Das utopische Politikmagazin

#04 | Sommer 2017 | 9,80 €

KATER DEMOS

SCHWERPUNKT

ÜBERWACHUNG

Wir haben ja nichts zu verbergen?! | Überwachung – das schleichende Gift | CIA-Katzen
Too Smart Home | Verschlüsselungs-1x1 | Orwell 2017 | Snowdens Vermächtnis

WIR HABEN JA NICHTS ZU VERBERGEN!?

Wovor hat eigentlich die NSA Angst? Natürlich, vor Überwachung! Nicht, dass noch jemand unentdeckt an Informationen gelangt, die staatstragenden Ausmaßes sind. Oder, dass gar der Umfang der geheimdienstlichen Aktivitäten auf der ganzen Welt diskutiert wird, weil ohne Kenntnis Daten entwendet wurden. Genau das passierte der NSA, also der National Security Agency, dem größten Auslandsgeheimdienst der USA, im Jahr 2013: Dank des Whistleblowers Edward Snowden, der mit seinen Veröffentlichungen und einer gehörigen Portion Mut das Ausmaß weltweiter Überwachung aufdeckte.

Nun wissen wir zwar eine Menge über PRISM, XKeyscore und andere Programme, die fleißig all unsere Daten sammeln, verknüpfen und daraus Schlüsse ziehen. Doch wer denkt, dass die Datensammelei deshalb weniger geworden ist, der irrt.

Gilt denn nicht: »Ausspähen unter Freunden – das geht gar nicht.«, wie es die deutsche Bundeskanzlerin 2013 Obama ins Telefon säuselte, als die Überwachung ihres eigenen Telefons publik wurde? Es geht. Es darf nur keiner mitbekommen! Und genau hier lag tragischer Weise der mit Abstand größte Ärger der Amerikaner. »Weiß ich, ob du morgen noch mein Freund bist?«, wäre die ehrliche Antwort der USA auf Merkel gewesen und hätte auch ein wenig entlarvt, wie Sicherheitspolitik funktioniert: Traue bloß niemandem! Schon gar nicht deinen Bürgern, diesen gemeingefährlichen Individuen. Denn »Alle Gewalt geht vom Volke aus!«. Da muss der Staat sich ja wohl rechtzeitig schützen!

2017, vier Jahre später, blickt Kater Demos hinter die Kulissen unserer überwachten Gesellschaft und fragt nicht nur, »Was von Snowden übrigblieb?« (S. 30), sondern auch wie leicht es eigentlich wäre, wenn George Orwells Buch »1984« heute Wirklichkeit werden würde. Sagen wir »In einem Land aus unserer Zeit« (S. 6), in dem ein verrückter, orangefarbener Präsident mit autokratischen Zügen und willigen Geheimdiensten regiert.

Darüber hinaus schauen wir genauer hin, wer uns denn so alles überwacht. Da wären natürlich Kameras (S. 94), aber auch Supermärkte (S. 72), Sprachassistenten (S. 58), Detektive (S. 112), der eigene Kühlschrank (S. 26), der Innenminister (S. 92) oder auch der Online-Schuhhändler eures Vertrauens (S. 78). Und manche werden gar von ihrem Nachbarn überwacht (S. 42).

Paranoid werden (S. 100) ist allerdings keine Lösung. Darum geben wir euch Werkzeuge an die Hand, um den Datenkraken zu entkommen. Hier hilft nicht nur das ominöse Darknet (S. 48), sondern vor allem unser Verschlüsselungs-1x1 (S. 136). Neben all dem Dystopischen sehen wir aber auch die Utopie, wie in der Wissenschaft, in der Open Data-Projekte Daten für alle zur Verfügung stellen (S. 90) oder wenn wir den Staat dank Informationsfreiheit zurücküberwachen – oder zumindest ausfragen – können (S. 86).

Am Ende hilft es schon Bewusstsein zu schaffen und »Überwachung als schleichendes Gift« (S. 12) wahrzunehmen, wie Konstantin von Notz, der seit 2013 im NSA-Untersuchungsausschuss des Bundestags gegen den Unwillen der Großen Koalition um Aufklärung ringt.

Die stillen Helden finden sich sonst in den merkwürdigsten Formen. So konkretisiert sich die Angst der NSA unter anderem in einem zwanzig Zentimeter hohen, flauschigen Kinderspielzeug aus den 90ern, dem Furby, der seit 1999 in alle NSA-Gebäuden streng verboten ist (S. 40) und den wir daher zum Maskottchen dieser Ausgabe erkoren haben.

Unsere abschließende Utopie lässt sich kaum besser formulieren, als in dem über 200 Jahre alten Lied »Die Gedanken sind frei« (S. 128). Wir hoffen, dass es dabei bleibt.

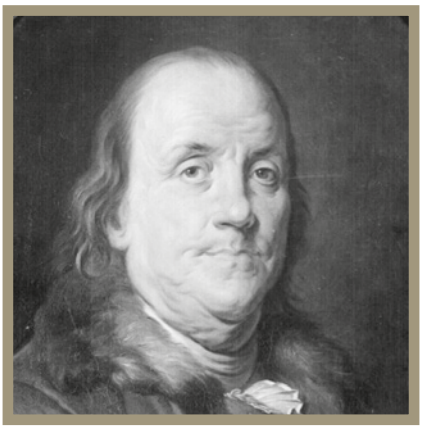
Viel Spaß mit unserer latent dystopischen vierten Ausgabe!

Alexander Sängerlaub, Chefredakteur, alexander@katerdemos.de
Redaktion Kater Demos, Frankfurter Allee 43, 10247 Berlin

info@katerdemos.de | katerdemos.de | facebook.com/katerdemos
twitter.com/katerdemos | instagram.com/katerdemos

#04 AGENDA ÜBER WACHUNG

Benjamin Franklin
Pennsylvania Assembly: Reply to the Governor, Printed in Votes and Proceedings of the House of Representatives, 1755-1756 (Philadelphia, 1756)



»WER DIE FREIHEIT AUFGIBT, UM SICHERHEIT ZU GEWINNEN, DER WIRD AM ENDE BEIDES VERLIEREN.«

»Mensch, passt das hervorragend zur Debatte um Überwachung, die NSA und Snowden!« werdet Ihr Euch sicherlich denken. Doch im eigentlichen Original als Anschreiben an den Gouverneur von Pennsylvania 1755 ist das Zitat tatsächlich ein wenig differenzierter: »Wer wesentliche Freiheit aufgeben kann, um eine geringfügige, bloß jeweilige Sicherheit zu bewirken, verdient weder Freiheit noch Sicherheit«. Noch dazu ging es Franklin auch nicht um staatliche Überwachung, sondern um Steuern und die Frage wie viel Geld die Amerikaner damals in die Verteidigung gegen die Franzosen und Indianer stecken sollten. Das in 262 Jahren schon mal der Kontext flöten gehen kann – geschenkt! Oder »Fake news!«, wie wir heute sagen würden. Dennoch: Ein super Satz!

Edward Snowden
2015 bei Reddit

»ZU ARGUMENTIEREN, DASS SIE KEINE PRIVATSPHÄRE BRAUCHEN, WEIL SIE NICHTS ZU VERBERGEN HABEN, IST SO, ALS WÜRDEN SIE SAGEN, DASS SIE KEINE MEINUNGSFREIHEIT BRAUCHEN, WEIL SIE NICHTS ZU SAGEN HABEN.«

Das Totschlagargument schlechthin aller Überwachungsbefürworter hat in der englischen Wikipedia als ›nothing to hide argument‹ sogar einen eigenen Eintrag, da es immer wieder in der Diskussion aufploppt und immer wieder widerlegt werden muss. Dort erfährt man auch, dass die Briten ihr Massenüberwachungsprogram CCTV, also die fast flächendeckende Überwachung des öffentlichen Raumes via Kameras, konkret mit dem Claim »If you've got nothing to hide, you've got nothing to fear« beworben haben.

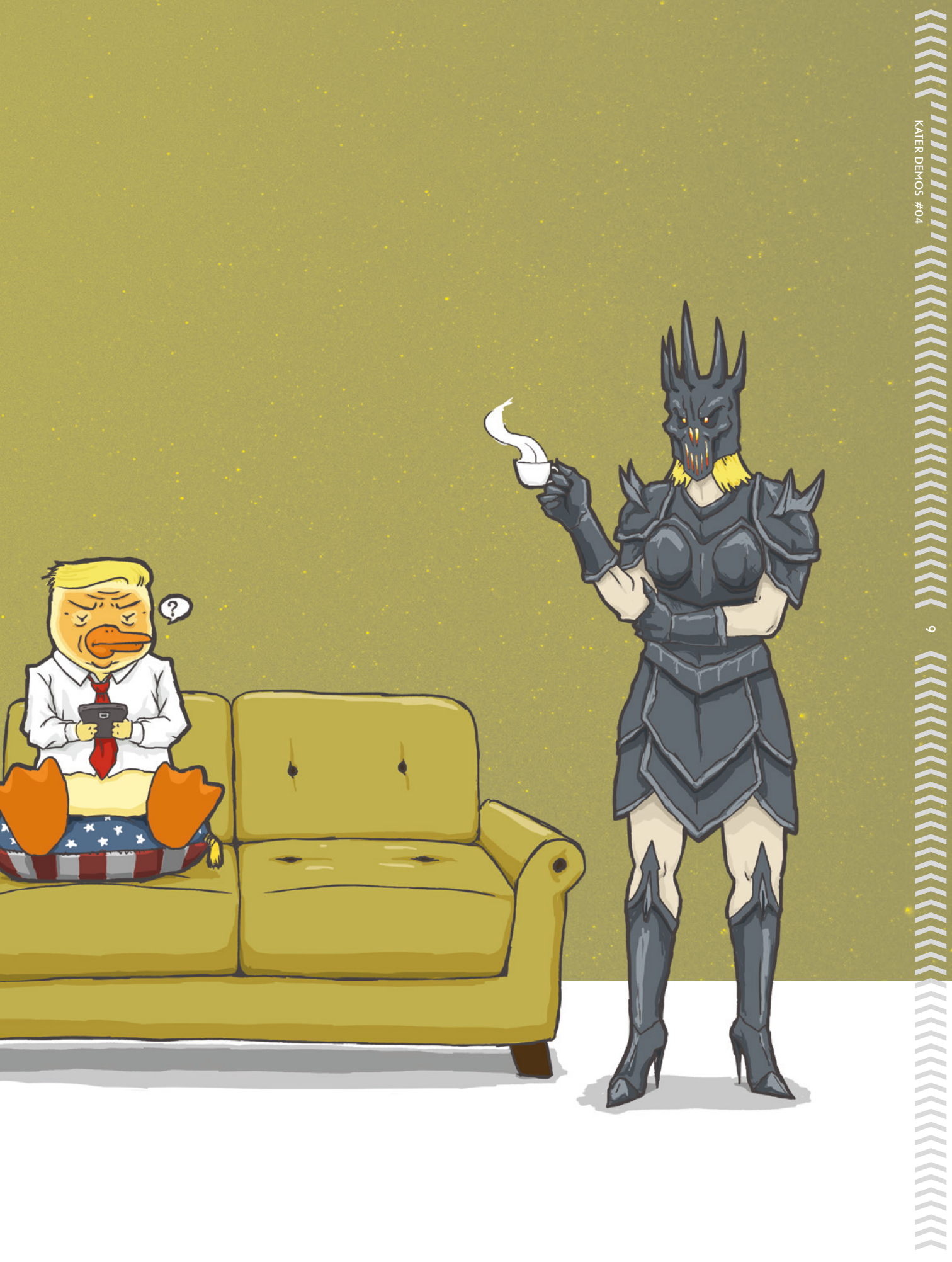
Und wo wir schon unfassbar journalistisch in unser aller Online-Lieblingslexikon herumstochern, noch ein Zitat von Wikileaks-Gründer Julian Assange: »Es gibt noch keine ›Killer‹-Antwort. Jacob Appelbaum hatte eine clevere Antwort, indem er Leute, die dies sagten, bat, ihm ihr entsperrtes Handy zu geben und ihre Unterhosen herunter zu ziehen. Meine Version davon ist, ›Gut, wenn du so langweilig bist, dann sollten wir nicht mit dir sprechen, und auch kein anderer sollte dies tun‹, aber philosophisch, die richtige Antwort ist dies: Massenüberwachung ist eine massive strukturelle Veränderung. Wenn die Gesellschaft sich zum Schlechten verändert, wird es dich mit ziehen, auch wenn du die uninteressanteste Person auf der Welt bist.«

SCHWERPUNKT ***ÜBERWACHUNG***

IN EINEM LAND AUS UNSERER ZEIT

Alle in diesem Text geschilderten Handlungen und Personen sind nur bedingt frei erfunden. Ähnlichkeiten mit lebenden oder verstorbenen Personen sind daher nicht zufällig und total beabsichtigt.

TEXT ALEXANDER SÄNGERLAUB
ILLUSTRATION MARC HEINRICH



Unsere Reise führt uns heute in die *Unmöglichen Staaten von Umerica* (kurz USU), einem völlig fiktiven Staat, in dem sich gerade die Demokratie selbst abschafft. In diesem regiert, noch nicht allzu lange, ein latent wahnsinniger, autokratischer Präsident namens Dagobert Ace – vom Volk gewählt: Ein Mann ohne moralischen Kompass, ohne großes Verständnis für die demokratischen Grundwerte und Errungenschaften seines fast 250 Jahre alten Landes und mit erstaunlich kleinen Händen. Ihm zur Seite steht nicht nur ein Beraterstab, dessen Wurzeln bis tief hinein in die faschistischen Bewegungen des Landes reichen, sondern auch die wohl mächtigsten Inlands- und Auslandsgeheimdienste der Welt.

Es ist 7:30 Uhr. Dein Wecker klingelt. »Alexa stopp!«, rufst Du diesem 24 Zentimeter hohen, schwarzen Zylinder zu, welcher seit neuestem in Deinem Zimmer steht. Diese Siri in der Plastikdose nennt sich Amazon Echo und hört auf den Namen Alexa. Von ihr kannst Du Dir nicht nur Musik vorspielen, einen Witz erzählen oder einen Wecker stellen, sondern auch Dein ganzes Zuhause, Dein sogenanntes Smart Home, steuern lassen. Alexa hört Dir dabei die ganze Zeit zu, denn sie wartet darauf, dass Du ihren Namen (ihr Buzzword) sagst, damit sie für Dich Dinge erledigen kann. Doch keine Angst, nur die Dinge, die Du mit ihr besprichst, werden auf die Server von Amazon weitergeleitet.

Draußen scheint die Sonne, Vöglein zwitschern. Es ist Frühling. Wie schön. Nach dem Aufstehen lässt Du mit Hilfe von Alexa die Rollläden herunter, nicht dass die Nachbarn Dir noch in die Wohnung schauen. Du willst schließlich Privatsphäre. Doch für das Erkennen von Doppelmoral und die zynische Skurrilität des Alltags ist es für Dich um 7:30 Uhr noch etwas zu früh.

Präsident Ace hatte auch einen guten Morgen. Denn gerade eben hat er ein weiteres seiner Wahlkampfversprechen eingelöst und seine Kontrahentin, Vallery van Clanton, verhaften lassen. »Lock her up!« riefen seine Anhänger begeistert im Wahlkampf und nach den ersten 100 Tagen im Amt ist klar: Ace hält, was er verspricht – zur großen Überraschung und Verwunderung von Presse und Weltöffentlichkeit gleichermaßen... Die Anklage gegen van Clanton lautet irgendwas mit Korruption und Beihilfe zum Terrorismus; da wird sich schon was finden lassen, wenn man tief genug gräbt.

