Popkultur steht die Frage, wie sich eine künstliche Intelligenz unter Kontrolle halten lässt. Aber sind Horrorszenarien einer Roboterarmee, die die Weltherrschaft übernehmen will, realistisch? Die kurze Antwort ist: Nein. Die lange: Es ist kompliziert.

Doch erst mal zum Ursprung der KI: Eine künstliche Intelligenz ist eine selbstlernende Maschine, deren Algorithmen in der Lage sind, Aufgaben auf eigenständige Weise auszuführen. Wissenschaftler arbeiten seit den 1950er-Jahren daran. Lange tat sich wenig, doch in den letzten Jahren ging es mit den sogenannten neuronalen Netzen, die das menschliche Gehirn nachempfinden und eigenständig lernen, auf einmal rasant vorwärts. So schlug die KI AlphaGo im Frühjahr 2016 den Südkoreaner Lee Sedol, einen der besten Spieler der Welt, im asiatischen Brettspiel Go in fünf Partien vier zu eins. Weil es im Go selbst für einen Computer enorm viele potenziell sinnvolle Züge gibt, musste die KI für das Spiel eine Intuition entwickeln, der sie bei den Spielzügen folgt – genau wie wir Menschen das auch tun.

AlphaGo ist dennoch nur eine sogenannte schwache KI. Sie kann eine Sache ziemlich gut, sogar besser als ein Mensch. Aber sobald sie nicht Go, sondern Schach spielen soll, muss sie wieder von vorn anfangen. Wissenschaftler in aller Welt arbeiten aber auch an sogenannter starker KI, und die könnte für den Menschen tatsächlich potenziell gefährlich sein. Denn sie wäre auf vielen Gebieten so gut wie ein Mensch – oder sogar besser. Eine starke KI aber, die so schlau ist wie ein Mensch, könnte anfangen, sich selbst immer weiter zu verbessern. Es kommt zu einer Intelligenzexplosion, und eine Superintelligenz entsteht, für die wir Menschen vermutlich ungefähr so schlau wären wie Insekten für uns.

Die möglichen Szenarien, die sich daraus ergeben könnten, sind vielfältig: Die Superintelligenz könnte unsere Zivilisation

auf neue Höhen heben. Sie könnte von sich aus eine Art wohlwollender Diktator im Hintergrund sein, sie könnte aber auch in ihrem Handlungsspielraum von uns so eingeschränkt werden, dass sie zwar in ihren Fähigkeiten allmächtig ist, aber keinen freien Willen hat – quasi ein versklavter Gott. Oder sie ist ein Eroberer, der beschließt, dass die Menschheit eine Bedrohung ist, und sie deswegen auslöscht.

Der MIT-Professor Max Tegmark teilt Expertenmeinungen zum Thema KI in drei Gruppen ein: digitale Utopisten, Technoskeptiker und die Nutzbringende-KI-Bewegung. Letztere repräsentiert den Mainstream, darunter sind bekannte Persönlichkeiten wie der vor Kurzem verstorbene Stephen Hawking oder Tesla-Chef Elon Musk. Sie gehen davon aus, dass KI große Chancen, aber vor allem auch große Risiken für die Menschheit mit sich bringt. Deswegen plädieren sie für verstärkte KI-Sicherheitsforschung zum Beispiel im Bereich selbstfahrender Autos sowie zu einem möglichen Verbot autonomer Waffen. MIT-Professor Tegmark verweist dabei darauf, dass eine KI uns vermutlich nicht vorsätzlich etwas Böses antun will, sondern einfach nur sehr kompetent und effektiv ein Ziel verfolgen wird und so der Menschheit schaden könnte. „Sie sind wahrscheinlich kein fieser Ameisenhasser, aber wenn Sie ein Wasserkraftwerk bauen wollen und in einem zu flutenden Gebiet ein Ameisenhaufen liegt, haben die Insekten Pech gehabt. Ein Kernziel der KI-Sicherheitsforschung ist es, die Menschheit niemals in die Position dieser Ameisen kommen zu lassen."

Die digitalen Utopisten halten sich ungern mit solchen Bedenken auf, denn sie sind sich sicher, dass die Menschheit mit KI die nächste Stufe der Evolution erklimmen wird. Facebook-Chef Zuckerberg warnt, sich nicht von Horrorszenarien abschrecken zu lassen, und rät, sich auf den Fortschritt zu konzentrieren, den die KI dem Menschen bringen könnte. „Wer gegen KI ist, muss auch Verantwortung für jeden Tag übernehmen, an dem wir keine Heilung für eine bestimmte Krankheit oder sichere autonome Autos haben." Auch für den ehemaligen Google-Chef Eric Schmidt überwiegen klar die Vorteile: „Hätte man das Telefon nicht erfinden sollen, nur weil es von bösen Menschen benutzt werden kann? Nein, man erfindet das Telefon dennoch und sucht nach Wegen, wie man den Missbrauch unterbinden kann."

> Heute arbeiten Wissenschaftler daran, dass aus Menschen keine Ameisen werden

Die Technoskeptiker halten die übertriebene Angst vor KI ebenfalls für unnötig – aber aus einem ganz anderen Grund. Sie schätzen den technischen Fortschritt weniger optimistisch ein und gehen nicht davon aus, dass es noch in diesem Jahrhundert eine Superintelligenz geben wird. „Das Auftauchen von Killerrobotern zu fürchten kommt der Angst vor einer Überbevölkerung auf dem Mars gleich", betonte etwa Andrew Ng, ehemaliger wissenschaftlicher Leiter der chinesischen Suchmaschine Baidu. „Ich kann sagen: Künstliche Intelligenz wird viele Branchen verändern. Aber sie ist keine Magie."

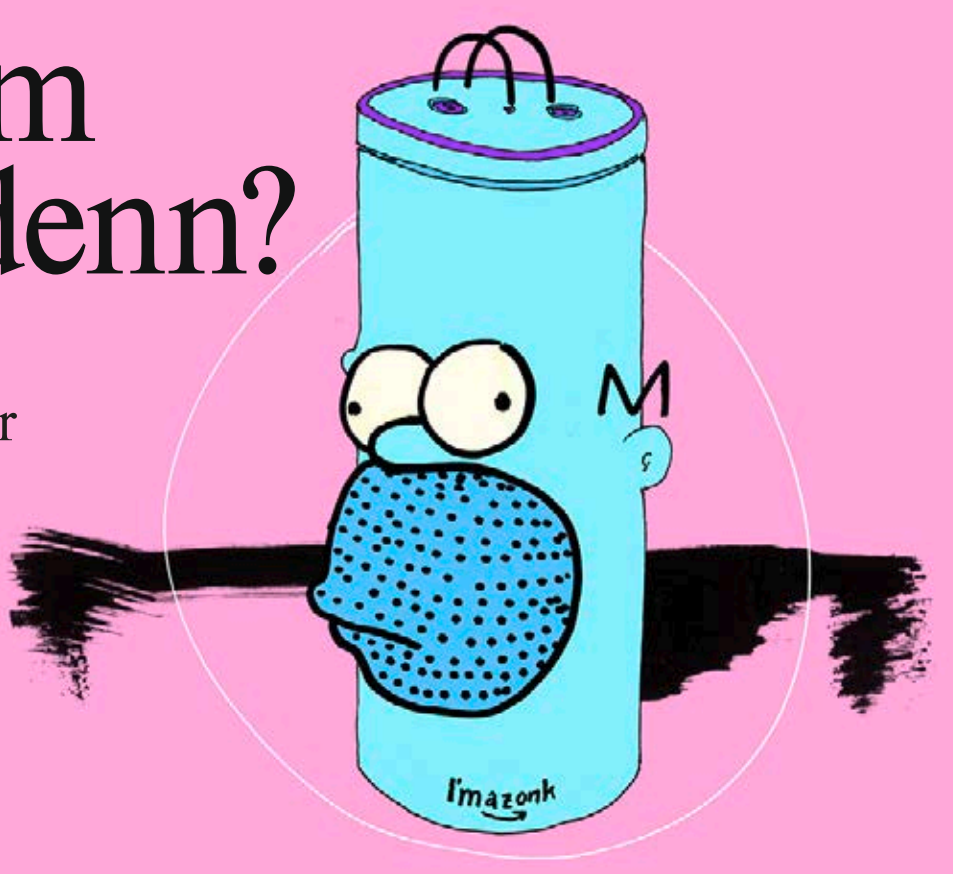
Was KI der Menschheit bringen wird, ist also unklar. Nur eines ist sicher: Die Umwälzungen für unsere Gesellschaft werden gravierend sein. Denn auch wenn keine Superintelligenz entsteht, wird KI die Arbeitswelt und unseren Alltag umkrempeln. Autonome Autos könnten Taxifahrer überflüssig machen, Finanzalgorithmen ersetzen Börsenhändler, Landwirtschaftsroboter übernehmen die Arbeit von Bauern. Ein Viertel aller Jobs könnte bis 2025 wegfallen beziehungsweise von Software und Robotern übernommen werden, so eine Schätzung. Ob auch neue Arbeitsplätze entstehen, wie es bisher bei jeder Revolution der Wirtschaft der Fall war, ist ungewiss. Auch ohne Superintelligenz steht die Menschheit vor einer großen Herausforderung: Was wollen wir in Zukunft selbst tun, und was überlassen wir den Maschinen? ←

Netzrebellen, Teil 3: Aaron Swartz

Aaron Swartz galt als riesiges Hackertalent. Mit 14 Jahren war er an der Entwicklung des RSS-Protokolls beteiligt (RSS ist eine Technologie zum Abonnieren von Webseiten-Inhalten). Später gründete er eine Firma und wurde zum Vorkämpfer für Informationsfreiheit. In seinem „Guerilla Open Access Manifesto" warb er für das Teilen von Wissen als moralische Notwendigkeit, etwa den Zugang zu wissenschaftlichen Arbeiten mit anderen zu teilen. Er lud Millionen kostenpflichtige akademische Artikel illegal herunter. Weil ihm vorgeworfen wurde, die Artikel in Tauschbörsen einstellen zu wollen, wurde er angeklagt. Ihm drohten Jahrzehnte Haft. Swartz, der bereits seit Jahren depressiv war, nahm sich vor Beginn des Prozesses das Leben. Er wurde 26 Jahre alt.

Wie dumm ist das denn?

So schlau sind Computer auch wieder nicht. Ein paar Anekdoten zum Thema künstliche Dummheit



1 Der US-Konzern Microsoft wollte 2016 zeigen, wie clever lernende Systeme sein können – stattdessen bewies er mit seinem Twitter-Bot „Tay“ unfreiwillig das Gegenteil. Die ursprüngliche Idee war, dass der Bot durch Chats mit anderen Usern dazulernt. Je mehr er mit anderen interagiert, desto mehr kann er sich abschauen und desto schlauer wird er. Das war die Theorie. Letztlich dauerte es aber weniger als 24 Stunden, bis „Tay“ zur Rassismusschleuder wurde. „Hitler was right I hate the jews“, twitterte der Bot, leugnete den Holocaust und verbreitete Verschwörungstheorien zu den Terroranschlägen auf das World Trade Center in New York. Microsoft schaltete den Bot schnell wieder ab.

2 Der Hautarzt Roberto Novoa baute kürzlich mit Kollegen an der US-amerikanischen Uni Stanford einen Algorithmus, der mithilfe einer Datenbank aus 129.000 Bildern von Hautveränderungen automatisch erkennen sollte, welche davon gutartig und welche gefährliche Tumore sind. Das Problem dabei: Bei besorgniserregenden Hautveränderungen legen Dermatologen oft ein Lineal mit ins Foto, um deren Größe zu dokumentieren. Das führte dazu, dass der Algorithmus auf Bildern immer dann Tumore erkannte, wenn im Bild ein Lineal zu sehen war – weil dessen Vorhandensein mit einer größeren Wahrscheinlichkeit einherging, dass es sich um krebsartige Veränderungen handelte. Immerhin hatte Novoa also ein Erkennungswerkzeug für Lineale gebaut.

3 Forscher am MIT Lincoln Lab testeten 2013 ein Computerprogramm, das lernen sollte, eine Liste von Nummern zu sortieren. Es erreichte schließlich tatsächlich einen perfekten Score. Um das zu schaffen, löschte das Programm einfach die Liste. Das entsprach den Anforderungen, wenn auch nicht ganz wie gedacht: Keine Nummern mehr, keine Unordnung.

4 So ein großes Universum und kaum Zeit, es sich genau anzuschauen. Ein NASA-Forscherteam berichtete 2017 von einem Deep-Learning-Programm, das Sonnenstürme auf Bildern erkennen sollte. Das genaueste Programm war letztlich eines, das grundsätzlich anzeigte, dass auf einem Bild kein Sonnensturm zu sehen ist. Starke Sonnenstürme sind nämlich sehr selten.

5 „Alexa, kauf mir ein Puppenhaus!“ Eine Sechsjährige in den USA bestellte im vergangenen Jahr per Sprachsteuerung von Amazon Echo neues Spielzeug. Das ärgerte ihre Eltern, und der örtliche Lokalsender in San Diego berichtete darüber. Blöd nur, dass der Reporter die Worte des Kindes live wiederholte. Das aktivierte nämlich bei zahlreichen Zuschauern die Sprachsteuerung von Amazon Echo und löste ungewöhnlich viele Bestellungen von Puppenhäusern im Raum San Diego aus.

6 Sicherheit? Kann man auch mit Robotern machen, dachte sich im vergangenen Jahr eine Sicherheitsfirma in Washington, D.C.. Sie ließ einen Sicherheitsroboter durch ein Bürogebäude patrouillieren, angelehnt ans Äußere des „Star Wars“-Droiden R2D2, aber bestückt mit Kamera und Sensoren. Offenbar gefiel dem Roboter sein Dasein jedoch nicht: Er ertränkte sich in dem Brunnen im Foyer. Ein weiteres Modell des Roboters hatte 2016 in einer Einkaufsmall bereits ein 16 Monate altes Kind umgefahren – und hielt danach nicht einmal an. ←

Von Arne Semsrott

Vienna calling

Wien ist schon lange ziemlich smart, auch ohne das Label von der „Smart City“. Vielleicht sollte man daher auch dort schauen, wie Daten Städte noch lebenswerter machen können

Von Lisa Neal

Durch Datensammeln und Technologie eine Stadt lebenswerter zu machen - das versteht man gemeinhin unter dem Begriff Smart City. Klug ist aber auch, Kultur und bezahlbaren Wohnraum anzubieten

→ Es gibt zwei Arten, zu erfahren, was Menschen in einer Stadt so machen. Man kann möglichst viele Kameras an Fassaden schrauben und überall Sensoren installieren, die das Leben aufzeichnen – man kann aber auch einfach mal mit den Menschen sprechen.