Nun trifft Ace mit seinem Nationalen Sicherheitsrat zusammen, einem Gremium höchster Integrität und Rechtsstaatlichkeit, welchem die Sicherheit der Bürger der USU am Herzen liegt – also früher einmal, bevor Lord Voldemort und Lady Sauron zu ständigen Mitgliedern ernannt wurden. Heute steht auf dem Programm, wie man mithilfe der Geheimdienste und Tech-Konzerne Terroristen und Systemkritiker, also Anhänger der gescheiterten Präsidentschaftskandidatin van Clanton, einfacher loswerden kann. Präsident Ace hat Lord Voldemort hierfür schon ein Dekret vorbereiten lassen, welches der Präsident am Nachmittag unterzeichnen soll.

Du machst Dir einen Kaffee, beziehungsweise lässt Dir von Alexa einen Kaffee zubereiten, denn auch die Kaffeemaschine ist vernetzt und Teil deines Smart Homes. Alles was Du noch machen musst, ist die Tasse mit dem frischgebrühten Kaffee in die Hand zu nehmen und dabei zwei Fingerabdrücke von Daumen und Zeigefinger auf dieser zu hinterlassen. Die gleichen Fingerabdrücke liegen auch den 18 Staaten vor, in die Du in Deinem bisherigen Leben mit Deinem elektronischen Reisepass gereist bist. Unter diesen 18 Staaten sind übrigens nur neun wirkliche Demokratien. Das könnte an anderer Stelle noch einmal wichtig werden, das ist Dir nur gerade noch nicht klar.

Du checkst Deine E-Mails. Die vielen komischen Spam-Mails von der Lotterie in Morakka, die Du angeblich gewonnen hast, löschst Du. Die Geheimdienste wissen dennoch von diesen und den anderen Mails, denn genau solche Daten werden mittels Selektoren-Listen überprüft und in einigen Ländern bis zu einem halben Jahr gespeichert. Wie? Das geht ganz einfach: Die Geheimdienste zapfen hierfür Tiefseekabel an, denn Dein Mailprovider sitzt auf der anderen Seite des Ozeans. Diese Selektoren sind wiederum Metadaten wie zum Beispiel einzelne E-Mail-Adressen, Telefonnummern, Keywords, URLs, oder Geokoordinaten. Treffen zu viele Selektoren zusammen, gerät man ins Visier der Behörden und diese schauen sich Deine Nachrichtenverläufe dann genauer an. Sicher ist sicher. Zum Beispiel: Wenn sich zu viele E-Mails aus Morakka mit zu vielen verdächtigen Keywords in Deinen Mails befinden. Dabei sprichst du ja nicht einmal die Sprache.

Dein bester Freund und Mitbewohner kommt zur Küche hinein und macht sich ebenfalls einen Kaffee. »Hast du schon gehört?«, fragt er Dich, während er sich einen Schluck Milch dazu gießt, »Vallery van Clanton ist heute Morgen verhaftet worden. Da müssen wir doch was dagegen tun! Heute Abend soll es spontane, landesweite Demos geben. Kommst Du mit?« Als Anhänger der Demokratie, für den die Wahl von Dagobert Ace, einem Soap-Darsteller aus dem Fernsehen, die Versinnbildlichung eines Worst-Case-Szenarios ist, sagst Du natürlich: »Ja!«

»Operation Röstaroma ist in vollem Gange.«, zischt Lord Voldemort vergnüglich und schaut vielsagend zu Präsident Ace. »Tremendous!«, entgegnet der Präsident begeistert. Die Regierung arbeitet schon lange mit den großen Internet- und Technologiefirmen zusammen, um die Überwachungsmaßnahmen massiv auszuweiten. Die Internetfirmen wurden mithilfe großer Summen zur Kooperation überredet und mit der Ankündigung verschiedentlicher Gesetze zu ihren Ungunsten auch noch ein bisschen bedroht. Das gibt natürlich niemand nach außen hin freiwillig zu. Erst die Erkenntnisse, die der Whisteblower Eduard Rainden veröffentlicht hat, bestätigten die Vermutungen von Presse und Experten – viel passiert ist jedoch nicht.

Doch die Internetfirmen machen es der Regierung nicht einfach, schließlich fürchten sie auch um ihren eigenen Ruf, wenn das Ausmaß der Zusammenarbeit mit den Behörden bekannt wird. Daher heckte Lord Voldemort einen raffinierten Plan aus, den der Präsident Ace begeistert »Operation Röstaroma« getauft hat. Die Idee war so einfach wie krude: Um sich von den störrischen Konzernen nicht mehr auf der Nase herumtanzen zu lassen und unabhängig agieren zu können, hat der Auslandsgeheimdienst zusammen mit der Regierung eine Scheinfirma gegründet, mit der sie ein Alltagsprodukt entwickelten das mit eingebautem Mikrofon und Chip selbst zum Überwacher schlechthin wird – eine Art trojanisches Pferd für jeden Haushalt. Eines, das jeder Umerikaner im Hause hat: Die Smart Sauron 2020, eine simple Kaffeemaschine. Zugegeben: Sie ist schön designt, der Renner auf dem Markt und dazu noch Bluetooth- und W-LAN-fähig – außerdem in gleich sechs verschiedenen Farben erhältlich. Zudem wird sie in zahlreichen landesweiten Werbespots raffiniert von der Tochter des Präsidenten mit dem Slogan beworben: »Make coffee great again!«.

Du verlässt das Haus, kaufst Dir eine Zeitung am Kiosk und steigst in die U-Bahn. Nicht nur vor dem Kiosk hängt eine öffentliche Kamera, der gesamte U-Bahnhof inklusive Bahnsteig wird überwacht. Inzwischen können Menschen auf diesen Videoaufnahmen dank Gesichtserkennungssoftware problemlos identifiziert werden, vor allem, wenn man, so verdächtig wie Du, gleich zwei Mal in die gleiche Kamera guckt. Da wird die biometrische, durch Algorithmen gesteuerte Verhaltensanalyse nämlich neugierig. »Das lag an der Taube, die auf dem Bahnsteig auf der Kamera saß«, wirst Du später sagen. Genau davon gab es aber leider keine Kamera-Aufnahme. Schade.

Währenddessen meldet Deine mit dem Internet vernetzte Kaffeemaschine übrigens Deinen Kaffeekonsum an Deine Krankenkasse. Du wirst in der nächsten Woche die dritte Tariferhöhung binnen sechs Monaten bekommen. Da hättest du mal besser die 200-seitige Datenschutzvereinbarung vorher lesen sollen, selber schuld.

Apropos, die Kaffeemaschine hat zudem einen Produktionsfehler und kann nicht unterscheiden wer wie viel Kaffee bei Euch in der Wohnung trinkt. Sie sendet den Kaffeekonsum Deiner drei Mitbewohner auch gleich als Deinen eigenen an Deine Krankenversicherung mit. Die Tariferhöhung geschieht hier komplett automatisch – schlecht programmierte Algorithmen haben bei Deiner Krankenkasse schon längst einen Großteil der Mitarbeiter aus Fleisch und Blut überflüssig gemacht. Die einzig gute Nachricht an diesem Tag wird sein, dass Du von dieser Krankenkassen-Tariferhöhung nichts mehr mitbekommst.

Präsident Ace sitzt in seinem Büro und schlürft eine große Tasse Kaffee. Sein Sicherheitsberater, Lord Voldemort, sitzt auf dem Sofa links vom Schreibtisch des Präsidenten, seine Beraterin ohne Geschäftsbereich und Wahlkampfmanagerin Lady Sauron auf dem Sofa rechts. Sie sind gut gelaunt und nutzen die kurze Kaffeepause für einen angeregten Plausch.

»Kaum zu glauben wie einfach doch letztlich alles gelaufen ist«, zischt Lord Voldemort vergnüglich. »Amazing!«, freut sich der Präsident. »Dass uns die ▸

vorhergehenden Regierungen den Weg dafür freigemacht haben, müssten wir ihnen eigentlich noch einmal danken. Vor allem dem ehemaligen texanischen Präsident Strauch ist mit dem Patriot Act ein genialer Coup gelungen. Davon profitieren wir noch Jahrzehnte.«, ergänzt Lady Sauron.

»Und das alles ganz einfach im Namen des Kampfes für den Terrorismus«, fügt Lord Voldemort hinzu. »Huch, ich meine natürlich im Kampf gegen den Terrorismus.« Alle drei lachen laut auf.

»Das Framing ist aber auch einfach zu perfekt. Denn wir machen das ja alles für den Erhalt der Demokratie«, kichert Lady Sauron.

»Great!«, fährt es Präsident Ace heraus. Er scheint, der Diskussion kaum folgen zu können und versucht auf seinem Smartphone parallel herauszufinden, was der Patriot Act eigentlich ist.

»Was das aber auch für ein wunderbarer Begriff ist – Demokratie!«, beginnt Lord Voldemort zu sinnieren und schaut an die Decke des Oval Office. »Er ist so dehnbar, so interpretierbar, wie Knete, aus der sich jeder das formen kann, was er möchte. Kann ich noch ein Stück Zucker haben, Verehrteste?«

Lady Sauron reicht ihm ein Stück Zucker aus der kleinen, elefantenförmigen Zuckerdose auf seiner Seite des Tisches, deren Keramik in den Farben der Flagge der USU bemalt ist. Sie bringt einen Toast aus: »Ein Hoch auf die Unmöglichen Staaten von Umerika!«

Newspeak), die fiktive Sprache zur Indoktrination der Bevölkerung. Für den Euphemismus alternative Fakten gibt es auch das passende Wort in Orwells Roman: Quaksprech (engl. Duckspeak), wenn man ohne Unterlass, wie eine Ente schnatternd, lügt und Unsinn erzählt.

Du sitzt in der U-Bahn, plötzlich vibriert Dein Handy. Deine Schwester, die gerade ein Auslandssemester im Mittleren Osten verbringt, fragt Dich, ob Du ihr etwas Geld überweisen kannst. Sie hat Angst, dass Sie überfallen wird und daher nie mehr als 500 Dollar auf ihrem Konto. Manchmal, wenn sie knapp bei Kasse ist, schickst Du wieder etwas von Deinem Konto auf das Ihre. Über diese regelmäßigen Transaktionen auf Deinem Bankkonto sind die Behörden natürlich bestens informiert. Zumal das Land, in dem Deine Schwester gerade studiert, offiziell zur Achse des Bösen gehört. Dass Deine Schwester dort parallel ehrenamtlich in der Entwicklungshilfe tätig ist und mindestens genauso eine Anhängerin von Freiheit und Rechtsstaat wie Du, ist kein Grund für die Behörden bei Euch nicht genauer hinzuschauen.

Nachdem Du mit Deinem Smartphone Deiner Schwester Geld überwiesen hast, kommst Du endlich dazu, an Deinem Buch, George Orwells Science-Fiction-Roman 1984, weiterzulesen. Was für eine gruselige, traurige Welt, die der Autor da beschreibt. Gott sei Dank ist die Welt heute eine andere. Obwohl Du irgendwie schon beim Lesen gruselige Parallelen entdeckst – wie die alberne Diskussion um die Zahl der Besucher bei Dagobert Aces Amtseinführung. Laut dem Präsidenten waren es so viele wie noch nie, dabei gab es unbestreitbare Luftaufnahmen, die belegen, dass dem nicht so war. Oder wie das lächerliche Beharren Aces darin gipfelte, dass die Beraterin des Präsidenten meinte, den Mitarbeitern des Weißen Hauses hätten halt »alternative Fakten« zur Verfügung gestanden. Übersetzt sind das »widerlegbar falsche Behauptungen«. Orwell nannte das Neusprech (engl.

Am Nachmittag versammeln sich im Westflügel des Weißen Hauses die Überreste der freien Presse. Präsident Ace will sich zur Verhaftung von van Clanton äußern; außerdem zu der Tatsache, dass zahlreiche Sympathisanten, Richter, Lehrer und Parteianhänger ebenfalls heute Morgen festgenommen wurden, da sie angeblich mit der Kontrahentin unter einer Decke stecken würden. Sogar einen Putsch hätten sie geplant. Die Anklage lautet demnach für alle: Beihilfe zum Terrorismus.

»Stimmt es, dass Sie heute über 9.000 Umerikaner verhaften lassen haben, die angeblich Mitverschwörer von van Clanton sind«, fragt die erste Journalistin in der Pressekonferenz aufgebracht.

»Ach, Fake-News«, bügelt der Präsident die Frage ab und verzieht das Gesicht wie ein beleidigter Fünfjähriger.

»Wir haben hier bestätigte Aussagen von staatlichen Stellen, dass Sie Richter, Lehrer und sogar Vertreter der Demokratischen Partei verhaften lassen haben«, bohrt die Journalistin weiter nach und wedelt mit einem großen Stapel ausgedruckter Papiere.

»Möchten Sie mich nicht lieber etwas zu meinem tippy-top Entwurf zur Erhöhung des Verteidigungsetats fragen?«

Die Journalistin lässt nicht locker: »Und stimmt es, dass Sie überall Geheimgefängnisse bauen lassen haben, in denen es keine rechtsstaatlichen Verfahren für die Verhafteten gibt – wie in Guantanamo?«

Der Präsident schaut hilfesuchend nach links und rechts und tritt schließlich vom Pult herab, um das Wort an Lord

Alexander Sängerlaub ertappt sich selbst zuweilen dabei, wie ihn die Bequemlichkeit die eigenen Daten furchtlos in die Welt entlassen lässt. Freiheit und Demokratie werden es schon richten, dass niemand etwas Böses damit treibt, doch die Geschichte des eigenen Landes oder wie der sorgenvolle Blick in die Türkei und in die USA zeigen, verheißen wenig Anlass für den guten Glauben. Es bleibt, den Dingen manchmal den Stecker zu ziehen; wie Alexa, die ungefragt den Einzug in das eigene Wohnzimmer geschafft hat.

Voldemort weiterzugeben. Ihm selbst sind diese Fragen viel zu lästig. »I will grab them by the coffee!«, gackert er den Journalisten entgegen und verschwindet hinter der Bühne.

»Meine Damen und Herren, verehrte Journalisten«, beginnt Lord Voldemort mit seiner hohen, schlangenartig-zischenden Stimme den anwesenden Medienvertretern zuzusäuseln. »Der Krieg gegen den Terrorismus hat für den Präsidenten oberste Priorität. Jeder, der uns – also der Demokratie – in die Quere kommt, wird die volle Härte des Rechtsstaates zu spüren bekommen.«

»Haben Sie die Demokratie nicht längst schon abgeschafft?«, fährt es aus einem anderen Journalisten wütend heraus.

Lord Voldemort lächelt gütig und wählt seine Worte mit Bedacht: »Teile meiner Antworten würden Sie nur verunsichern.«

Am Abend, nach der Demonstration, kommst Du müde und erschöpft nach diesem langen, turbulenten Tag nach Hause. Als Du den Lichtschalter im Treppenhaus betätigst, wunderst Du Dich noch kurz, warum die Beleuchtung nicht funktioniert. Kurz darauf hast Du einen schwarzen Sack über dem Kopf und wirst mit Wucht zu Boden gedrückt. Jemand bindet Dir mit Kabelbinder die Hände hinter den Rücken und trägt Dich aus dem Treppenhaus hinaus. Dir kommt es vor, als ob Du in einen Transporter geworfen wirst. Deine Knie und Deine Arme scheinen zu bluten. Wo fahren sie nur mit Dir hin und vor allem: Warum?

Im Kopf läuft dein ganzer Tag noch einmal Revue: Dein Morgen mit Alexa, dein Gespräch über van Clanton und die Demo, die seltsamen E-Mails, deine Fingerabdrücke, die Kamera auf dem U-Bahnhof mit der gurrenden Taube, die Überweisung an deine Schwester – nur an diesem einen einzigen Tag hast auf Schritt und Tritt überall Daten hinterlassen, wo du dich bewegt hast. War irgendwas an diesen Aktionen falsch? Vielleicht ist es alles auch nur eine schreckliche Verwechslung? Du wirst es nie erfahren, denn seit Präsident Ace im Amt ist, ist Umerica kein Rechtsstaat mehr. Dir stehen kein Verfahren und kein Anwalt zu. Denn ab jetzt bist Du nur noch eines: Terrorist. •

KONSTANTIN VON NOTZ

Für seine Partei Bündnis 90/Die Grünen sitzt er seit 2009 im Deutschen Bundestag. Dort ist er stellvertretender Vorsitzender und netzpolitischer Sprecher seiner Fraktion. Von Notz ist der Obmann seiner Partei im NSA-Untersuchungsausschuss.

»ÜBERWACHUNG IST EIN SCHLEICHENDES GIFT«

Konstantin von Notz sitzt seit über drei Jahren als Obmann für die Grünen im NSA-Untersuchungsausschuss des Bundestages. Zu Mitte diesen Jahres ist die Arbeit des Ausschusses mit der Veröffentlichung seines Abschlussberichts offiziell beendet: Das Problem der Überwachung aber noch lange nicht. Wir sprachen mit ihm über die anlasslose, massenhafte Überwachung, Dinosaurier und Currywurst.

INTERVIEW ALEXANDER SÄNGERLAUB & RAIMON KLEIN
FOTOS JOHANNES BERGER

KATER DEMOS *Die EU-Kommission, Mitglieder des französischen Außenministeriums, das Telefon der Kanzlerin, deutsche Wirtschaftsunternehmen und auch der NSA-Untersuchungsausschuss* – wer wird eigentlich nicht durch Geheimdienste ausgespäht?*

KONSTANTIN VON NOTZ Das ist eine berechtigte Frage und so genau kann das niemand sagen. Denn für die Selektoren*, welche die Inhalte aus dem Datenstrom herausfiltern, gibt es kein Prüfverfahren. Zudem gibt es keine komplette Übersicht, da jeder Dienst seine eigene Agenda hat. Häufig geht es nicht nur um ein konkretes Ziel, sondern auch um dessen Umfeld, um mitzubekommen, was beispielsweise dem Überwachten erzählt wird. Insofern kann man die Frage gar nicht so konkret beantworten – sicher ist nur, dass massenhaft überwacht wird. Und da reden wir jetzt nur über die Inhaltsdaten. Über das ebenso problematische Abgreifen von sehr aussagekräftigen Verkehrsdaten*, die wahrscheinlich global fast komplett erfasst werden, reden wir noch gar nicht.

*NSA-UNTERSUCHUNGS-AUSSCHUSS

Angestoßen durch die Enthüllungen Edward Snowdens wurde der parlamentarische Untersuchungsausschuss am 20. März 2014 vom Deutschen Bundestag im Auftrag aller Fraktionen eingesetzt. Ziel ist es, »Ausmaß und Hintergründe der Ausspähungen durch ausländische Geheimdienste in Deutschland aufzuklären«.

KD *Nach der Aussage von Bundeskanzlerin Angela Merkel vor dem Untersuchungsausschuss am 16. Februar 2017 muss man sich zwangsläufig fragen: Führen die deutschen Geheimdienste ein Eigenleben? Wo bleibt die Kontrolle durch das Bundeskanzleramt oder das Parlament?* ▸

KVN Ich hatte den Eindruck, dass auch das Kanzleramt findet, dass die Geheimdienste ein Eigenleben führen. Der Kern der Aussage von Frau Merkel ist: Sie hätte von vielen dieser Vorgänge überhaupt nichts gewusst und zwar bis zum März 2015, also weit über die Snowden-Enthüllungen hinaus. Jedoch ist es wahrscheinlich zu kurz gegriffen, die ganze Schuld bei den Diensten zu suchen. Denn dazu gehört natürlich auch eine Politik im Bundeskanzleramt, die sich das gefallen lässt, obwohl man die Dienst-, Fach- und Rechtsaufsicht für den BND hat.

Das grundlegende Abkommen* zwischen den Diensten, auf das sich alles zurückführen lässt, ist 2003 unter Rot-Grün entstanden, mit der Verantwortung des damaligen Chefs des Kanzleramts Frank-Walter Steinmeier. Deswegen wäre es zu einfach nur zu sagen, die Dienste führen ein Eigenleben. Denn da gibt es eine realpolitische Rückkopplung. Aber trotzdem ändert das nichts an der Tatsache, dass man vieles bewusst an den parlamentarischen Kontrollgremien vorbeigezogen hat, und dass das Problem überhaupt so groß werden konnte.

KD ***Der ehemalige NSA-Chef Michael Hayden sagte, dass man stets im Sinne der Demokratie agiert habe, im Gegensatz zur Stasi etwa. Kann man zwischen »guter« und »böser« Überwachung unterscheiden oder ist das kein Trost?***

KVN Also wenn es ein Trost ist, dann ein geringer. Natürlich stimmt es, dass die Menschen in den USA und in Deutschland nicht nach Bautzen abtransportiert werden. Aber wir merken gerade in der heutigen Zeit, in der es einen Hang zum Autokratischen gibt, was es bedeutet, wenn diese Instrumente in die Hände der falschen Leute geraten. Jeder kann sich überlegen, ob es ihn stört, wenn jemand wie Trump offen sagt, dass er die EU für zerschlagungswert hält und ganz offensichtlich gegen deutsche und europäische Interessen arbeiten will. Ist dieses mächtige Überwachungsinstrument also in guten Händen?

Demokratien müssen auch für schwierige Zeiten gerüstet sein. Am Ende des Tages muss unsere Verfassung uns schützen, wenn Herr Gauland oder Frau Petry Innenminister sind oder Frau Le Pen in Frankreich regiert und Mr. Trump in den USA. Für diesen Fall sind wir nicht gut aufgestellt, weil die verfassungsrechtliche Einhegung dieser Überwachungsmaschinerie nur sehr unzureichend funktioniert.

KD ***Wer müsste denn den Bundesnachrichtendienst (BND) auf seine Rechtsstaatlichkeit und Verfassungsmäßigkeit hin überwachen? Im neuen BND-Gesetz wird ein unabhängiges Gremium präsentiert, dessen Mitglieder jedoch von der Regierung selbst ausgesucht werden. Kann das funktionieren?***

KVN Auf jeden Fall muss man die parlamentarische Kontrolle stärken. Das Problem mit diesem Kontrollgremium ist, dass die Person, die da hingesetzt wird und die Koordination übernimmt, von der Bundesregierung benannt wird. Denn es ist immer schlecht, wenn sich die Exekutive selbst kontrolliert. Selbst wenn man in die USA fährt, sagen die Amerikaner, dass wir in Deutschland die parlamentarische Kontrolle stärken müssen.

In der Diskussion wird es häufig so dargestellt, dass in den USA alles ganz furchtbar ist und wir in Deutschland die Opfer sind – das stimmt so nicht. Denn Deutschland und seine Dienste kooperieren sehr eng mit den Amerikanern. Was per se übrigens nicht ganz verkehrt ist. Natürlich braucht man Geheimdienst-Kooperation, nur muss sie streng rechtsstaatlich erfolgen und das ist bisher nicht der Fall. Insgesamt lässt sich also festhalten: Die unterentwickelte parlamentarische Kontrolle ist ein erhebliches Problem in Deutschland.

KD ***Wie haben Sie sich gefühlt, als Sie herausgefunden haben, dass der Untersuchungsausschuss abgehört wird und diverse Handys Ihrer Kollegen angezapft wurden?***

KVN Na gut, dafür gibt es ja keinen Nachweis. Aber ich glaube, dass man schon davon ausgehen kann, dass es da ein gesteigertes Interesse gab und auch noch gibt. Der ganze Umgang mit dem Thema Überwachung hat sich hier im Haus stark verändert: Früher haben nur die Paranoiker ihre Handys vor die Tür gelegt, inzwischen tun das alle. Wenn man heutzutage vertrauliche Dinge bespricht, müssen alle elektronischen Geräte, wie Handys oder Laptops, aus dem Raum. Das ist inzwischen auch streng eingehaltene Hausordnung des Deutschen Bundestags.

KD ***In der Presse hat man von einer Metallkiste lesen können, in die alle Teilnehmer des Untersuchungsausschusses ihre Telefone legten. Zudem spielte man klassische Musik, um ein mögliches Abhören zu erschweren. Das führte sicher zu einer etwas seltsamen Stimmung oder?***

KVN Genau, das war während der ersten Phase so, wo dann im Hintergrund leise Musik dudelte. Es gibt tatsächlich vor jedem Sitzungssaal diese Schließfächer, die nun wieder zu Ehren gekommen sind. Es benutzen auch wieder mehr Leute die Haustelefone, weil diese anonymisiertes Telefonieren ermöglichen. Es gibt sogar mittlerweile Dinge, die wir gar nicht mehr elektronisch zu kommunizieren versuchen.

Die Bundesregierung hat das Problem bisher nicht lösen können: Einerseits wollen die Geheimdienste alles mitlesen, andererseits wollen wir aber die Privatsphäre und die Sicherheit unserer IT-Strukturen schützen, weil es für deutsche Unternehmen, für die Bürger und auch für die Politik existenziell ist, dass es Vertrauensschutz und ▸

*SELEKTOREN

Eine Art von Suchbegriffen, um aus großen Datenströmen gezielte Informationen zu erhalten. Selektoren können URLs, IP- und E-Mail-Adressen, Telefonnummern, MAC-Adressen oder Geokoordinaten sein. Es können aber auch Namen oder Kürzel von Unternehmen oder Behörden sein.

IT-Sicherheit gibt. Das ist einer der großen Widersprüche, mit denen wir im Augenblick leben.

KD ***»Man kann nicht 100 Prozent Sicherheit und 100 Prozent Privatsphäre und null Unannehmlichkeiten haben.«, sagte Barack Obama 2013. Wie viel Privatsphäre haben wir denn überhaupt noch? Oder müssen wir uns mittlerweile einfach abfinden, dass wir dauerhaft überwacht werden?***

KVN Der Kern von Obamas Ausspruch ist, dass es Verhältnismäßigkeit gibt. Und das ist rechtsstaatlich erst einmal nicht verkehrt. Wobei ich immer sagen würde: Alle tun so, als könnte man Sicherheit und Freiheit wie in einer Waagschale gegeneinander abwägen. Wenn man Freiheit auf null fährt, bekommt man 100 Prozent Sicherheit – das ist natürlich totaler Quatsch!

Freiheitsrechte sind ja auch Sicherheitsrechte. Vor dem Hintergrund der deutschen Geschichte bedeutet das etwa, mich vor Gewalt zu schützen. Das sind überaus wichtige Rechte. Ein konsequenter Datenschutz und eine Ende-zu-Ende-Verschlüsselung ist immer auch Vorbedingung für die Sicherheit im Digitalen. Man muss sich doch nur einmal in den Unrechtsstaaten dieser Welt umschauen, um das zu verstehen. Deswegen kann man am Rad der Freiheitsrechte nicht immer weiter nach unten drehen und dann behaupten »So, jetzt sind wir alle sicher«.

Auch in der analogen Welt gab es ja schon Überwachung, zum Beispiel via Telefon, nur musste es dafür einen konkreten Tatverdacht geben. Ich finde es richtig, wenn der Staat ein Telefon abhören darf, solange die Voraussetzungen, Schranken und rechtliche Kontrolle definiert sind. Das verheerende Problem besteht heute jedoch im Ansatz der Massenüberwachung – also zu sagen, wir sammeln erst einmal alle möglichen Daten, rastern die dann durch und gucken am Ende, ob sich daraus ein möglicher Tatverdacht ergibt. Wenn man dieser Logik folgt und die technische Entwicklung der nächsten zehn Jahre antizipiert, führt das direkt in die Hölle.

KD ***Staatliche Überwachung ist vom Prinzip also in Ordnung, so lange es einen ausreichenden Grund gibt?***

KVN Nicht ohne Grund basiert unser Rechtsstaat, darauf dass der Bürger zunächst einmal frei ist und der Staat nur bei einem konkreten Anlass etwas gegen ihn unternimmt. Wenn man dies nun umdreht, der Staat alle Bürger durchleuchtet und man sich nichts zu Schulden kommen lassen muss, um als juristisch unverdächtig zu gelten, dann verdreht man das freiheitliche Denken unseres Rechtsstaats jedoch komplett.

Genau das ist das schleichende Gift und deswegen werden die Auseinandersetzungen um die Vorratsdatenspeicherung auch so hart geführt, weil es eben um sehr viel geht. Mich irritiert es, dass nach all den Jahren weder die Union noch die SPD dieses Grundproblem offenbar verstehen. Nachvollziehen kann ich dagegen den unumgänglichen Kampf gegen den internationalen Terrorismus – so er mit Augenmaß und also rechtsstaatlich geführt wird. Dieser kostet Geld und wir müssen dafür unsere Dienste stärken. Die Abkehr vom konkreten Verdacht oder die Involvierung Deutschlands in den geheimen Krieg z.B. bei rechtswidrigen Drohnenschlägen auf Basis von Erkenntnissen aus der internationalen Massenüberwachung zeigen jedoch die Unverhältnismäßigkeit, die in den letzten Jahren entstanden ist.

*VERKEHRSDATEN

Diese Telekommunikations-Verbindungsdaten werden auch Metadaten genannt. Es geht hier nicht um den Inhalt, sondern darum wer mit wem wann wo und wie lange kommuniziert. Daraus lassen sich dann umfangreiche Bewegungsprofile und Kontaktlisten erstellen. Manche Kritiker sprechen sogar von möglichen Rückschlüssen auf den sozialen Status und die Hierarchie in der Arbeitsstelle.

KD ***Wie beurteilen Sie es, dass Edward Snowden selbst nicht vor dem NSA-Untersuchungsausschuss aussagen konnte?***

KVN Die Bundesregierung hat hier eine große Chance vertan. Wir haben Frau Merkel dazu kürzlich befragt und ihre Antwort lautete lediglich »Tja, ich habe das an die zwei SPD-Ministerien Justiz und Auswärtiges gegeben und die haben sich irgendwie noch gar nicht zurückgemeldet. Keine Ahnung, was da los ist«. Wir fragen das Justizministerium auch jede zweite Sitzungswoche, wann wir denn einmal eine Antwort erhalten, wie wir Snowden nach Deutschland holen könnten. Deren Antwort lautet jedoch stets: »Wir prüfen das noch«.

KD ***Gerade in Deutschland betrachten viele Menschen Edward Snowden mehr als Helden, denn als Verräter. Können Sie diese Sichtweise verstehen?***

KVN Für mich ist Snowden kein Held, weil ich mich mit diesem Heldenbegriff sehr schwer tue. Menschen haben gute und schlechte Seiten. In jedem Fall hat er jedoch etwas Bewundernswertes getan, in dem er sein bisheriges gut situiertes Leben aufs Spiel gesetzt hat, um wichtige Informationen uneigennützig an die Öffentlichkeit zu bringen. Wenn man sich die weltweiten Diskussionen anschaut, die daraus entstanden sind, dann ist das höchst relevant. Ebenso wenig wie Frau Merkel wusste, dass sie abgehört wird und was ihr Geheimdienst macht, war den Kontrollinstanzen in den USA bekannt, dass die NSA die inneramerikanische Kommunikation erfasst. Auch das ist durch Snowden ans Licht gekommen und dann korrigiert worden.