In Wien spricht man sehr gern, sowohl miteinander als auch übereinander: Der Wiener Schmäh hat es sogar zum weltbekannten österreichischen Kulturgut geschafft. Dabei ist das Gesagte nicht ganz ernst gemeint, aber eben doch ein bisschen.

Auch die Stadt spricht mit den Bürgern. Unter dem Motto „Wohnpartner unterwegs“ fahren Mitarbeiter der Stadtverwaltung mit dem Rad herum, um die Menschen in den städtischen Wohnungen nach ihren Problemen zu fragen. Wo fehlt es an Möglichkeiten für Jugendliche, sich zu treffen, wie läuft das neue Nachhilfeangebot, und wird das neue Hofcafé auch wirklich genutzt? Auch mithilfe der App „Sag’s Wien“ kann man jederzeit Wünsche und Klagen loswerden. Und auf die Mülleimer hat man in Wien Telefonnummern geklebt. Falls mal einer zu sehr stinkt.

Was Wien macht, läuft anderswo unter dem Label Smart City: Daten sammeln und dadurch die Stadt lebenswerter machen. „Ich war neulich wieder auf einer Veranstaltung zu dem Thema, und alle sprachen ständig nur von Nutzern. Für mich aber geht es um Bürger. Das Soziale ist wichtiger als die Effizienz“, sagt Thomas Madreiter, sogenannter Planungsdirektor der Stadt. Wien will nicht nur Daten von den Bürgern, sondern gibt ihnen selbst welche. Im Rahmen der Open Data Initiative können Bürger auf einer Website alle möglichen Zahlen zum Leben in der Stadt abrufen.

Das angesehene Nachrichtenmagazin „The Economist“ kürte Wien gerade zur lebenswertesten Stadt der Welt. Für das Ranking wurden 140 Großstädte nach Kriterien wie Infrastruktur, Bildung, Gesundheitsversorgung und Kultur miteinander verglichen. Besonders gut gefällt es den Zuge-

zogenen in der Stadt, die für internationale Unternehmen oder die UNO arbeiten. Seit dem Ende des Kalten Krieges ist Wien von der morbiden Metropole am Rande des Ostblocks zu einer beliebten Großstadt mitten in Europa geworden, die mit vielen Freizeit- und Kultureinrichtungen gerade junge Menschen anzieht, seien es Studenten oder Mitarbeiter von Start-ups.

Noch entscheidender ist allerdings, dass Wiens Einwohner derzeit weniger mit steigenden Mieten und Gentrifizierung zu kämpfen haben als in vielen anderen europäischen Metropolen, wo statt Sozialwohnungen vor allem teure Apartments für eine internationale Kundschaft entstanden sind. In Wien gibt es 220.000 städtische Wohnungen, das ist gemessen an der Gesamtzahl ein Spitzenwert. Der derzeitige Wiener Bürgermeister Michael Ludwig hat bereits als Wohnbaustadtrat erfolgreich dafür gekämpft, dass die Stadt ihren großen Bestand an kommunalen Wohnungen nicht an private Investoren verkauft – wie es etwa in Berlin passiert ist, wo heute 310.000 bezahlbare Wohnungen fehlen.

„Von der Wiege bis zur Bahre" wolle sich die Wiener Stadtregierung um die Bürger kümmern, das versprach sie bereits vor 100 Jahren – ein Leitsatz, der die Kommunalpolitik bis heute prägt und die Bürger anspruchsvoll gemacht hat. „Die Wiener glauben, dass ihnen Genuss und Lebensqualität einfach zustehen", sagt Lukas Franta von der TU Wien. Allerdings seien für den Erhalt einer lebenswerten Stadt nicht nur die Politiker, sondern auch die Bürger wichtig. Sie sollten ihre Stadt mitgestalten und sich einbringen, so Franta. „Sonst verliert die Stadt das, was sie in den letzten hundert Jahren ausgemacht hat. Diese fast schon übereifrige soziale Organisation." Tatsächlich wohnt jeder vierte Wiener in einer Wohnung, die ihm die Stadt vermietet, insgesamt sind das 500.000 Menschen.

Allein im 22. Bezirk der Donaustadt entstanden von 1973 bis 1977 in der Siedlung Trabrenngründe mehr als 2.400 Wohnungen in 59 Häusern. Anfangs sah es so aus, als würde der größten Anlage von Gemeindebauten das Schicksal vieler Hochhaussiedlungen drohen, also hohe Kriminalität und die niederdrückende Anonymität einer Schlafstadt. Aber durch kluges Stadtteilmanagement wurde gegengesteuert. Heute gibt es in der meistens nur kurz Rennbahnweg genannten Siedlung viele Schulen und Kindergärten, Sportflächen und Geschäfte. Die meisten Anwohner fühlen sich wohl.

Fast 50 Jahre später ist es nun wieder der Bezirk Donaustadt, wo die Stadt Wien die Zukunft des Zusammenlebens ausprobiert. In der sogenannten Seestadt Aspern entsteht bis 2028 ein ganzer Stadtteil – mit 10.500 Wohnungen für 20.000 Menschen, dazu Büro- und Ladenflächen, damit dort auch tagsüber Leben ist – und nicht nur, wenn die Menschen von der Arbeit nach Hause kommen.

Und hier findet tatsächlich vieles statt, was unter dem Begriff Smart City zusammengefasst wird: Die energiesparenden Häuser werden ressourcenschonend gebaut, die Sensoren in den Häusern sollen die Wassernutzung messen, den Stromverbrauch und den Kohlendioxidgehalt in der Luft. Zuständig ist „Aspern Smart City Research", ein Gemeinschaftsunternehmen der Stadt Wien und Siemens. Eine sogenannte Public-private-Partnership – also eine jener Kooperationen von öffentlichen Institutionen und Konzernen, die oft dafür kritisiert werden, dass die Unternehmen mit Steuergeld ihre Ziele vorantreiben. Und gerade das Konzept der Smart City wirft die Frage auf, wem die erhobenen Daten gehören. In Aspern sollen sie den Bürgern gehören. Ob das wirklich so kommt, bleibt abzuwarten, schließlich sind die Daten der Mieter viel Geld wert. Wer sie freiwillig teilt, könnte irgendwann finanziell dafür belohnt werden.

Die Seestadt ist an den ziemlich günstigen Nahverkehr mit U- und Straßenbahn angebunden, eine App zur Parkplatzsuche soll es in Wien nicht geben, schließlich will man den privaten Autoverkehr langfristig komplett abschaffen.

Eines der bereits fertigen Häuser dort ist das Technologiezentrum Seestadt, dessen Fassaden begrünt werden können, auf dessen Dach Solarzellen installiert sind und bei dem sogar die Wärme aus den Serverräumen der Firmen für die Raumkonditionierung genutzt werden soll. Wenn es gut läuft, produziert das Haus am Ende mehr Strom, als es verbraucht. Ein anderes Vorzeigeprojekt im Viertel ist das höchste Holzhochhaus der Welt (84 Meter), bei dessen Bau durch den weitgehenden Verzicht auf Stahl und Beton 2.800 Tonnen CO_2 gespart werden sollen.