Ein enormer Imageschaden ist es allerdings, dass sich Snowden in Russland aufhalten muss. Dass man ausgerechnet Putin diese PR-Möglichkeit einräumt, ist diplomatisch das Eigentor des Jahrzehnts. Ähnlich den Gefängnissen von Abu Ghraib und Guantanamo oder dem ▸

Drohnenkrieg schadet es der westlichen Welt und ihren Werten erheblich. Snowden einen Verräter zu nennen, hilft uns nicht weiter – es lenkt nur von der strukturellen Frage nach Sinn und Rechtmäßigkeit dieser Massenüberwachung ab.

KD ***Knapp vier Jahre nach den Enthüllungen von Edward Snowden – hat sich denn etwas zum Besseren verändert?***

KVN Natürlich sind Dinge abgestellt worden und das BND-Gesetz hat auch ein paar Probleme angegangen, nur halt bei weitem nicht genug, teils wurde sogar die bisherige Praxis gegen alle rechtlichen Bedenken einfach legalisiert. Zudem ist es aber in der Debattenlage so, dass wir über eine ganze Reihe von Dingen nicht öffentlich reden können, die wir gelesen haben. Es hat sich etwas bewegt, aber es liegt noch ein weiter Weg vor uns.

Wir werden ganz oft gefragt, jetzt wo wir auf die Zielgerade biegen mit der Erstellung des Abschlussberichts, hat sich das alles gelohnt?

Am ehesten würde ich hier den gleichen Ton wie Snowden anschlagen, denn ich kann ja die Leute nicht belabern und ihnen sagen, was für sie das wichtigste politische Thema ist. Das muss jeder für sich selbst entscheiden. Die politische Relevanz des Themas bestimmt nicht die Politik, sondern die Öffentlichkeit von uns allen. Und wir konnten mit unserem Ausschuss im Grunde auch nur auf die Dinge hinweisen, die wir rausgefunden haben und geben als Schlussfolgerungen Hinweise darauf, welche politischen Konsequenzen daraus zu ziehen sind und die Menschen müssen dann entscheiden, ob das für sie ein wichtiges Thema ist.

KD ***Aber werden sie von den Grünen es zu einem Thema machen im Wahlkampf?***

KVN Ja, klar! Wir haben in den letzten drei Jahren mit einem enormen Aufwand diesen Untersuchungsausschuss betrieben – und noch vier weitere Untersuchungsausschüsse – da haben wir einen großen Teil unserer Arbeitskraft investiert. Wenn sie in den Sitzungen waren, dann wird ihnen der Abgrund der großen Koalition völlig bewusst. Wenn von jeder Stunde, die Union 27 Minuten, die SPD 17 Minuten und die zwei Oppositionsparteien acht Minuten fragen können. Und das geht dann Stunde, um Stunde, um Stunde bis Mitternacht. Dann bekommen sie eine Idee, was das für ein harscher Kampf ist.

Für uns sind die Bürger- und Freiheitsrechte in einer digitalen Welt eine zentrale Frage und wir werden das auf jeden Fall auf die Agenda setzen! Das kann man an den Unrechtsstaaten dieser Welt ja sehen: Man kann nur für mehr Gerechtigkeit oder eine bessere Umwelt streiten, wenn man in einer Demokratie lebt. Die Freiheit vor Überwachung ist eine Lebensgrundlage für die Demokratie.

KD ***Und dennoch ist das Thema für viele extrem abstrakt zu verstehen. Was antwortet man den Leuten auf die klassische Aussage: »Ich habe ja nichts zu verbergen?«***

*MEMORANDUM OF AGREEMENT

Im Zuge der Terrorismusbekämpfung soll es ein grundlegendes Abkommen zwischen der NSA und dem BND zum gegenseitigen Datenaustausch gegeben haben. Zudem soll der damalige Kanzleramtschef Frank-Walter Steinmeier die Operation Eikonal bewilligt haben, bei der am Frankfurter Internetknotenpunkt DE-CIX abgefangene Daten direkt an die NSA weitergeleitet wurden.

KVN Die Aussage – ich habe ja nichts zu verbergen – ist ein naiver Satz. Wer das für sich sagt, kann das natürlich tun. Dazu fällt mir eine Begebenheit ein: Ich war neulich auf einer Richtertagung, im Raum waren etwa 100 Verwaltungsrichter und der Moderator bat, dass jeder sein Handy zur Hand nimmt. Dann wurden alle gebeten, einmal die Fotos zu öffnen und dann sagte der Moderator »und jetzt reichen sie ihr Handy an den Partner links von ihnen«.

Jeder der über das Thema mal eine Viertelstunde nachdenkt oder zwei Sätze dazu liest, kann ein Gefühl dafür bekommen, was für ein gewaltiges Problem das ist: Ob als Verbraucher, Patienten, Wähler oder Privatmensch – hier will am Ende niemand gläsern dastehen. Nicht nur vor dem Hintergrund der deutschen Geschichte, auch aufgrund der aktuellen Entwicklungen.

KD ***Kann man denn sagen, dass die Leute sich bisher zu wenig mit Überwachung auseinandergesetzt haben? Bei großen Demonstrationen zu anderen abstrakten Themen wie beispielsweise TTIP waren eine viertel Million Menschen auf der Straße – und zu Überwachung?***

KVN Das stimmt schon. Obwohl wenn man mit den Leuten darüber redet, dann gibt es eine Wirkung und die Menschen passen ihr Verhalten an – leider oft in einem schlechten Sinne: Die Leute trauen sich nicht mehr sarkastische Dinge per WhatsApp zu schreiben. »Wenn das jemand liest, könnte ich missverstanden werden und sehe aus wie ein Terrorist«. Dieser Mangel an Vertrauen in die Kommunikation ist eine krasse Fehlentwicklung, die der ganzen Gesellschaft schadet.

Die Auswirkungen der Datensammelei und Überwachung treten ja nicht am Tag eins auf. Die Wirkung ist verzögert, aber wenn sie dann eintritt, ist die Empörung dann umso größer. Wenn zum Beispiel die USA anfangen, bei der Einreise nun unsere Social-Media-Accounts zu öffnen und zu gucken, was man gepostet hat und man deshalb nicht mehr in die USA einreisen darf.

KD ***Der große Protest kommt also erst noch?***

KVN Das ist schwer zu sagen, da gesellschaftliche Erkenntnisprozesse ihre Zeit brauchen. Was ist, wenn etwa der eigene E-Mail-Account gehackt wird? Jeder versteht inzwi-

schen, dass da auch jeder schlecht aussehen kann. Wenn ich Kommunikation partiell nehme und veröffentliche, sieht jeder scheiße aus (lacht). Diese Einsicht, dass Artikel 10, also der Schutz der Privatsphäre und der Vertraulichkeit, konstituierend ist für die eigene Freiheit, verstehen immer mehr Menschen.

Wenn erst einmal klar ist, was das Geschäftsmodell von Facebook ist, dann wird es große Diskussionen geben. So klickt man die AGBs von Facebook einfach an. Man liest sie nicht und wenn man sie doch liest, versteht man sie nicht. Ich verstehe sie auch nicht und ich habe zwei Staatsexamen. Und es gab mit den »Freiheit statt Angst«-Demonstrationen oder der Kampagne gegen Netzsperren ja bereits seit längerem durchaus breitenwirksame Proteste, die etwas verändert haben.

KD ***Viele sind ja auch unbeholfen im Umgang und posten dann sinnlos in ihrem Status, dass sie den AGBs widersprechen. Ist es nicht auch eine bildungspolitische Aufgabe – die alte Frage nach der Medienkompetenz?***

KVN Klar, Medienkompetenz ist immer gut. Ich verstehe den Punkt, aber auch der Staat wird nicht drum herumkommen zu entscheiden, welche Geschäftsmodelle finde ich okay und welche nicht. Noch ist dieses Szenario nur hypothetisch, aber ohne rechtlichen Schutz durchaus naheliegend: Wenn meine Apple Watch aufgrund einer Herz-Rhythmus-Störung, von der ich nichts weiß, aus meiner Krankenversicherung rausfliege und keinen Versicherungsschutz mehr habe, außer ich zahle das Dreifache des Betrages, den ich mir gar nicht leisten kann. Dann kann man auch nicht mehr im Nachhinein sagen »Ja, hast du die AGBs etwa nicht gelesen?« – gerade wenn es um solch existenzielle Fragen geht. Da hilft es auch nicht, darüber in der 4. Klasse gesprochen zu haben. Medienkompetenz ist also wichtig, aber der Staat darf sich nicht aus seiner regulatorischen Verantwortung ziehen.

KD ***Regulatorische Verantwortung? Ein Beispiel bitte.***

KVN Analoge Beispiele sind immer schief, aber: Wenn Sie in Berlin eine Currywurst essen, egal wo, an einem öffentlichen Verkaufsstand, unabhängig davon, ob sie 20 Cent oder 20 Euro kostet, gehen sie zu Recht davon aus, dass sie an dieser Currywurst nicht verrecken. Warum ist das so? Weil der Staat sagt, Ernährung ist ein sensibler Bereich: Das ist schlecht für den Rechtsstaat, wenn viele Menschen am Currywurstgenuss sterben. Deswegen ist es hart reguliert: Die Produktion, die Lieferung, der Verkauf. Und wenn was Schlimmes passiert, wird der Laden geschlossen und die Verantwortlichen kommen vor den Staatsanwalt.

Sagt man nun – es ist die Eigenverantwortung der Leute – wer eine Currywurst für 20 Cent isst und verreckt, ist selber schuld und wenn man daran verreckt, dann bitte schön. So ist nun mal die Welt, es ist wichtig, dass der Würstchenmarkt sich entwickelt – so etwas sagt ja niemand. Alle sagen ganz klar: Der Schutz der Bürger geht vor und der Staat reguliert.

Im digitalen Bereich, beim Datenschutz, findet man diese Haltung nicht. Herr Maas sagt immer nur »Facebook, wir müssen reden!«. »Fleischindustrie, wir müssen reden, Menschen wird schlecht?« – das wäre doch ein absurder Zustand.

Ich bin von meiner Grundhaltung ein sehr liberaler Typ. Ich finde eigentlich, man soll nicht alles regulieren und den Menschen Wahlmöglichkeiten lassen. Aber ich finde es im Digitalbereich einfach bizarr, wie man schlicht gar nichts macht und sich am Ende über den Vertrauensschwund und die Probleme wundert.

KD ***Was hat die Arbeit im Untersuchungsausschuss mit ihrem eigenen Vertrauensverhältnis zur Demokratie gemacht?***

KVN Der Untersuchungsausschuss ist eine gute Sache und genauso die freie Presse, die über all die Jahre berichtet hat, was dort kritisch läuft. Hier zeigt sich die Relevanz und auch Stärker unserer Demokratie und Rechtsstaatlichkeit. Das ändert aber nichts daran, dass es auch krasse Frustrationen gab: Wie etwa der Kampf um die Herausgabe von Akten, was davon (teils jenseits jeder Verhältnismäßigkeit) geschwärzt ist, welche Aussagegenehmigungen die Zeugen haben oder was genau zum Untersuchungsgegenstand gehört und was nicht.

Wenn man die Überwachungsmaschinerie als ein großes Dinosaurierskelett nimmt, dann haben wir nur einen bestimmten Bereich archäologisch ausgepinselt. Snowden hat wiederum ein anderes bisschen ausgepinselt und wir haben dann noch einmal neue Stränge erkannt. Aber es gibt eben auch weite Teile, die aus unserem Untersuchungsauftrag herausdefiniert wurden. Etwa die Frage, was der BND im Ausland macht, wo er meint, sich an überhaupt keine Gesetze halten zu müssen.

Am Ende des Tages kommt in einem Land wie der Bundesrepublik eine Bundeskanzlerin sieben Stunden in einen Ausschuss und muss unter Wahrheitspflicht Fragen von Abgeordneten beantworten. Das ist nicht so verkehrt. Und oben sitzen Journalisten auf der Bühne, bilden sich ihre Meinung und schreiben am nächsten Tag, was ihnen dazu einfällt. Das ist auch erst einmal gut. Ich habe jetzt nicht nur Glücksgefühle bezüglich dieses Ausschusses, aber ich verstehe es als ein großes Privileg, dass man diese Möglichkeiten der Aufklärung und Selbstkorrektur hat. Die Verantwortung liegt halt nicht nur bei der Politik, sondern bei Wählern, Wirtschaft und Medien gleichermaßen. Denn wenn sie einen Skandal aufdecken und allen ist es wurscht, dann passiert nun einmal nichts.

KD ***Herr von Notz, wir danken Ihnen für das Gespräch.*** •

DER ROTE FADEN

In unserem roten Faden reisen wir durch die Geschichte der Privatsphäre. Wir folgen unseren Zeitzeugen, die schon seit dem Mittelalter versuchen, endlich mal ihre Ruhe zu haben.

ILLUSTRATION MARC HEINRICH

Manchmal ist es wie mit der Henne und dem Ei – denn wenn wir über Überwachung und Digitalisierung sprechen, definieren wir auch automatisch mit, was Privatsphäre für uns bedeutet. Doch diese festzunageln ist gar nicht so einfach – denn denken wir dabei wirklich alle an dasselbe? Der Rote Faden beschäftigt sich mit der Frage, ob unsere Idee von einem Recht auf gewolltes Alleinsein schon immer so war, wie wir heute denken.

ME, MYSELF AND I

ÜBER PRIVATSPHÄRE UND DAS RECHT, ALLEIN GELASSEN ZU WERDEN

VON SYLVIA LUNDSCHIEN

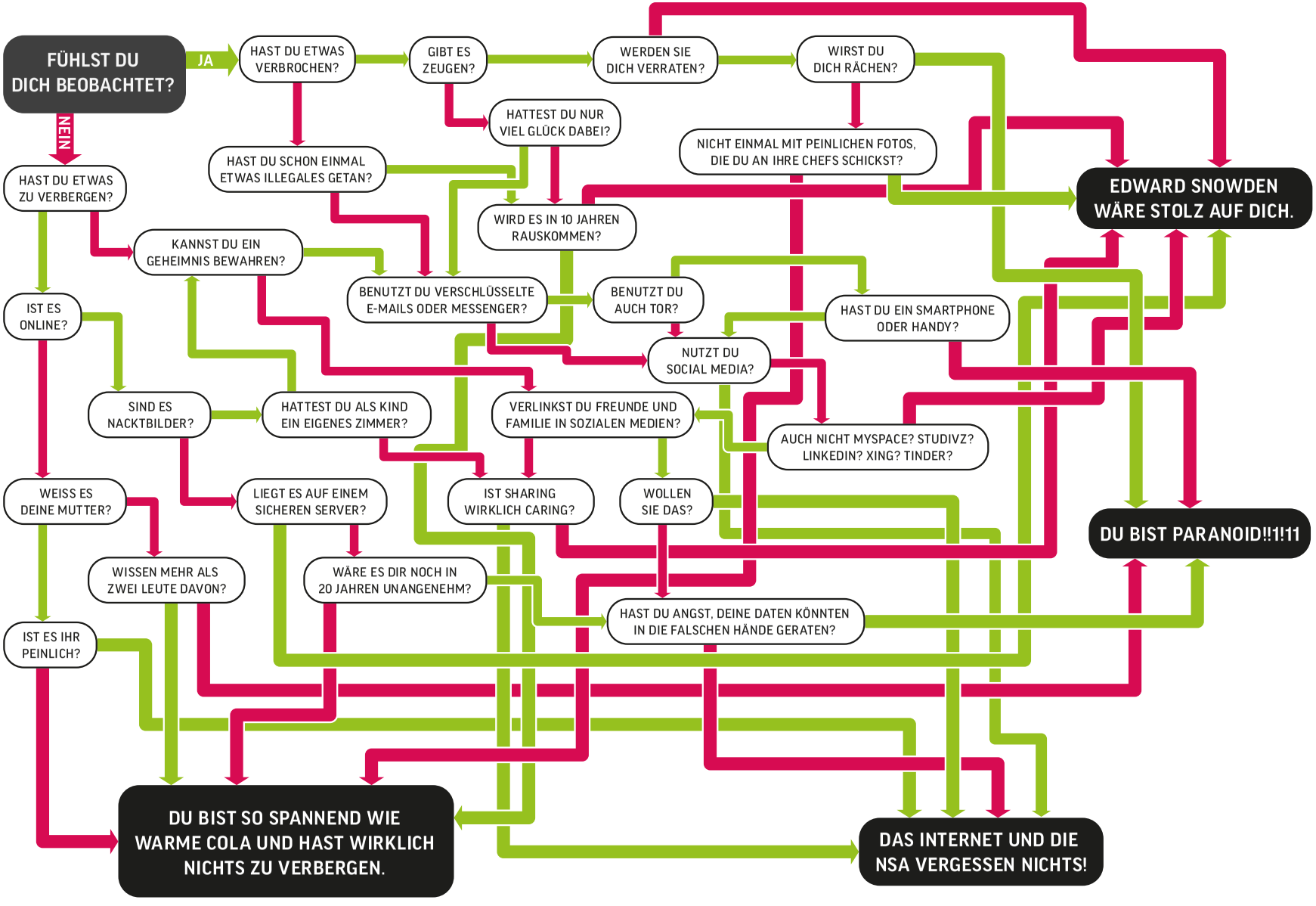
Morgens, irgendwo in Deutschland. Wer zur Schule, Uni oder Arbeit pendelt, zückt in Bus und Bahn gerne mal das Smartphone, um sich die Zeit zu vertreiben. Dabei kommt es nicht selten vor, dass etliche neugierige Augenpaare einen Blick erhaschen oder man selbst auf den Bildschirm Fremder schielt. Plötzlich weiß das halbe Abteil, wer eure Freunde sind, wie viele Bussi-Smileys ihr euren Liebsten schickt und an welches sexy Bild du gerade auf der Foto-App Instagram ein Herzchen vergibst. Peinlich? Nö, denn wir haben ja nichts zu verbergen und rechtfertigen müssen wir uns schon gar nicht. Ist doch alles Privatsache. Aber kommt es niemandem komisch vor, dass wir intime Nachrichten über öffentliche Netzwerke schicken, für die Ewigkeit bei Instagram im Bikini posieren oder der Facebook-Community unsere gesamte Familie vorstellen? Wie passt es da, dass wir gleichzeitig darüber jammern, wenn eine App plötzlich Zugang zu unseren Fotos und Kontakten will?

PRIVATSPHÄRENSTATUS: IT'S COMPLICATED

Früher war es mit der Privatsphäre nicht weniger kompliziert. Historisch lebt die Mehrheit in Zentraleuropa erst seit Kurzem in einem eigenen Haus, Wohnung oder Zimmer, in die man sich zurückziehen kann. Noch bis Mitte des 20. Jahrhunderts zwängten sich Großfamilien in winzige Häuser oder enge Zimmer; auch eine Institution wie der Dorftratsch hat die Digitalisierung bisher erfolgreich überlebt. Privatsphäre als unbehelligter Rückzug in die eigenen vier Wände war lange vorrangig ein Privileg gesellschaftlich gehobener Schichten. Diese verfügten über genügend Platz für separate Räume zum Essen, Schlafen oder Waschen; oft gab es auch Räume für das Personal, für Gäste oder die eigene Freizeitgestaltung. Die bürgerliche Vorstellung davon, Zeit und Raum nur für sich zu beanspruchen, ist auch bis in die Rechtsprechung gesickert. So wurde im 20. Jahrhundert in Deutschland das »Allgemeine Persönlichkeitsrecht« (APR) als das Recht auf Privatsphäre formuliert. Diese gesetzliche Regulierung zeichnet nach, wie schwierig es bisweilen ist, eine klare Linie zwischen Außen und Innen zu ziehen. Zudem ist diese Linie auch noch ständig in Bewegung – und zwar innerhalb der Gesellschaft und auch innerhalb von sozialen Gruppen und Szenen, für die Privatsphäre etwas anderes bedeuten kann als für den Mainstream.

ALLEINSEIN NACH MATROSCHKA-PRINZIP

Hinzu kommen ganz unterschiedliche globale Interpretationen von »Privatsphäre« und »freiwilligem Alleinsein«, die sich in kulturellen, sozialen, räumlichen und juristischen Normen ausdrücken. So unterscheidet das APR in Deutschland mindestens drei soziale Sphären, die wie ein verschachteltes Paket aus drei Lagen bestehen: Außen gibt es eine große Box namens Individualsphäre, mit der wir uns in der Öffentlichkeit bewegen – also auf der Straße, im Bus oder im Büro. Diese Sphäre ist am wenigsten vom APR geschützt, da in diesem Bereich bei Konflikten andere Gesetze wie zum Beispiel das Ordnungs- oder Arbeitsrecht viel besser greifen. In dieser großen Box steckt wiederum die juristische Idee der Privatsphäre – also Dinge, die wir nur mit engen Freunden oder der Familie teilen. Dazu zählen auch die Unverletzlichkeit unseres Zuhauses sowie das Recht darauf, dass niemand unsere Post mitliest und das Telefon abhört. Schließlich findet sich ganz tief unten in der Box die Intimsphäre. Dort sind wir ganz bei uns selbst – Tagebucheinträge, Sexualität, aber auch Krankheiten, Intimpflege und Körperfunktionen gehen in der Regel niemanden etwas an, im Zweifelsfall nicht einmal unsere Familie oder Partner.


FÜHLST DU DICH BEOBACHTET?
JA
NEIN
HAST DU ETWAS VERBROCHEN?
GIBT ES ZEUGEN?
WERDEN SIE DICH VERRATEN?
WIRST DU DICH RÄCHEN?
HATTEST DU NUR VIEL GLÜCK DABEI?
NICHT EINMAL MIT PEINLICHEN FOTOS, DIE DU AN IHRE CHEFS SCHICKST?
HAST DU SCHON EINMAL ETWAS ILLEGALES GETAN?
HAST DU ETWAS ZU VERBERGEN?
EDWARD SNOWDEN WÄRE STOLZ AUF DICH.
WIRD ES IN 10 JAHREN RAUSKOMMEN?
KANNST DU EIN GEHEIMNIS BEWAHREN?
BENUTZT DU VERSCHLÜSSELTE E-MAILS ODER MESSENGER?
BENUTZT DU AUCH TOR?
HAST DU EIN SMARTPHONE ODER HANDY?
IST ES ONLINE?
NUTZT DU SOCIAL MEDIA?
SIND ES NACKTBILDER?
HATTEST DU ALS KIND EIN EIGENES ZIMMER?
VERLINKST DU FREUNDE UND FAMILIE IN SOZIALEN MEDIEN?
AUCH NICHT MYSPACE? STUDIVZ? LINKEDIN? XING? TINDER?
WEISS ES DEINE MUTTER?
LIEGT ES AUF EINEM SICHEREN SERVER?
IST SHARING WIRKLICH CARING?
WOLLEN SIE DAS?
DU BIST PARANOID!!1!11
WISSEN MEHR ALS ZWEI LEUTE DAVON?
WÄRE ES DIR NOCH IN 20 JAHREN UNANGENEHM?
HAST DU ANGST, DEINE DATEN KÖNNTEN IN DIE FALSCHEN HÄNDE GERATEN?
IST ES IHR PEINLICH?
DU BIST SO SPANNEND WIE WARME COLA UND HAST WIRKLICH NICHTS ZU VERBERGEN.
DAS INTERNET UND DIE NSA VERGESSEN NICHTS!

In Deutschland stützt sich das APR auf Artikel 1 und 2 des Grundgesetzes (Schutz der Menschenwürde und freie Entfaltung der Persönlichkeit). Das klingt erst einmal gewichtig, doch wägt man das Recht auf Privatsphäre auch gegen öffentliches Interesse ab. Decken Journalisten beispielsweise auf, dass ein Politiker Sparsamkeit predigt, aber Steuergelder für seine Villa verpulvert, dann greift das APR nicht. Auch die Kunst- und Meinungsfreiheit schränken das APR ein, vor allem, wenn es um die Privatsphäre von Personen des öffentlichen Lebens geht. Der Staat kann das Recht auf Privatsphäre ebenfalls einschränken, wenn von einer Person beispielsweise Terrorgefahr ausgeht oder man ein schwerwiegendes Verbrechen hinter geschlossenen Türen vermutet. Unantastbar bleibt hingegen die Intimsphäre, deren Verletzung in der Regel saftige Strafen nach sich zieht.

DAS RECHT AUF DIGITALE INTIMSPHÄRE

2008 versuchte man in Deutschland, das Thema Privatsphäre ins 21. Jahrhundert zu bringen. Denn was nützt das einstige Recht darauf, dass unsere Briefe nicht gelesen und unser Haustelefon nicht angezapft wird, wenn Kommunikation heute überwiegend digital erfolgt? Das etwas hölzern klingende »Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme« versucht seit gut einem Jahrzehnt, die technologischen Innovationen der letzten 25 Jahre zu berücksichtigen. Dieses »Recht auf digitale Intimsphäre« ist eine Art Selbstzensur für den Staat, die Bürger nicht anlasslos und unbemerkt auf digitalem Weg auszuhorchen. Denn wer sich bespitzelt fühlt, hält in vielen Situationen lieber den Mund. Die Befürchtung ist, dass dadurch kein echter öffentlicher Meinungsaustausch mehr stattfindet und dies die Gesellschaft in ihrer demokratischen Mitwirkung schwächt.

So viel zur Theorie – denn jetzt liegt es an uns: Mitmachen und weiterhin fleißig liken, swipen und Herzchen verteilen? Oder lieber digitaler Detox und unterhalb des Radars leben? Obwohl wir wissen, dass unsere Daten und damit auch ein Teil unseres Lebens immer öffentlicher werden, machen wir weiter. Der Rote Faden begleitet Euch bei diesen Fragen in kleinen historischen Skizzen. Sie zeigen: Es war nie wirklich einfach, sich für eine Seite zu entscheiden. •

DER ROTE FADEN

OPERATION ACOUSTIC KITTY

TEXT YANNICK VON EISENHART ROTHE
ILLUSTRATION PAUL STURM

Es gibt Geschichten, die so perfekt passen, dass sie erstmal unglaubwürdig klingen. Hallo, wir sind Kater Demos, wir machen ein Politikmagazin mit Cat Content, in dieser Ausgabe geht es um Überwachung. Achja, übrigens, passt ganz gut, die CIA hat mal Mikrofone in Katzen verpflanzt, um damit die Russen zu belauschen. Ach komm, so ein Quatsch, glaubt doch kein Mensch. Stimmt aber.

Wie 2001 deklassifizierte CIA-Dokumente belegen, gab es im Kalten Krieg tatsächlich Versuche, Katzen zur Überwachung einzusetzen. Die präparierten Tiere sollten abgerichtet werden und unauffällig durch den Garten der russischen Botschaft in Washington, D.C. streunen, um dort Gespräche mitzuschneiden. Mitarbeiter der Botschaft hatten nämlich entdeckt, dass die Amerikaner das Gebäude verwanzt hatten und daraufhin vertrauliche Gespräche nach draußen verlegt. Da es aber etwas auffällig gewesen wäre, den Kätzchen einfach ein fellfarbenes Mikrofon um den Hals zu hängen, begann die CIA unter dem Projektnamen »Acoustic Kitty« mit Versuchen, den Tieren die Abhörtechnik zu implantieren. Der ehemalige CIA-Agent Victor Marchetti erzählte der britischen Zeitung The Telegraph: »Sie schlitzten die Katze auf, steckten Batterien hinein und verkabelten sie. Der Schwanz wurde als Antenne genutzt. Sie erschufen eine Monstrosität.« In die Gehörgänge wurden Mikrofone eingesetzt und damit der tierische Agent nicht durch Mäuselust von seiner Mission abgelenkt werden konnte, wurde zusätzlich sein Hungergefühl künstlich unterdrückt.

Nach mehrjähriger Forschung war die erste »Acoustic Kitty« 1966 bereit zum ersten Testeinsatz. Doch dieser endete tragisch: Die Katze schaffte es nur wenige Meter aus dem CIA-Van und wurde dann von einem Taxi überfahren. »Da saßen sie, in ihrem Van voll mit Empfangsgeräten und die Katze war tot,« erinnert sich Verchetti.

Kurz darauf wurde die Operation eingestellt, nach knapp fünf Jahren Forschung und Kosten von geschätzt 15 Millionen US-Dollar. Der teilgeschwärzt veröffentlichte Abschlussbericht der CIA will die Operation trotzdem als Erfolg verkaufen. Der Einsatz von Katzen zur Abhörung habe sich zwar für ihre Zwecke als unpraktikabel erwiesen. Die Forscher hätten mit ihrer Arbeit jedoch gezeigt, dass dies möglich sei, was »an sich eine bemerkenswerte wissenschaftliche Errungenschaft« sei. Sie könnten mit ihrer »Energie und Vorstellungskraft Vorbilder für Pioniere der Wissenschaft« sein. Besonders wird die Leistung gepriesen, dass Katzen erstmals abgerichtet wurden und auf Befehl kürzere Distanzen zielgerichtet zurücklegten. Leider scheinen die Forscher es versäumt zu haben, die Konzepte Fußgängerampel oder Zebrastreifen in ihren Unterricht einzubauen.