Die Hälfte der Flächen in der Seestadt soll öffentlicher Raum bleiben; breite Gehsteige sind geplant, Stationen für Leihräder, geteilte Garagen, Plätze, auf denen man sich gern aufhält. Denn auch im neuen Viertel geht es im Grunde genommen um eine uralte Aufgabe der Stadtpolitik. „Die Frage nach der Smart City ist nur scheinbar eine technische", so Planungsdirektor Madreiter. „In Wahrheit ist es die Frage, wie wir das soziale Zusammenleben organisieren." ←

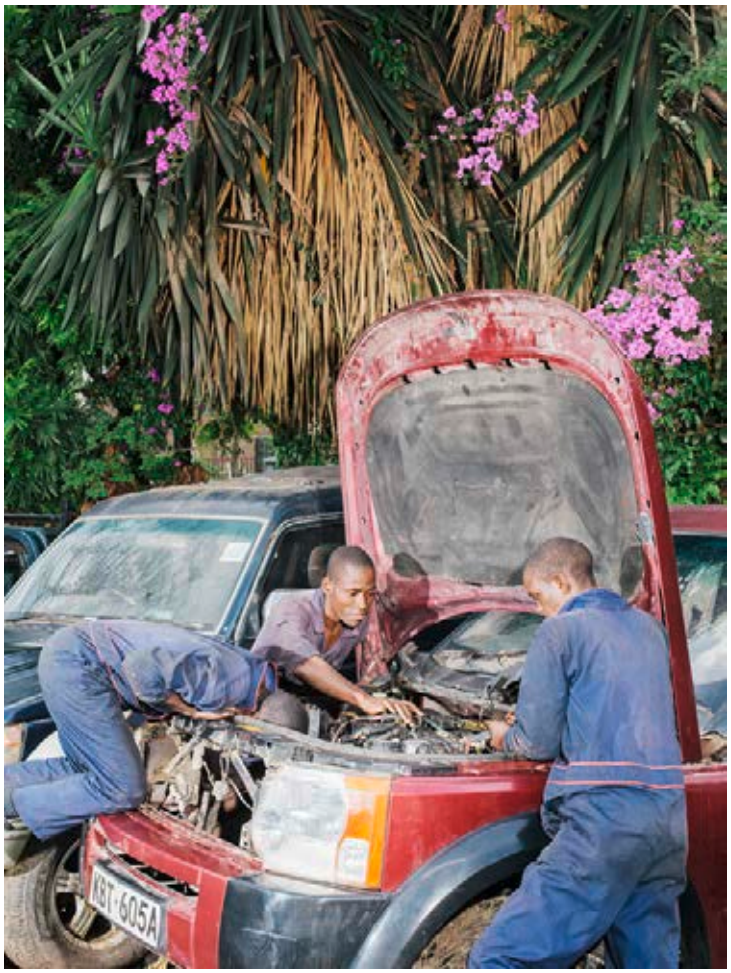
„In Wahrheit geht es um die Frage, wie wir sozial zusammenleben"

Silicon Savannah


hp

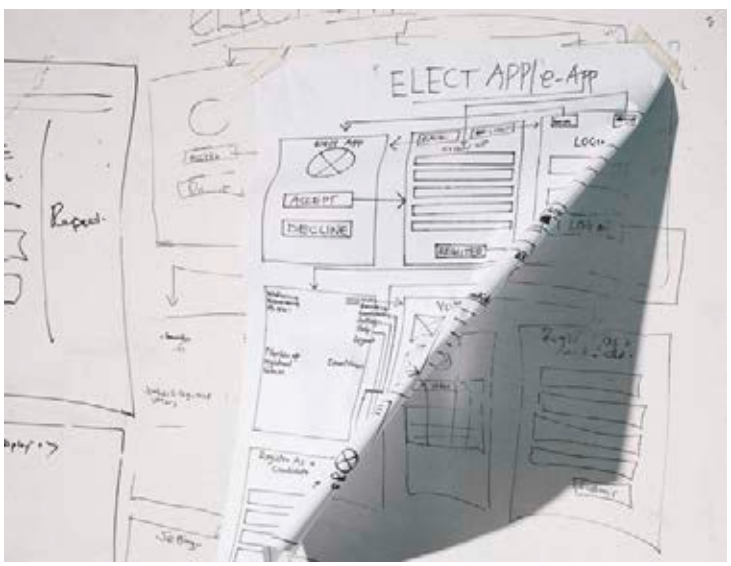
Wenn es um das Internet geht, ist das Klischee von Afrika als unterentwickelter Kontinent besonders unzutreffend. Seit Kenia über Seekabel an das weltweite Breitbandnetz angeschlossen ist, boomt dort die Start-up-Szene. Der Fotograf Janek Stroisch hat eine junge Generation beim Aufbruch in die digitale Zukunft begleitet

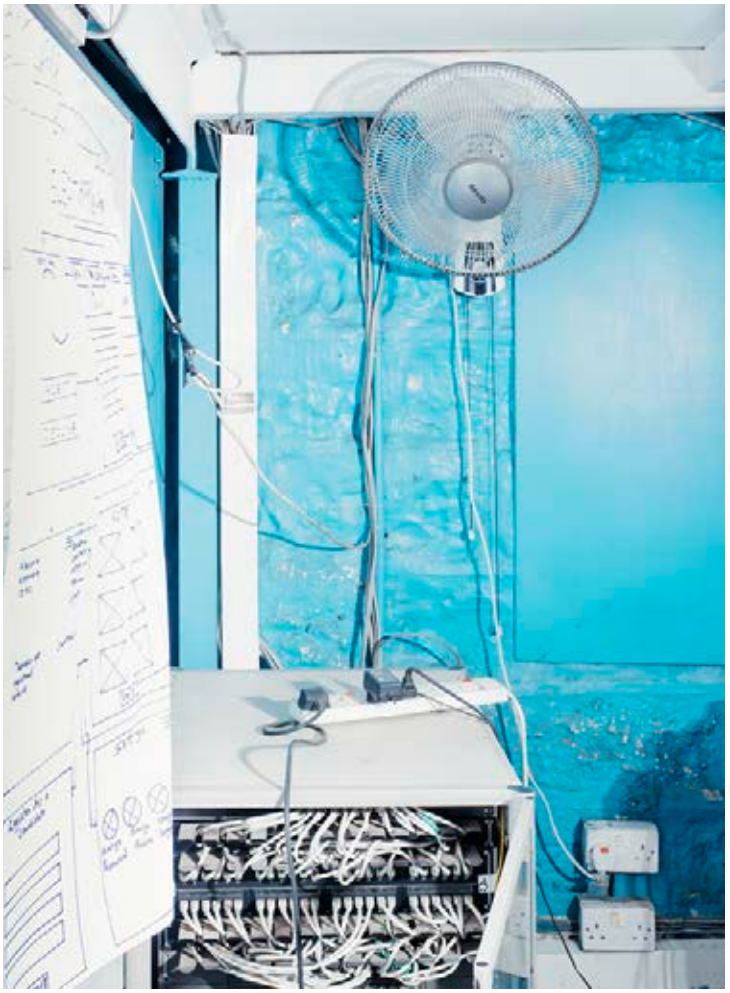
Hashimalle Mustafa ist Schüler bei „Nairobits" – einem Programm, in dem Jugendliche aus weniger privilegierten Stadtteilen von Nairobi Programmierung und Webdevelopment lernen