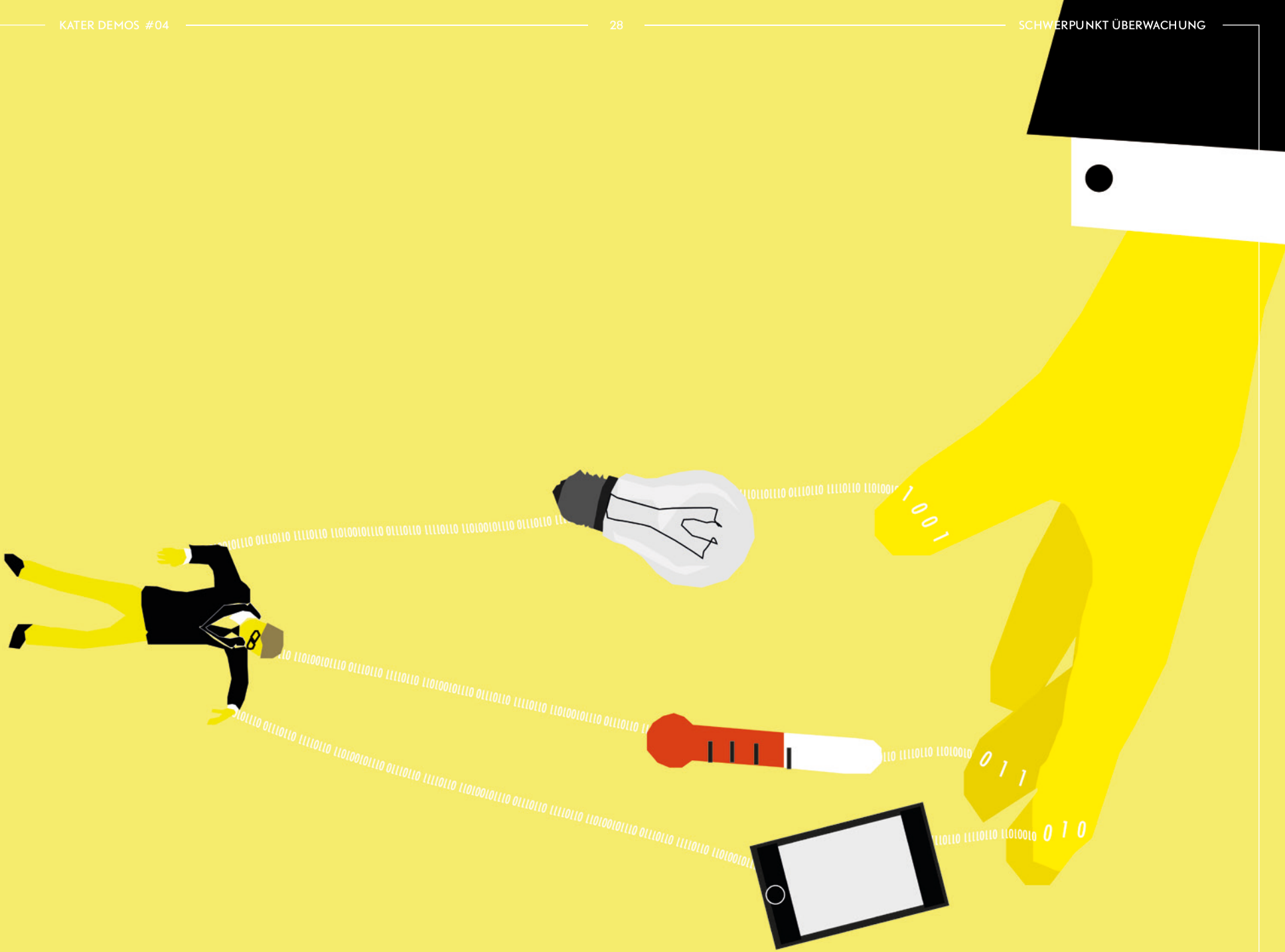
Die britische Filmemacherin Jennifer Sheridan fand »Acoustic Kitty« so bizarr und spannend, dass sie die Geschichte in einem gleichnamigen Kurzfilm adaptiert hat. In ihrer Version hat Agent Cooper die grandiose Idee, Katzen zur Überwachung einzusetzen. Weil er aber zunächst »genug tote Katzen, um Shanghai zu füttern« produziert (politisch nicht ganz korrekte Aussage seines Vorgesetzten), wird er zum Gespött seiner Kollegen und auf den Fluren mit hämischem Miauen bedacht. Schließlich schafft er es doch, eine Katze überlebt: Agent Mr. Pickles ist einsatzbereit. Spoiler-Alarm: Ein Happy End bleibt aus.

»Acoustic Kitty« ist einer der wenigen belegten Fälle, bei denen Tiere zur Überwachung eingesetzt wurden. Bis auf Brieftauben, die schon öfter mal verschlüsselte Botschaften zwischen Spionen transportierten, ist wenig nachgewiesen. Verdächtigungen gab es aber schon öfter: 2011 beispielsweise fing ein Jäger in Saudi-Arabien einen Geier, der einen GPS-Sender der Universität Tel Aviv trug. Daraufhin schrieben einige lokale Zeitungen, dass der Vogel ein israelischer Spion sei. Israel versicherte belustigt, dass der Sender lediglich Forschungszwecken diene. Das Land wurde schon so oft verdächtigt, Tiere als Spione einzusetzen, dass es in der englischen Wikipedia einen ganzen Artikel zu Verschwörungstheorien bezüglich israelischer Tiere gibt.

Die CIA hat aber gezeigt, dass nicht jede krude klingende Geschichte gleich ins Reich der Fabeln verwiesen werden kann. Schau also demnächst zweimal hin, wenn Deine Nachbarskatze mal wieder den ganzen Tag durch Deinen Hinterhof streunt. •

FILMTIPP

»Acoustic Kitty« (2014), Kurzfilm


1001
011
010

SMART NEW WORLD

Marco Maas' Wohnung weiß viel über ihn. Sie weiß, wie lange er schläft, wann er zu Hause ist, welche Musik er gerne hört und was er wann gerne isst. Marco ist Technikfreund und Datenjournalist – 130 Geräte sind in seiner Wohnung miteinander verbunden. Was macht es mit uns und unseren Beziehungen, wenn die Technik unseren Alltag dominiert? Eine Reise in die Zukunft.

TEXT LARISSA ROBITZSCH
ILLUSTRATION SOPHIE DREHER

Marco Maas ist vernetzt. Mit einem Knopfdruck kann er seinen Fernseher ein- und ausschalten – egal, ob er in New York, Tokio, Südafrika oder zu Hause bei sich auf dem Sofa sitzt. Er braucht dafür nur sein Smartphone.

Seine Freundin Yong-Er kann das nicht. Wenn sie keine Lust hat, zur Fernbedienung zu greifen, schreibt sie Marco einfach eine Nachricht. Sie akzeptiert zwar den vernetzten Haushalt, hat sich aber nicht alle Apps heruntergeladen. Auch wenn Marco nicht zu Hause ist, kann er sehen, wann seine Freundin im Badezimmer ist, Klavier spielt, Musik hört, wann sie das Haus verlässt und wann sie zurückkommt. Privatsphäre? Fehlanzeige. Marco und Yong-Er teilen sich eine 65 Quadratmeter große Wohnung im Hamburger Stadtteil St. Pauli. Insgesamt sind 130 Geräte in der Wohnung miteinander vernetzt und versenden ständig Daten an verschiedene Server weltweit.

Aber Marco lässt sich nicht nur von den Geräten überwachen, sondern überwacht sie im Gegenzug ebenfalls: Mithilfe eines kleinen Computers analysiert er, wohin die gesammelten Daten gehen und in welchen Clouds sie gespeichert werden.

»60 bis 70 Prozent der Daten landen in den USA. Für solche großen Datenmengen muss es eine entsprechende Infrastruktur geben und die haben eben nur Firmen wie Amazon und Google«, sagt der Datenjournalist.

Von der Lampe bis zur Heizung, vom Bett bis zum Fernseher: Alles ist so programmiert, wie Marco sich das wünscht. Wenn seine Freundin zu Hause ist, ist das Licht heller, bei ihm strahlt es eher indirekt. Sind beide zu Hause, ist es eine Mischform.

»BIST DU ALLEIN?«

Die neue Technik wirkt sich auch auf das Beziehungsleben der beiden aus. In der intelligenten Wohnung wird jede kleine Notlüge ohne große Mühe aufgedeckt – das Vertrauen wird auf eine neuartige Probe gestellt. Mit CO_2-Sensoren, Kameras oder einer smarten Matratze kann Marco schnell feststellen, wann seine Freundin wirklich zu Hause ist. Auch ob sie den Abend zuvor allein in der Wohnung verbracht hat oder Besuch hatte, kann er problemlos überprüfen.

Einmal startete Marco ein interessantes Experiment: Er installierte CO_2-Sensoren in der Wohnung, die messen sollten, wie viel Luft in einem Zimmer verbraucht wird und ob die Luft schlechter oder besser wird. Ein LED-Licht sollte zeigen: Grünes Licht heißt gute Luft, bei rotem Licht sollte das Fenster mal wieder geöffnet werden. ▸

Um zu sehen, wie viel Luft eine Person durchschnittlich verbraucht, testete Marco, wie sich der Luftverbrauch im Wohnzimmer entwickelt, wenn eine Person anwesend ist. Am nächsten Tag im Büro verfolgte er die Luftentwicklung im Wohnzimmer live auf seinem Smartphone. Er stellte fest: Die Kurve verlief viel steiler als am Vortag. Er begann zu rechnen: Wie viele Personen müssten in dem Raum anwesend sein, damit die Werte mit dem zuvor gemessenen Luftverbrauch zusammen passen? Das Ergebnis: 2,6. Er rief zu Hause an und fragte seine Freundin, wer denn gerade alles in der Wohnung sei. Sie antwortete ihm, dass eine Mutter und ihr sechsjähriges Kind zum Klavierunterricht da seien.

»So etwas führt natürlich zu Gesprächsbedarf. Meistens ist es in Beziehungen so, dass eine Person technikversiert ist und die andere Person das erträgt. Derjenige, der die Technologie beherrscht, hat einen großen Informationsvorteil und die Möglichkeit, den anderen auszuspionieren. Wenn man ein Problem mit Vertrauen hat, ist das echt übel«, sagt der Datenjournalist. »Meine Freundin akzeptiert das, weil sie weiß, dass ich ihr nicht hinterherspionieren möchte, sondern mich in so einem Fall frage, ob ich eine Formel falsch berechnet habe.«

DIGITALE EIFERSUCHT

Marco ist der Ansicht, dass es in einer gesunden Beziehung auch in Zukunft nur eine theoretische Option bleiben wird, die Partnerin oder den Partner zu überwachen. Aber wie viele Beziehungen haben heute schon schwere Krisen erlebt, weil WhatsApp viel verrät: Die Nachricht ist schon gelesen, aber noch nicht beantwortet. Zuletzt online um 03:24 Uhr. Hat der andere also einfach nur schlecht geschlafen oder die Nacht durchgefeiert?

Marco hat auch eine Bettunterlage, die mit 200 Sensoren ausgestattet ist und das Schlafverhalten von zwei Personen überwachen kann. Sie misst genau, wie oft man sich in der Nacht dreht, wann man eingeschlafen ist, wann die Tief- und wann die Langschlafphasen sind. Auch das Sexleben kann damit aufgezeichnet werden. In der ersten Version der App konnte der Anbieter auf alle Daten erhobenen Daten zugreifen. Das ist in der aktuellen Version laut Aussage des Herstellers nicht mehr möglich. »Ob diese Daten wirklich nicht mehr erhoben werden, weiß ich nicht. Letztendlich bleibt mir nichts anderes übrig, als dem Hersteller zu vertrauen«, sagt Marco.

WILLKOMMEN, SMARTE WELT

Zu zweit sind Marco und Yong-Er in ihrer gemeinsamen Wohnung schon lange nicht mehr. Die intelligente Sprachassistentin Alexa unterstützt die beiden, wo sie nur kann. Sobald man ihren Namen sagt, antwortet sie. Wenn man alles per Sprache steuert, das Licht über den Bewegungsmelder angeht, die Musik in den Räumen gesteuert wird – Will man darauf irgendwann nicht mehr verzichten? Marco ist überzeugt davon, dass sich die Smart Homes durchsetzen werden. Anfangs hatte er noch neun Apps auf seinem Handy installiert. Jetzt braucht er nur noch zwei, um die Geräte in der Wohnung zu steuern. Mit Assistentin Alexa sind die Apps bald völlig überflüssig.

Seit fast drei Jahren läuft Marco Maas' Projekt einer immer smarter werdenden Wohnung. Ihn treibe der Wissensvorsprung in Bezug auf technische Entwicklungen voran, sagt er. In seinem Experiment, das gleichzeitig sein Zuhause ist, testet er, wie praktisch die Technik im Alltag ist, wo sie ihn einschränkt und wo sie ihm hilft, Probleme zu lösen. »Ich verändere mich konstant. Dank der Datenerfassung habe ich mehrere Metriken, die mir helfen, die größten Potentiale hierfür zu finden. Da geht es dann primär um Bewegung, Ernährung und Schlaf«, sagt Marco.

IN DER INTELLIGENTEN WOHNUNG WIRD JEDE KLEINE NOTLÜGE OHNE GROSSE MÜHE AUFGEDECKT

Marco will herausfinden, welche Probleme durch ein Smart Home entstehen und welche Lösungen es dafür geben kann. Als Datenjournalist interessiert er sich schon berufsbedingt für die Thematik – und verdient damit sein Geld. Mit seiner Firma Datenfreunde forscht er an der Mediennutzung der Zukunft und versucht herauszufinden, welche Rolle dabei das Smart Home spielt.

»Die spannenden Themen eines Smart Home sind nicht der Kühlschrank, der neue Milch bestellt, sobald die alte verbraucht ist. Es geht darum, welche Auswirkungen das Smart Home auf Themen wie Beziehung und Eifersucht oder Gleichberechtigung hat, vor allem, wenn eine Person mehr weiß als die andere. Wie kann man den Komfort aufrechterhalten ohne die Privatsphäre zu vernachlässigen? Welche Kompromisse müssen eingegangen werden?«, erklärt Marco.

Er hatte mal die Idee eines Badezimmerbaukastensystems. Dabei erkennt der Badezimmerschrank, wer vor ihm steht, woraufhin personalisierte Nachrichten angezeigt werden. So wird zum Beispiel für das Kind beim Zähneputzen die Lillyfee-App aufgerufen, für die Mutter die Wirtschaftsnachrichten und den Vater das Feuilleton. Aber es gibt ein Problem: »Um die Person zu erkennen, die vor dem Spiegel steht, ist eine Kamera notwendig. Und möchte man wirklich, dass eine Kamera filmt, während man morgens nackt im Badezimmer steht? Und kann man überhaupt sicher sein, dass diese Bilder dann nicht über ein System in einer Cloud gespeichert und schlimmstenfalls weiterverbreitet werden?« Viel besser sei da doch das Smart Home, das automatisch erkennt, wer sich in welchem Raum befindet.

Kameras gibt es in seiner Wohnung bisher nicht. Aber er überlegt, eine Kamera an seiner Haustür anzubringen, die überprüft, wer dort steht und ob die Person hereingelassen werden darf. Was ihn daran hindert? »Was ist mit den Persönlichkeitsrechten der Personen, die an der Wohnungstür in einem Mehrparteienhaus einfach nur vorbeilaufen und dabei aufgezeichnet werden? Dafür müsste ich Rechtsbruch begehen.«

Doch das System Smart Home ist angreifbar. Bisher sind Marco Maas keine Hackerangriffe auf seine Wohnung bekannt. Der Router ist gut abgesichert, es gibt mehrere WLAN-Netzwerke und eine gute Firewall. Sobald Marco jedoch jemandem die Passwörter seines Routers oder des WLANs gibt, entsteht eine Sicherheitslücke. Dazu kommt die Möglichkeit eines Angriffs durch das Smart Home selbst, bei Sicherheitslücken auf Seiten der Anbieter.

»Der Fall wird kommen, dass jemand bei einer Sicherheitslücke zum Beispiel 12 Millionen Lampen eines Herstellers übersteuert, die dann erhitzen und kaputtgehen. Eventuell sind es auch Firmen selbst, weil sie wollen, dass man sich neue Lampen kauft. Damit wird dann die Infrastruktur der Smart Homes weiter ausgebaut«, stellt Marco sich vor.

GOODBYE PRIVATSPHÄRE, ADIEU DATENSCHUTZ?

Was mit den Daten, die in einem Smart Home anfallen, passiert, weiß Marco nicht genau. Insgesamt 600 MB fließen pro Tag unkontrolliert durch die gemeinsame Wohnung. Welche Datenschutzgesetze gelten für Daten, die in Deutschland entstehen und in den USA und den Niederlanden zwischengespeichert werden?

Die Datenschützer aller Bundesländer sind sich uneinig und auch Marco ist sich nicht sicher, ob er als Betreiber der Geräte, die er in seiner Wohnung installiert hat, die rechtliche Verantwortung für die Aufzeichnung der Daten trägt. »Rechtlich ist nicht geklärt, welches Land wirklich zuständig ist. Momentan ist das eine komplette Grauzone«, meint Marco.

Trotzdem werde sich die Technik Smart Home und damit auch die Möglichkeit der Überwachung ausbreiten, da ist sich Marco sicher. »Die Frage lautet nicht: Finde ich das gut oder nicht? Dass die Technik Einzug in unser Leben finden wird, ist sicher. Wir können nur versuchen Wege zu finden, um unsere Privatsphäre mehr zu schützen. Solange sie einen Nutzwert für die Menschen hat, werden sie die Produkte auch kaufen«, meint Marco.