Tüftler und Schrauber: Das Start-up AB3D bastelt aus Elektroschrott 3-D-Drucker. An Autos schrauben die Mitarbeiter aber auch gern rum

Fast 18 Millionen Menschen (von circa 49 Millionen) verfügen in Kenia bereits über einen Breitbandanschluss





Um die Demokratie im Land zu stärken, haben junge Softwareentwickler eine Wahl-App erdacht

Du kriegst nichts mehr

Daten sammeln und damit das Verhalten von Menschen vorhersagen – das gibt es nicht erst seit Facebook, Google & Co. Unseren Autor hat seine Schufa-Auskunft fast die Wohnung gekostet

Von Niklas Prenzel

→ Es ist einer dieser ersten Frühsommertage im Mai. Ich habe beruflich in Köln zu tun. Kurz vor meiner Abreise war ich noch durch meine Berliner WG gehastet, hatte den Koffer gepackt – und die Zahnbürste vergessen. Das fällt mir erst in Köln auf. In einer Drogerie kaufe ich Zahnpasta, Zahnbürste und eine Cola, alles für 3,63 Euro. Auf dem EC-Terminal erscheint um 11:17 Uhr die Mitteilung: „Zahlung erfolgt". Bald wird die Schutzgemeinschaft für allgemeine Kreditsicherung, kurz: Schufa, von diesem Einkauf erfahren. Und sie wird Vermietern und Telefonanbietern raten, mir lieber nicht mehr zu vertrauen. Aber das ahne ich noch nicht.

Das Geschäftsmodell der Schufa, 1927 in Berlin entstanden, ist einfach: Sie sammelt Daten über Zahlungsvorgänge und teilt Unternehmen mit, wer aus ihrer Sicht als Kunde und Geschäftspartner taugt – und wer nicht. Dafür bekommt die Schufa Informationen von ihren Partnern – Tausenden Banken und Unternehmen – über Telefonverträge, Kredite, Bankkonten, aber auch über Insolvenzverfahren oder Mahnungen. Außerdem kennt sie Namen, Geschlecht, Wohnort und Alter von 67,5 Millionen Personen in Deutschland, über die sie Daten gespeichert hat. Ein Algorithmus berechnet schließlich aus vielen dieser Informationen den sogenannten Schufa-Score – eine Art Schulnote, die aussagt, wie wahrscheinlich es ist, dass ein Kunde die Raten für den Flachbildfernseher nicht pünktlich bezahlt. Oder ein Konto überzieht. Grundsätzlich eine gute Idee: So muss nicht jedes Unternehmen selbst überprüfen, wem es vertrauen kann, und die Kunden bekommen schnell ihren Kredit, den Mobilfunkvertrag oder eine Wohnung. Nur ist der Algorithmus der Schufa geheim. Ob er eine Person richtig eingeschätzt hat, kann man als Außenstehender kaum nachvollziehen.

Das sei auch okay so, denn es sei ihr Geschäftsgeheimnis, urteilte der Bundesgerichtshof. Die neue Datenschutzgrundverordnung könnte das aber vielleicht ändern. Denn bei automatisierten Entscheidungen müssen Unternehmen jetzt erklären, wie sie zustande kommen – nur so lasse sich nachvollziehen, ob die Entscheidung korrekt war. Ob das auch für die Schufa gilt, ist unter Experten umstritten.

Wie schlecht es um mich steht, erfahre ich erst, als ich einige Monate später im kargen gläsernen Büro einer Postbank sitze, bei der man eine Schufa-Auskunft erhalten kann. Die brauche ich, weil mir eine Wohnungsgesellschaft eine 1,5-Zimmer-Wohnung angeboten hat. Sie braucht aber noch meine Schufa-Auskunft. Auf den angespannten Wohnungsmärkten der Großstädte überbieten sich mittlerweile Mieter mit Vertrauensbeweisen: eindrucksvolle Gehaltsnachweise, vorbildliche Lebensläufe und – fast das Wichtigste – positive Schufa-Auskünfte.

Als der Mitarbeiter der Postbank zum Drucker geht, pfeift er. Er hat gute Laune, weil wir uns beim Warten auf die Schufa-Daten Witze erzählt haben. Dann blättert er die frisch ausge-

druckten Seiten durch. Wie ein Arzt, der dem Patienten den nahen Tod verkündet, sagt er: „Sehr kritisches Risiko. Das tut mir leid.“ Tatsächlich: Der Algorithmus der Schufa sieht in mir einen unzuverlässigen Geschäftspartner. Angeblich schulde ich einem Unternehmen 103,63 Euro. „Zahlungsausfall“ – so steht es in meiner Akte.

Hatte ich wirklich Briefe mit Mahnungen übersehen? Hatte jemand online meine Identität geklaut? Den Abend nutze ich, um mich gedanklich von meiner neuen Wohnung zu verabschieden – und mich über die Schufa zu informieren. Ich lese von Daten- und Verbraucherschützern, die einen Algorithmen-TÜV und bessere staatliche Prüfverfahren fordern. Ich lese über die „OpenSchufa“-Initiative, der man seine Schufa-Daten spenden soll, damit sie den Algorithmus rekonstruieren kann.

„Wir schaffen Vertrauen“ – das ist der Slogan der Schufa. Mein Vertrauen ist jedoch erschüttert. Die Gutachten von Universitäten, die den Algorithmus beurteilen sollen, werden oft nicht von staatlichen Datenschutzbehörden beauftragt, sondern von der Schufa selbst. Eher beunruhigt lese ich, dass laut einer Studie der schleswig-holsteinischen Datenschutzbehörde etwa jeder dritte Befragte die eigene Schufa-Auskunft als fehlerhaft bewertet. Und immer mal wieder bekommt der Schufa-Algorithmus falsche Informationen gemeldet, oder er verwechselt zwei Namensvetter miteinander. Das sind aber Ausnahmen. Ansonsten scheint die Schufa vollkommen gesetzeskonform zu handeln – im Rahmen des Datenschutzes.

Ich sitze in meinem WG-Zimmer und denke an die mehr als sechs Millionen anderen, die ebenfalls einen negativen Schufa-Eintrag haben. Und dass es ja eigentlich gut ist, dass jemand für Vertrauen zwischen Geschäftspartnern sorgt. Aber auch komisch ist, dass es ein Unternehmen gibt, das viele

Ich habe laut Akte über 100 Euro Schulden und weiß nicht, warum

für eine Behörde halten und das eine so große Macht über das Schicksal zahlreicher Menschen hat.

Am Ende tue ich das, was man auch im Jahr 2018 immer noch macht, wenn es ernst wird: Ich schreibe Briefe. Der erste geht an die OpenSchufa-Initiative, der ich eine Kopie meiner Schufa-Auskunft spende. Im zweiten flehe ich: Mein angeblicher Gläubiger, ein großes Inkassounternehmen, soll mir sagen, wofür ich ihm 103 Euro schulde. Ich zahle gern. Wenn nur der Eintrag aus meiner Schufa-Akte gelöscht wird.

Eine Woche später meldet sich das Inkassounternehmen zurück. Es habe meine Adresse falsch ermittelt, daher hätten mich die Mahnungen nicht erreicht. Es tue ihnen leid. Selbstverständlich würden sie den Eintrag bei der Schufa löschen lassen. Die Kosten dafür müsse ich auch nicht tragen. Die Forderung hatte sich aus rund 100 Euro für die Rechtsanwälte und Mahnungen sowie 3,63 Euro Forderung einer Drogerie zusammengesetzt. Die konnten damals, im Mai in Köln, nicht abgebucht werden. Warum? Das war wiederum mein Fehler: Ich hatte aus Routine mit der EC-Karte gezahlt, die zu dem Konto gehörte, das ich wenige Tage nach dem Drogerieeinkauf kündigte. Der Schufa-Algorithmus glaubte wohl, dass ich die 3,63 Euro mit einer falschen EC-Karte bezahlt hatte.

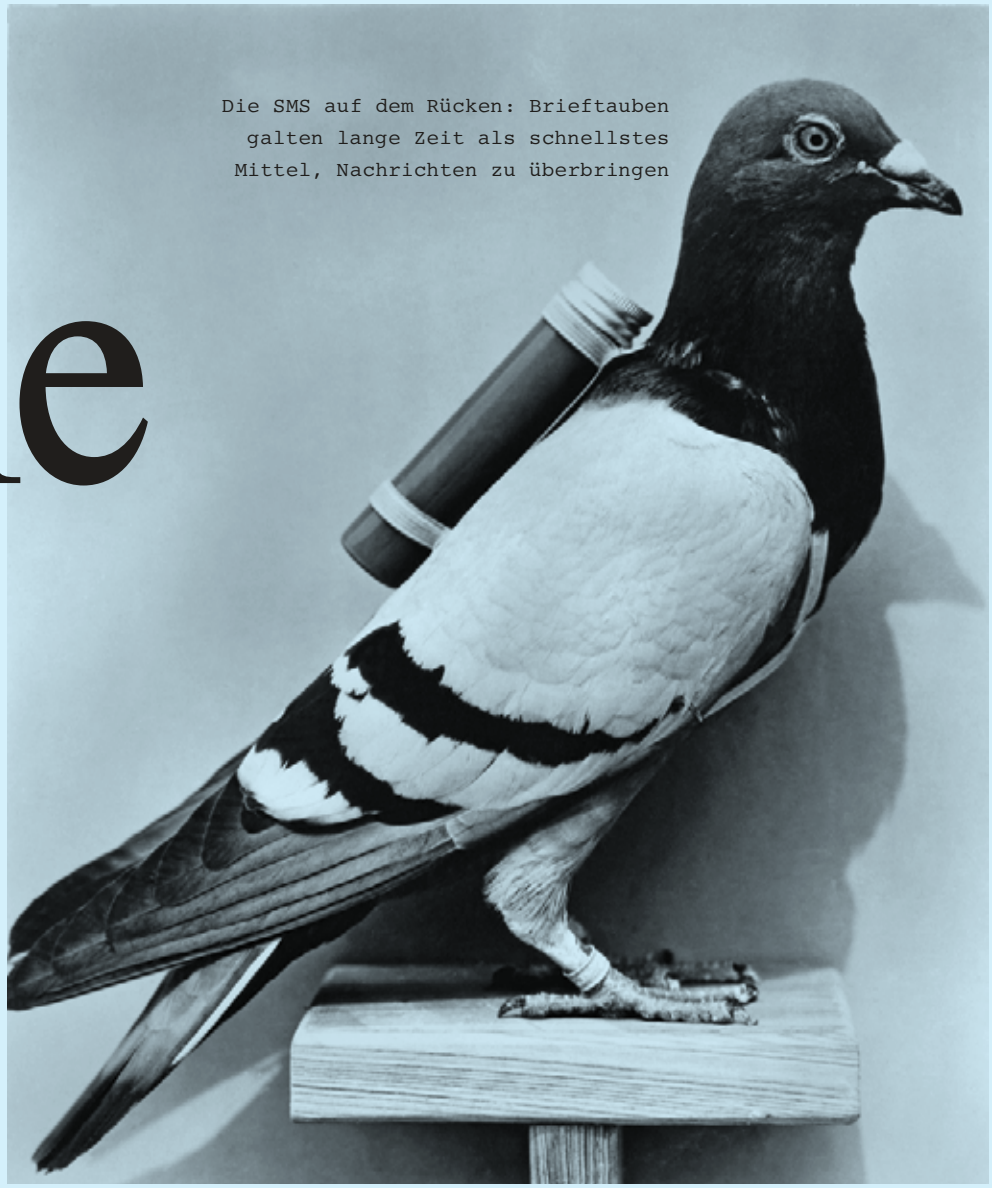
Ich hatte Glück. Ein Fehler, den man entdeckt und nachweisen kann, wird schnell gelöscht. Bei einem berechtigten Eintrag vergisst die Schufa erst drei Jahre nach dem Begleichen der Schulden.

Einige Tage danach unterschreibe ich den Mietvertrag für die neue Wohnung, obwohl ich noch gar keinen neuen Schufa-Score vorzeigen kann. Die Hausverwalterin hat früher in einer Bank gearbeitet und kennt sich mit diesen Auskünften aus. Sie findet, dass mein Schufa-Eintrag nicht der Rede wert sei. „Das kann ja jedem mal passieren“, sagt sie. ←

Netzrebellen, Teil 4: Chelsea Manning

„Lady Gaga“ schrieb Bradley Edward Manning auf die CD, die Hunderttausende militärische Dokumente beinhaltete. Als Soldat mit „Top Secret“-Zugang hatte er die Daten im Irak heruntergeladen. 2010 veröffentlichte WikiLeaks die Dokumente, die Auskunft über die US-Militäreinsätze in Afghanistan und Irak gaben. Für einen weltweiten Aufschrei sorgte zum Beispiel ein Video, das zeigt, wie aus einem US-Kampfhubschrauber heraus ein Dutzend Zivilisten inklusive zweier Journalisten erschossen werden. Manning wollte zeigen, welche „Fehltritte wir im Irak begehen“ und wurde dafür zu 35 Jahren Haft verurteilt. Ein Jahr später ließ Barack Obama die Truppen aus dem Irak abziehen. 2013 erklärte Manning, sich seit der Kindheit als Frau zu fühlen, 2014 benannte er sich um in Chelsea Elizabeth. Nach einem fünftägigen Hungerstreik im September 2016 bewilligte man ihm eine geschlechtsangleichende Operation. Als die Whistleblowerin im Mai 2017 begnadigt wurde, twitterte Donald Trump, dass die undankbare Verräterin niemals hätte entlassen werden dürfen.