Die Technik ist dem Datenschutz dabei immer einen Schritt voraus. »Über die Technologie werden Fakten geschaffen. Wenn die Produkte gekauft werden, ist die Situation erstmal da und erst dann kann nachgebessert werden«, so Maas. »Wenn du akzeptierst, dass Technik sich disruptiv und nicht linear durchsetzt, kannst du versuchen damit umzugehen und die richtigen Fragen stellen.«

Solange sie einen Mehrwert hat, ist Datensammlung für Marco halb so schlimm. Er glaubt nicht daran, dass man sich davor schützen kann: »Man kann vielleicht eine Pseudonymisierung einrichten. Das wird ein möglicher Kompromiss sein, aber der Hersteller wird immer mehr über dich wissen. Zu wenige Menschen haben das Thema Datenschutz überhaupt auf der Agenda. Wir haben es größtenteils mit multinationalen Konzernen zu tun, die sich nicht an Staatsgrenzen halten müssen. Ich kann ein Gerät in den USA kaufen, in Deutschland benutzen und die Daten werden in Kanada gespeichert.«

»WENN DER SERVICE GUT IST, SETZT SICH DAS DING DURCH.«

Dabei kann Überwachung durchaus ihr Gutes haben: Kurz vor Ostern hat sich Marco ein neues Elektrofahrrad gekauft; leider wurde es direkt am zweiten Tag geklaut. Im Fahrrad befand sich jedoch ein GPS-Sensor, der es dem Technikfreund ermöglichte, den Weg, den der Dieb mit dem Fahrrad zurück legte, nachzuverfolgen. Den Dieb erwischte er zwar nicht, aber immerhin konnte er das Fahrrad zurückholen.

»In dem Moment, in dem mein Fahrrad geklaut wurde, ist mein einziges Interesse, dass ich es wieder zurückbekomme. Dafür nehme ich dann auch Überwachung in Kauf – weil sie mir hilft. Aber was das für eine Gesellschaft bedeutet, das sehe vielleicht ich, weil ich mich damit beschäftige, aber noch längst nicht jeder«, sagt Maas, der beim Fahrradkauf unterschrieben hat, dass der Hersteller seine GPS-Daten speichern darf. »Ich lasse mich überwachen, aber der Gegenwert dafür ist, dass mein Fahrrad sicherer ist. Obwohl ich auf einer großen Ebene gegen Überwachung bin, bin ich es auf dieser kleinen doch wieder nicht. Das ist ein Deal, den ich gerne eingehe.«

Und was ist, wenn die Geräte irgendwann intelligenter sind, als sie sein sollen, und eigenständig Entscheidungen treffen? Wenn das Haus nicht möchte, dass man es verlässt und einfach die Türen abschließt? »Das halte ich für sehr unwahrscheinlich«, sagt Marco und schließt hinter sich die Tür. •

WAS VON SNOWDEN ÜBRIG BLIEB

Nach den Enthüllungen durch Edward Snowden im Juni 2013 war die Aufregung groß. Manche sahen durch die Massenüberwachung unsere Demokratie gefährdet, andere sprachen bereits von einer unfreien Gesellschaft. Wie sieht es vier Jahre später aus? Wie viel Macht haben die Geheimdienste und wie steht um den Schutz unserer Privatsphäre?

TEXT RAIMON KLEIN
ILLUSTRATION JANA VAN THIEL

Leicht verstrubbelte Haare, Dreitagebart und etwas blass um die Nase: Eher unscheinbar sieht er aus, dieser 29-jährige Geheimdienstmitarbeiter, wie er da in seinem Hotelzimmer in Hongkong sitzt und darauf wartet, dass die Kamera zu filmen beginnt. Viel geschlafen hat er wahrscheinlich nicht, wenn man bedenkt, was er der Öffentlichkeit gleich verkünden wird: »Es gibt eine Infrastruktur in den USA und auf der ganzen Welt, die von der NSA in Kooperation mit anderen Regierungen errichtet wurde, mit der im Prinzip jegliche digitale Kommunikation abgefangen wird.«

Als Edward Snowden dies im Juni 2013 publik machte, saß der Schock tief. Zu umfangreich waren die enthüllten Überwachungsprogramme PRISM, Tempora oder XKeyscore. Zu allumfassend war die Macht der Geheimdienste, damit tun und lassen zu können, was sie wollen. Deren standardmäßige Argumentation – der Kampf gegen den internationalen Terrorismus – wurde von Snowden als Mythos entlarvt.

Um abgehört zu werden reichte es schon, sein Handy zu benutzen, eine E-Mail zu verschicken oder im Internet zu surfen. Durch PRISM etwa hatte die National Security Agency (NSA) einen direkten Zugriff auf die Server von Google, Facebook oder Apple und damit auch auf alle Dateien, Dokumente und Verbindungsdaten der Nutzer. Damit konnten dann Bewegungsprofile und Kontaktlisten erstellt werden. »Wenn ich in Ihre E-Mails oder in das Telefon Ihrer Frau hineinsehen wollte, müsste ich nur die abgefangenen Daten aufrufen. Ich kann Ihre E-Mails, Passwörter, Gesprächsdaten und Kreditkarteninformationen bekommen«, erklärte Edward Snowden.

SICHERHEIT VS. PRIVATSPHÄRE

Eine anlasslose und verdachtsunabhängige Massenüberwachung der Bürger – das kannte man bis dahin nur aus Diktaturen oder Science-Fiction-Filmen. Die Reaktionen in Deutschland waren heftig: »Wenn dauernd und massen- ►

haft Grundrechte gebrochen werden, ist die Demokratie bedroht und die Republik gefährdet«, sagte der Journalist und Verleger Jakob Augstein. Die damalige Justizministerin Sabine Leutheusser-Schnarrenberger mahnte: »Eine Gesellschaft ist umso unfreier, je intensiver ihre Bürger überwacht, kontrolliert und beobachtet werden.« Angela Merkels erste Reaktion war eine höfliche Aufforderung an Barack Obama, doch bitte die Balance zwischen dem Sicherheitsbedürfnis der Bürger und ihrem Recht auf Privatsphäre zu wahren. Ihr berühmter Satz zum Ausspähen unter Freunden kam ihr erst Monate später über die Lippen, als sie durch das Abhören ihres Handys persönlich betroffen war.

In der deutschen Bevölkerung wurde das Thema zunächst weniger wahrgenommen. In einer kurz nach Snowdens Veröffentlichungen durchgeführten YouGov-Umfrage sagte knapp die Hälfte der Befragten, dass sie sich nicht von der NSA überwacht fühlten. Sie wollten Facebook, Skype oder Google Mail weiterhin für ihre private Kommunikation nutzen. Knapp zwei Jahre später hatte sich die Stimmung gedreht: Bei einer Umfrage von Amnesty International im Februar 2015 waren fast 70 Prozent der Deutschen gegen die Überwachung ihrer Internet- und Mobilfunknutzung durch die eigene Regierung. Noch höher fiel die Ablehnung gegenüber der NSA aus: 81 Prozent fanden, dass US-Behörden in Deutschland nicht überwachen sollten.

EIN BISSCHEN AUSSPÄHEN UNTER GUTEN FREUNDEN

Was war passiert? Nun, Merkels Handy abzuhören war nicht das einzige Vergehen der NSA auf deutschem Boden. Auch hunderte andere Politiker, Entscheidungsträger und Wirtschaftsvertreter wurden ausgespäht. Verstörend kam hinzu, dass der Bundesnachrichtendienst (BND) seinen amerikanischen Kollegen bei der Massenüberwachung kräftig zur Seite stand. Aus seiner eigenen Fernmeldeaufklärung übermittelte der BND Milliarden Metadaten – also wer mit wem wann wo und wie lange kommuniziert – an die NSA. Die unterstützte damit unter anderem auch den Drohnenkrieg, den das US-Militär von seinem Stützpunkt im rheinland-pfälzischen Ramstein aus führt. Wie eng die Zusammenarbeit von deutschem und amerikanischem Geheimdienst war, zeigte die Operation Eikonal: Ende 2014 wurde bekannt, dass der BND am Frankfurter DE-CIX – einem der größten und wichtigsten Internetknoten der Welt – einen beträchtlichen Teil der dort abgefangenen Daten direkt an die NSA weitergeleitet hatte. Praktischerweise konnten sich die Deutschen dabei an eine Liste so genannter Selektoren halten, also eine Art von Suchbegriffen.

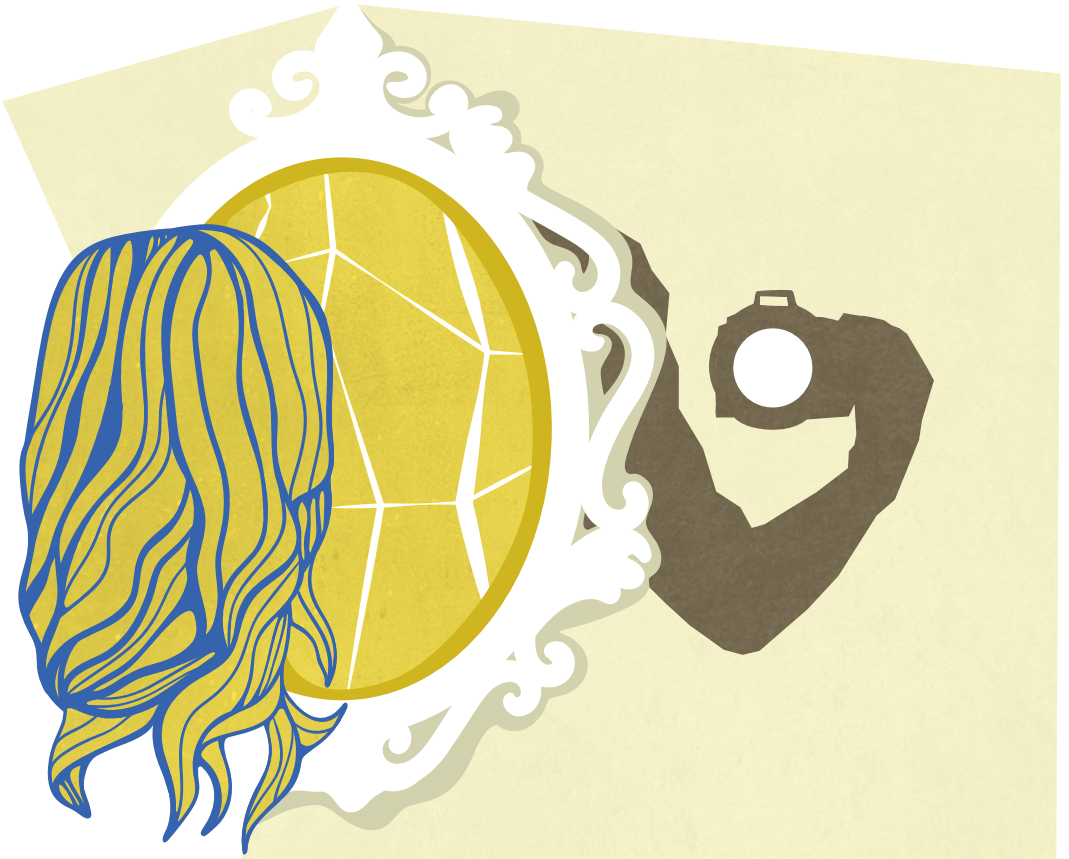
Im Laufe des Jahres 2015 wurden immer mehr Selektoren publik, deren Quelle der DE-CIX war, aber auch die BND-Station im bayerischen Bad Aibling. Ziele waren unter anderem deutsche Ministerien, französische Diplomaten, internationale Rüstungsunternehmen oder die EU-Kommission. Was das alles mit Terrorismusbekämpfung zu tun hatte, konnte niemand erklären. Vielmehr verfestigte sich der Eindruck, dass die USA mittels deutscher Hilfe ihre globale Vormachtstellung sichern wollte. Dafür betrieb sie nicht nur Wirtschaftsspionage, sondern hörte auch hochrangige Politiker ab, um sich einen Vorteil bei internationalen Verhandlungen zu verschaffen.

DAS BND-GESETZ EINE DREISTE LEGALISIERUNG ILLEGALER PRAKTIKEN ZU NENNEN, WÄRE NOCH FREUNDLICH FORMULIERT.

»DIE GESAMTE DEUTSCHE AUSLANDSAUFKLÄRUNG IST RECHTSWIDRIG«

Wenngleich manch deutsche Politiker die NSA-Affäre schon mehrmals für beendet erklärten, gab es fortlaufend neue Reaktionen, die ins Leere liefen. Zum Beispiel das No-Spy-Abkommen zwischen den USA und Deutschland, das sich am Ende als eine Fata Morgana der damaligen Bundesregierung herausstellte. Oder die Ermittlungen des Generalbundesanwalts, die dann schließlich doch kein Verfahren ergaben. Positiv hingegen war die Einrichtung des NSA-Untersuchungsausschusses im Frühjahr 2014, um »Ausmaß und Hintergründe der Ausspähungen durch ausländische Geheimdienste in Deutschland aufzuklären«, so die offizielle Zielsetzung. Gleich in der ersten öffentlichen Sitzung kamen die deutschen Verfassungsrechtler Wolfgang Hoffmann-Riem, Matthias Bäcker und Hans-Jürgen Papier jedoch zu einem vernichtenden Urteil über die eigenen Geheimdienste: »Die gesamte deutsche Auslandsaufklärung ist rechtswidrig.«

Innerhalb der folgenden drei Jahre wurden etliche Zeugen vernommen, darunter leider nicht Edward Snowden, dafür aber andere ehemalige NSA-Mitarbeiter, aktuelle



Angestellte des BND – und auch Klaus Landefeld, der im Beirat der DE-CIX Management GmbH sitzt. Laut seiner Aussage interessierte sich der BND bei der Überwachung des Internetknotenpunkts DE-CIX aber nicht nur für außerdeutsche Leitungen, wie zum Beispiel solche in den arabischen Raum, sondern auch für innerdeutsche. Jedoch ließe sich »absolut nicht trennscharf« unterscheiden, was im Netz »deutsch ist oder nicht«, so Landefeld. Dem Auslandsgeheimdienst ist es eigentlich per Grundgesetz verboten, die eigenen Staatsbürger abzuhören – eine Lehre aus der Zeit des Nationalsozialismus.

LEGAL, ILLEGAL, SCHEISSEGAL: DAS NEUE BND-GESETZ

In Anbetracht dieses Rückblicks auf die Überwachungsaffäre stellt sich nun die Frage: Welche Lehren hat die Bundesregierung gezogen? Von der Öffentlichkeit wenig beachtet legte sie im Juni 2016 schließlich das neue Gesetz zur »Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes« vor, das zum Jahreswechsel 2017 in Kraft getreten ist. Statt dem Geheimdienst Grenzen zu setzen und ihn mit klaren Regeln besser zu kontrollieren, wurde praktisch alles, was der BND macht, per Gesetz einfach legalisiert – und sogar noch ausgeweitet. So darf der BND nun auch im Inland abhören und ganz legal auf die eben beschriebenen deutschen Leitungen am Internet-Knoten DE-CIX zugreifen. Zudem durfte der BND bisher nur einzelne Leitungen abhören und auch davon eigentlich nur 20 Prozent der Kapazität. Nun fallen beide Grenzen: Der BND darf ganze Telekommunikationsnetze ohne Begrenzung anzapfen, also 100 Prozent der Leitungen und Netze der Telekom oder anderer Anbieter.