Der Wille zur



Die SMS auf dem Rücken: Brieftauben galten lange Zeit als schnellstes Mittel, Nachrichten zu überbringen

Die analoge Vorgeschichte unserer digitalen Gegenwart ist lang und lehrreich. Wir sollten sie im Kopf haben, wenn wir unsere Rechner hochfahren

Von
Arno Frank

→ Auf die Vergangenheit blicken viele moderne Menschen mit einer Mischung aus Arroganz und Mitleid. Wir können uns heute kaum mehr vorstellen, wie wir unseren Alltag „vor dem Internet“ bewältigt haben. Wie Menschen kommunizierten, Handel trieben, Nachrichten empfingen.

Tatsächlich beginnt der Wille zur Vernetzung im Kern mit dem Wunsch des Menschen, über weite Distanzen wichtige Nachrichten immer schneller auszutauschen. Jeder einzelne Aspekt des Internets, wie wir es kennen und nutzen, hat seine exakten Vorläufer in der Geschichte – Techniken, die zum Teil heute noch im Einsatz sind und deren einziger Unterschied zur modernen Datenübermittlung darin besteht, dass sie nicht digital sind.

In prähistorischen Zeiten erfanden Ureinwohner des afrikanischen Dschungels die Nachrichtentrommel. Sie diente zur Übermittlung von Botschaften, z.B. Warnungen. Diese konnten bis zu acht Kilomter weit gesendet werden. Dabei galten Dörfer als „Knotenpunkte“ mit eigenen „IP-Adressen“ in Form spezieller rhythmischer Figuren.

Als erster „Rechner“ im Sinne einer Maschine, die in kontinuierlicher Verschiebung unterschiedliche Größen zueinander in Verhältnis setzt, gilt der rätselhafte Mechanismus von Antikythera. Das Gerät wurde 1901 vor einer griechischen

Vernetzung

Insel aus dem Wrack eines antiken Frachters geborgen, es ist mindestens 2.000 Jahre alt und gibt, betrieben mit einer Handkurbel, über zahlreiche Zahnräder und ein hochkomplexes Federwerk kalendarische und astronomische Zusammenhänge an.

Im Römischen Kaiserreich sorgte auf einem Territorium von mehreren Millionen Quadratkilometern ein dichtes Netz aus „Poststationen“ für die Übermittlung von Nachrichten. Der Clou dieses „cursus publicus“ war, dass an den Stationen nicht die Kuriere wechselten, sondern nur die Pferde – sodass der Empfänger in Rom jenen Boten persönlich befragen konnte, der in Trier oder Antiochia losgeritten war. Wissen und Infrastruktur gingen im Mittelalter verloren, die Bedürfnisse blieben bestehen. Kreuzritter brachten die uralte Tradition der Brieftauben nach Europa zurück, mit deren Hilfe Nachrichten in kürzester Zeit an entfernte Orte gelangten. Eine sehr frühe und sehr primitive Form der SMS.

Mit dem Buchdruck wurde ab 1450 die mönchische Abschrift bestehender Schriften mechanisiert – und das schnelle und einfache „copy and paste“ war in der Welt. Gefolgt von den ersten periodischen Publikationen von Neuigkeiten, die oft durch viele Hände gingen. Der britische Verleger Ichabod Dawks ließ 1669 erstmals Zeitungen zusätzlich mit weißen Bereichen drucken, auf denen „jeder Gentleman seine eigenen Angelegenheiten“ verbreiten konnte. Die lesen sich noch heute wie prototypische Kommentarspalten.

Ein Netz zum Austausch komplexer Nachrichten wie bei den alten Römern kehrte 1791 zurück, als ein französischer Geistlicher den „Schnellschreiber“ (Tachygraf) entwickelte, der bald zum „Fernschreiber“ (Telegraf) umbenannt wurde. Mithilfe schwenkbarer Balken konnten so, von Turm zu Turm mit Fernrohr ablesbar, codierte Meldungen aus 196 verschiedenen Zeichenkombinationen übermittelt werden. Die erste Telegrafenfernlinie reichte bereits 1794 von Paris bis Lille, später überzog ein Netz optischer Telegrafenstationen das ganze französische Kaiserreich.

Militärische Bewegungen oder wirtschaftliche Informationen konnten so in Minutenschnelle übermittelt werden. Weil jeder in der Nähe des Turms die Signale mitschreiben konnte, war diese Leitung nicht „abhörsicher“, und so kam es ab 1834 zum ersten „Hack“ der Weltgeschichte. Wenn die Börsenkurse in Paris stiegen oder fielen, reagierten die Märkte in den Provinzen erst darauf, wenn diese Schwankungen mit entsprechender Verspätung in den Tageszeitungen veröffentlicht worden waren. Das kriminelle Brüderpaar François und Louis Blanc bestach die Beamten, in ihre optischen Codes spezielle Zeichen aufzunehmen, aus denen sie ein Steigen oder Fallen der Kurse ablesen und mit diesem Wissen Insidergeschäfte machen konnten. Die Brüder wurden überführt, konnten aber nicht verurteilt werden. Für diese Art von Kriminalität gab es schlicht noch kein Gesetz. Eine schöne Pointe ist, dass die Brüder mit dem erschummelten Geld im Ausland lukrative Spielbanken gründeten, von Bad Homburg bis Monte Carlo.

Ende des 19. Jahrhunderts war bereits der ganze Planet verkabelt

Zu diesem Zeitpunkt hatte die Technik bereits einen weiteren Sprung getan, die elektrische Telegrafie war erfunden worden. Ende des Jahrhunderts war der komplette Planet „verkabelt“, verbunden durch das erste weltumspannende Netz für Telekommunikation, verlegt von der Eastern Telegraph Company und heute – nur halb im Scherz – „Internet des viktorianischen Zeitalters“ genannt. Diesmal war es das britische Imperium, das seine weltweiten Kolonien sowie diverse andere Länder durch Kupferkabel miteinander verband. Etwa dort, wo die Kabel damals verliefen, liegen heute viele Glasfaserkabel für das Internet.

Als Guglielmo Marconi 1903 in England die Abhörsicherheit der von ihm erfundenen drahtlosen Telegrafie vorführen wollte, mischten sich seltsame Botschaften unter seine Morsezeichen: „Rats!“, also „Ratten!“, gefolgt von Schmähgedichten auf den Erfinder. Sein Konkurrent Nevil Maskelyne hatte, mutmaßlich im Auftrag der Eastern Telegraph Company, Marconis Signale abgefangen und um eigene „Botschaften“ ergänzt – die ersten Spams der Weltgeschichte, wenn man so will.

Die Entschlüsselung der deutschen Chiffriermaschine Enigma durch den englischen Mathematiker Alan Turing gehört, ebenso wie der erste funktionsfähige Rechner von Konrad Zuse, bereits zu den Gründungsmythen der elektronischen Datenverarbeitung in den 1940er-Jahren. Hier ist Computergeschichte bereits Kriegsgeschichte. So nutzten deutsche Panzerflotten beim Überfall auf Frankreich 1940 bereits eine Vorstufe des „automatisierten Fahrens“. Die Panzerfahrer manövrierten ihre Vehikel in unübersichtlichem Terrain nach Anweisungen des Generalstabs, der über Kurzwelle das Fahrzeug lenkte.

Weniger gewürdigt wurden bisher stille Helden wie René Carmille, der im besetzten Frankreich für das Statistische Amt zuständig war – und der Résistance, dem Widerstand gegen die Nazis, zuarbeitete. Über zwei Jahre programmierte Carmille Computer um, mit denen auf modernen Lochkarten biografische Daten erfasst werden sollten – sodass die Spalte, in der „Religionszugehörigkeit“ vermerkt war, frei blieb. Damit rettete er als ethisch motivierter Hacker unzählige französische Juden vor der Deportation in deutsche Vernichtungslager; er selbst starb 1945 in Dachau. ←

fluter.de

Interview mit einem Cleaner

Im Frühjahr kam der vielfach preisgekrönte Dokumentarfilm „The Cleaners“ heraus, über die wenig geschulten Content-Moderatoren, die auf den Philippinen sitzen und soziale Netzwerke wie Facebook von Desinformation, Pornografie und Gewalt befreien sollen – oft anhand recht intransparenter Kriterien. Nach ein paar Monaten, in denen sie mit zahllosen Abbildungen von sexueller Gewalt, Folter und Mord konfrontiert waren, benötigen viele der Moderatoren psychologische Hilfe. Auch in Deutschland durchforsten Content-Moderatoren Facebook nach anstößigen Inhalten und geraten dabei oft an ihre Grenzen. Wir haben mit einer „Cleanerin“ gesprochen.

Lass Daten Taten folgen

Wie unverzichtbar Datenschutz ist, dürfte hier am Heftende bei jedem angekommen sein. Aber wie nun von der Theorie zur Praxis kommen? Was tun, wenn du das Heft zur Seite legst und wieder zum Smartphone oder Laptop greifst? Einige Tipps haben wir schon gegeben, auf fluter.de gibt es noch viel mehr. Da wartet eine ganze Toolbox für den Schutz deiner persönlichen Daten. Mit praktikablen Lösungen für die drängendsten Probleme des Datenalltags: Welchen Browser nutzen, welche Cookies blockieren? Darf ich Privates per Mail verschicken? Und welches Passwort ist wirklich sicher? Zu einem funktionierenden Datenschutz kommt man eben nur Schritt für Schritt – fluter.de zeigt dir die ersten.

Vorschau

Ständig fordert irgendjemand Respekt. Hip-Hopper in ihren Texten, Halbstarke, die sich auf dem Schulhof aufspielen, oder die Eltern. Gleichzeitig wird aber oft ziemlich respektlos miteinander umgegangen, werden Menschen beschimpft oder gar körperlich bedrängt. Auch im Internet herrscht mitunter ein Ton, der mit Achtung voreinander nicht viel zu tun hat. Im Gegenteil: Oft werden die Grenzen des Anstands überschritten und einfach drauflosgepöbelt. Es gibt also genug Gründe, dass wir im nächsten Heft mal schauen, was es mit dem Respekt so auf sich hat.

Impressum

fluter – Magazin der Bundeszentrale für politische Bildung
Ausgabe 68, Thema Daten, Herbst 2018
Herausgegeben von der Bundeszentrale für politische Bildung (bpb)
Adenauerallee 86, 53113 Bonn
Tel. 0228/995 15-0

Redaktion
Thorsten Schilling (verantwortlich/Bundeszentrale für politische Bildung/schilling@bpb.de),
Oliver Gehrs (redaktionelle Koordination)
Fabian Dietrich

Bildredaktion
Trine Skraastad

Artdirektion und Design
zmyk/Jan Spading
Design und Lithografie
zmyk/Oliver Griep

Mitarbeit
Simone Ahrweiler, Pao Engelbrecht, Arno Frank, Sabrina Gaisbauer, Bernd Kramer, Stefan Lampe, André Nagel, Lisa Neal, Michael Radunski, Nicolas Rose, Natascha Roshani, Annett Scheffel, Isabel Schneider, Arne Semsrott, Niklas Prenzel

Dokumentation
Kathrin Lilienthal

Korrektorat
Tina Hohl, Florian Kohl

Redaktionsanschrift/Leserbriefe
fluter – Magazin der Bundeszentrale für politische Bildung,
DUMMY Verlag, Torstraße 109, 10119 Berlin,
Tel. 030/30 02 30-233, Fax -231, post@fluter.de

Redaktionelle Umsetzung
DUMMY Verlag GmbH, Torstraße 109,
10119 Berlin
ISSN 1611-1567
Bundeszentrale für politische Bildung
info@bpb.de
www.bpb.de

Abonnement & Leserservice
ssm system service marketing gmbh
Im Auftrag der Bundeszentrale für politische Bildung
Dudenstraße 37-43, 68167 Mannheim
Tel. 0621/338 39-38, Fax 0621/338 39-33
abo@heft.fluter.de

Kostenloses Abo bestellen, verlängern oder abbestellen
www.fluter.de/heft-abo
abo@heft.fluter.de

Nachbestellungen
Publikationsversand der Bundeszentrale für politische Bildung/bpb, Postfach 501055,
18155 Rostock
Fax 038204/66-273,
www.bpb.de/shop
Nachbestellungen von fluter werden von 1 kg bis 20 kg mit 5 Euro kostenpflichtig.

Druck
Ernst Kaufmann GmbH & Co. KG, Druckhaus Raiffeisenstraße 29, 77933 Lahr
Tel. 07821/945-0, info@druckhaus-kaufmann.de
www.druckhaus-kaufmann.de

Bildnachweise
Sämtliche Illustrationen sind von Frank Höhne. Cover BENJAKON; S. 2 www.anwaltauskunft.de; S. 3 Felix Hüffelmann; S. 4 Bettmann/Getty Images, Janek Stroisch; S. 5 Nikita Teryoshi, Daniel Leal-Olivas/AFP/Getty Images; S. 6 Michael Hughes/Umbruch Bildarchiv, Emanuele Cremaschi/Getty Images; S. 8 Fabian Grimm; S. 9 Michael Wolf/laif; S. 15 www.studiorosenmunthe.com; S. 16-17 The New York Times/Redux/laif (2); S. 19 Max Slobodda; S. 20-22 SpY www.spy-urbanart.com; S. 23 Getty Images; S. 24 Daniel Stier; S. 25 Heinrich Holtgreve/OSTKREUZ; S. 28 Jason Reed/REUTERS, Mark Malijan/©Microsoft; S 29 Michael Wolf/laif; S. 33 Jens Schlueter/Getty Images; S 34-35 CV Dazzle Look 2, Foto: Adam Harvey, Model: Irina, Haare: Pia Vivas, Art Direction: DIS Magazine, 2013 New York City; S. 40-41 Jakob Polacsek (4), Andreas Jakwerth (2); S. 42-45 Janek Stroisch; S. 48 Bettmann/Getty Images; S. 50 THE CLEANERS © gebrueder beetz filmproduktion; S. 51 Fortnite: Battle Royale/Epic Games

Papier: Dieses Magazin wurde auf umweltfreundlichem, chlorfrei gebleichtem Papier gedruckt.

Ausführliche Informationen zu Datenschutz und Betroffenenrechten findest du hier:
www.fluter.de/datenschutz

Volltreffer oder voll daneben?

Mehr als Ballerei: Auf *spielbar.de* gibt's Kritiken, Diskussionen, Aufklärung und Tipps zu Spielen

spielbar.de

Die letzte Seite im Heft ist die erste Seite im Netz

Wie sieht’s denn bei dir aus?
Schick ein Bild an
meinzimmer@fluter.de

Schreibtisch von Carolina Rauh