Als Anlass für die Überwachung dienten bisher Terror, Krieg oder Cyber-Angriffe. Im neuen BND-Gesetz stehen nun äußerst vage formulierte Anlässe wie »die Handlungsfähigkeit der BRD zu wahren« oder »sonstige Erkennt- ►

nisse von außen- und sicherheitspolitischer Bedeutung«. Mit solchen Gründen lässt sich nahezu jede Art von Überwachung rechtfertigen. Was die Inhalte anbelangt, so sammelte der BND bislang ohne Erlaubnis Metadaten in ganz großem Stil und gab jeden Monat mindestens 1,3 Milliarden Metadaten an die NSA weiter. Diese Weitergabe an Partner wie die NSA wird nun legalisiert, zudem dürfen die Metadaten anlasslos ein halbes Jahr gespeichert werden. Bei der Kontrolle der Geheimdienste preiste die Bundesregierung zudem ein neues, »unabhängiges« Gremium an, welches sie aber selbst ernennt. Der zu Kontrollierende bestimmt also, wer ihn kontrolliert.

VERTRAUEN IST GUT, SELBSTKONTROLLE IST BESSER

Das BND-Gesetz eine dreiste Legalisierung illegaler Praktiken zu nennen wäre noch freundlich formuliert. Andere Kritiker werden deutlicher, wobei die Beurteilungen von einem »Dokument der Ufer- und Maßlosigkeit« (Digitale Gesellschaft), über einen »Angriff auf die Informations- und Pressefreiheit« (Reporter ohne Grenzen) bis hin zu einem »absoluten Debakel« (DE-CIX-Management) und der Feststellung reichen, dass der »BND offiziell zur Massenüberwachungsmaschine wird« (Bündnis 90/Die Grünen). Markus Beckedahl von Netzpolitik.org bringt es auf den Punkt: »Die Enthüllungen Edward Snowdens wurden als Machbarkeitsstudie für den deutschen Markt gesehen, nicht als Warnung.«

Nun fragt man sich vielleicht: Wie kommt so eine offensichtliche Verletzung der Grundrechte, ja sogar ein Verfassungsbruch mit Ansage eigentlich zustande? Die Antwort lautet schlicht: weil die Bundesregierung es kann. Die Opposition ist zahlenmäßig zu klein und hatte daher nicht die Macht, das Gesetz zu verhindern oder substanzielle Änderungen durchzusetzen. Für alle Kritiker ist das BND-Gesetz ein zynischer Versuch, sie ruhig zu stellen, getreu dem Motto: Am Ende soll niemand mehr der Regierung vorwerfen können, es gebe keine Rechtsgrundlage für die Überwachung!

SCHNÜFFELGESETZ IN GROSSBRITANNIEN, BLACK BOXES IN FRANKREICH

In Deutschland hat sich also vieles zum Schlechteren entwickelt. Doch wie sieht es in anderen Ländern aus, etwa in Großbritannien, Frankreich oder den USA? Im Vereinten Königreich ist die damalige Innenministerin und jetzige Premierministerin Theresa May einen ähnlichen Weg gegangen wie die Bundesregierung. Sie hat mit dem »Investigatory Powers Bill« Ende 2016 ein Gesetz durchs Parlament gepeitscht, das die aufgedeckten Überwachungsaktivitäten des britischen Geheimdiensts Government Communications Headquarters (GCHQ) legalisiert und ausweitet. So dürfen sich die britischen Geheimdienste nun legal massenhaft in Netzwerke, Computer oder Smartphones hacken. Dabei dürfen sie Trojaner verwenden sowie Schwachstellen in Hard- und Software ausnutzen. Unternehmen können sogar gezwungen werden, bei der Entschlüsselung ihrer Dienste zu helfen oder Hintertüren einzubauen. Neben dem Zugriff auf private und öffentliche Datenbanken wie die des Nationalen Gesundheitsdienstes NHS wurde auch die Vorratsdatenspeicherung stark erweitert. Internetdienste sind nun dazu verpflichtet, die Telekommunikations-Verbindungsdaten zwölf Monate lang aufzubewahren. Daher hat sich im Volksmund bereits der Name »Snooper's Charter« (Schnüffelgesetz) eingebürgert. Bürgerrechtler wie Pam Cowburn von der Open Rights Group bezeichnen es als »eines der extremsten Überwachungsgesetze, das je in einer Demokratie verabschiedet wurde.«

»DIE ENTHÜLLUNGEN EDWARD SNOWDENS WURDEN ALS MACHBARKEITS-STUDIE FÜR DEN DEUTSCHEN MARKT GESEHEN, NICHT ALS WARNUNG.«

In Frankreich ist es vor allem die ständige Angst vor neuen Terroranschlägen, die ein neues Überwachungsgesetz vorangetrieben hat. Es verpflichtet Internetanbieter, sich aktiv am Abhören seiner Kunden zu beteiligen, indem sie sogenannte Black Boxes in ihren Rechenzentren aufstellen. Damit werden in Echtzeit alle Metadaten aufgezeichnet und nach bestimmten Algorithmen überprüft. Aufgrund dieser Raster wird dann entschieden, wer überwacht werden soll. Als Anlässe fürs Ausspähen gelten nun »wichtige außenpolitische Interessen«, »industrielle und wissenschaftliche Interessen« sowie die »Abwehr von Angriffen auf Institutionen der Republik«. Kritiker bemängeln, dass

derartig vage Vorgaben auch die Überwachung von politischen Aktivisten oder Journalisten rechtfertigen könnten. Als Kontrollorgan soll die neu eingerichtete Nationale Kommission dienen, die Geheimdiensteinsätze künftig genehmigen muss. Jedoch kann sie vom Präsidenten überstimmt werden, zudem enthält das Gesetz Ausnahmeregelungen für »Überwachung in Notfällen«, die keine Genehmigung durch die neue Kommission brauchen.

Seit dem »Patriot Act«, der nach 9/11 die Bürgerrechte im Namen des Anti-Terror-Kampfs massiv eingeschränkte, sind die USA das Mutterland der Überwachung. »Alles fing eine Woche nach den Anschlägen an, als sie damit begannen, aktiv alle Bürger dieses Landes auszuspionieren«, sagte William Binney, der als Crypto-Mathematiker über 30 Jahre für die NSA arbeitete. Zwar gab es in den vergangenen Jahren ein paar Reformen unter Barack Obama. Der »USA Freedom Act« zum Beispiel lockerte den Datenzugriff der Geheimdienste etwas. Jedoch sind die meisten Demokraten und Republikaner bis heute überzeugte Anhänger der »mehr Überwachung gleich mehr Sicherheit«-Doktrin und denken gar nicht daran, ihren Geheimdiensten stärkere Fesseln anzulegen. Wie sagte Obama doch so schön: »Wir werden uns nicht entschuldigen, nur weil unsere Dienste vielleicht effektiver sind.«

GEGEN DAS DIKTAT DER ÜBERWACHUNG

Man sei dabei, die größte Unterdrückungswaffe der Menschheit zu bauen, schrieb Edward Snowden an die Citizenfour-Regisseurin Laura Poitras, bevor er die NSA verließ. Betrachtet man nun die wachsende Macht der westlichen Geheimdienste in den Jahren nach seinen Enthüllungen, bekommt dieses Zitat einen dystopischen Klang. Während von den sicherheitsfanatischen US-Amerikanern vielleicht nichts anderes zu erwarten ist, begehen die terrorgeplagten Europäer leider die gleichen Fehler wie die USA nach 9/11: Sie werfen ihren Geheimdiensten elementare Grundrechte wie Datenschutz und Privatsphäre zum Fraß vor. Allerdings stellt sich angesichts der wachsenden Zahl an Terroranschlägen in letzter Zeit die berechtigte Frage nach der Legitimation der Geheimdienste, die doch gerade die Verhinderung solcher Attacken stets als Grund für die totale Überwachung angeben.

Mittlerweile zweifeln auch viele Tech-Unternehmen die eingeforderte bedingungslose Gefolgschaft der Dienste an und wehren sich. So hat etwa Apple, das beim PRISM-Programm noch mitbeteiligt war, die Betriebssysteme seiner Handys mit einer stärkeren Verschlüsselung ausgestattet. Zudem weigerte sich der kalifornische Konzern, vom FBI verlangte Hintertüren in sein Betriebssystem iOS einzubauen, um die iPhones von Terrorverdächtigen zu knacken. Damit verhinderte Apple einen Präzedenzfall von globalem Ausmaß. Die bahnbrechenden Snowden-Enthüllungen bewirkten einen gesellschaftlichen Wandel, der auch die Unternehmen umdenken ließ. Die öffentliche Debatte um Datenschutz und Privatsphäre rückte diese Themen ins Bewusstsein einer breiten Bevölkerungsschicht.

Es gab nicht nur zahlreiche Demonstrationen, Petitionen und offene Briefe in Deutschland, es gründeten sich auch diverse Initiativen und Organisationen, die gegen die Massenüberwachung protestieren. Zudem erhielt die Crypto-Party-Bewegung mehr Zulauf. Ihr ist es unter anderem zu verdanken, dass heute immer mehr Menschen Online-Verschlüsselungsmethoden wie TOR oder PGP benutzen. Außerdem überwinden immer mehr Nutzer ihre Bequemlichkeit und steigen auf weniger verbreitete, dafür aber sichere Messenger und E-Mail-Dienste um. Es scheint, dass die Zivilgesellschaft erkannt hat, dass sie den Kampf um ihre Freiheits- und Grundrechte selbst aufnehmen muss, da sie von der Gesetzgebung im Stich gelassen wird. »Für mich geht es letztlich um die Macht des Staates im Vergleich zu den Möglichkeiten des Volkes, sich dieser Macht zu widersetzen«, sagte Edward Snowden beim ersten Treffen mit Laura Poitras und dem Journalisten Glenn Greenwald im Juni 2013 in Hongkong. Sein Vermächtnis ist, dass dieser Widerstand nun geweckt ist. Angesichts der geheimdienstlichen Machtfülle könnte es jedoch schon zu spät sein. •

Das Thema Überwachung erinnert **Raimon Klein** an den Konsum von Fleisch. Wenn man erst einmal zu viel weiß, macht es keinen Spaß mehr. Daher setzt er nun auf eine Datenkraken-Diät und verzichtet gerne auf die Häppchen von Facebook, WhatsApp und Gmail. Dann erfahren auch weniger Leute von seiner Vorliebe für David-Hasselhoff-Emojis.

»ICH HATTE MIT DEM LEBEN ABGESCHLOSSEN«

Karsten Dümmel wurde in der DDR von der Stasi überwacht und schikaniert. Seinen Widerstand konnte der Staatsapparat aber nie brechen. Der Schriftsteller sieht sich als Gegner, nicht als Opfer der Gewalt.

TEXT KRISTINA REGENTROP
ILLUSTRATION PHILIPP HAACKE

Jede Nacht reinigt er Züge und Kaufhäuser, zwölf Stunden lang. Kontakt zur Außenwelt hat er nicht, auch nicht zur Familie oder zu Freunden. Karsten Dümmel ist ein Gefangener in seiner eigenen Stadt. Dazu gemacht hat ihn das Ministerium für Staatssicherheit (Stasi) der DDR.

Der Schriftsteller wird 1960 in Zwickau geboren. Unbeschwert wächst er in Gera auf. »Das Problem beginnt dann, wenn man ausschert«, erzählt er. Als 16-Jähriger organisiert er in Schlema eine Veranstaltung, bei der Bilder und Fotografien ausgestellt und Gedichte rezitiert werden. Er und die Mitorganisatoren werden zugeführt, kommen in Untersuchungshaft, da die Veranstaltung nicht offiziell genehmigt wurde. »Von da an bis zum Ende der DDR bin ich die Stasi nicht mehr losgeworden«, erinnert sich Dümmel. Für ihn ist es die Initialzündung seiner Stasi-Überwachung. Denn es bleibt nicht bei dieser einmaligen Zuführung, die ein taktisches Instrument der Geheimpolizei ist. Dümmel wird zum Ziel eines gigantischen Überwachungsapparats. In den 1980er Jahren arbeiten mehr als 90.000 hauptamtliche und etwa 180.000 inoffizielle Mitarbeiter für die Stasi und ermöglichen damit eine flächendeckende Überwachung, um Personen zu befragen, einzuschüchtern oder zu inhaftieren.

Mit 18 tritt Karsten Dümmel aus allen sozialistischen und kommunistischen Organisationen wie der Freien Deutsche Jugend (FDJ), der Gesellschaft für Deutsch-Sowjetische Freundschaft (DSF) und dem Freien Deutschen Gewerkschaftsbund (FDGB) aus. Nach seiner Ausbildung zum Elektromonteur besucht er ein Abendgymnasium, holt das Abitur nach und will Literaturwissenschaft in Leipzig und Berlin studieren. Acht Mal bewirbt er sich, erhält jedoch stets eine Absage. Später erfährt er aus seiner Akte, dass er aus politischen Gründen abgelehnt wurde. Dümmel ist oppositionell, leitet in den 1970 und 1980er Jahren mehrere staatsunabhängige und illegale kirchliche Arbeitskreise in Schlema und Gera, wie beispielsweise den Arbeitskreis Literatur.

In den wöchentlichen Treffen kommen Ende der 1970er Jahre 20 bis 60 Teilnehmer in Gera zusammen, die gemeinsam DDR-kritische Literatur lesen und besprechen. Christliche und jüdische Partnergemeinden aus Westdeutschland schleusen die Bücher über Ost-Berlin in die DDR, unter anderem auch die Schriften der Geschwister Scholl. Im Rahmen des NATO-Doppelbeschlusses und der Stationierung von Atomwaffen in Ost- und Westdeutschland fasst Dümmel im Jahr 1985 die Thesen aus den Flugblättern der Widerstandsgruppe Weiße Rose zusammen. Die Flugblätter werden zu tausenden Exemplaren vervielfältigt und während der Friedensdekade in Gera und Greiz von mehreren Kirchtürmen geworfen. Es war ein Akt, der gegen das Gesetz, gegen die Paragraphen 106 über »staatsfeindliche Hetze« und 107 über »staatsfeindliche Gruppenbildung«, verstieß. Glücklicherweise wird Dümmel nicht dafür belangt. ▸

DIE DUNKELSTE ZEIT SEINES LEBENS

Die Universitätsabsagen sind der Grund, warum Karsten Dümmel 1984 seinen ersten Ausreiseantrag aus der DDR stellt. Für ihn ist sie ein Ort ohne »Entfaltungsmöglichkeiten, Bewegungsfreiheit und Freiheit des Wortes«. Doch der Antrag wird abgelehnt.

Doch er lässt sich nicht entmutigen und stellt bis 1988 weitere Anträge – insgesamt 56 Stück. Nach eigenen Angaben gab es bei keinem anderen DDR-Bürger so viele Ausreiseanträge. Dem Ministerium missfallen diese oppositionelle Arbeit und seine Ausreisepläne. Ab Mai 1984 setzt die Stasi sogenannte Zersetzungsmaßnahmen ein, die die Aktivitäten von vermeintlichen Feinden des SED-Regimes lautlos unterbinden sollen. »Zersetzung bedeutet, ohne Urteil bestraft zu werden«, sagt Dümmel.

Nun bricht für ihn die dunkelste Zeit seines Lebens an. »Eine Phase, die für mich grau und schwarz war, voll von nicht endender Hoffnungslosigkeit. Man glaubt, das hört niemals auf und sieht keinen Horizont mehr. Eigentlich hatte ich damals schon mit dem Leben abgeschlossen«, erinnert sich Dümmel. Die permanente Überwachung des Ministeriums bestimmt sein Leben. Die Zersetzungsmaßnahmen sollen verhindern, dass er öffentlichkeitswirksame Aktionen durchführt. Der andersdenkende, unangepasste Dümmel wird von der Außenwelt abgeschirmt und soll zur Öffentlichkeit kaum Kontakt haben.

Zu diesem Zweck verhängt die Stasi eine Arbeitsplatzbindung und zwingt ihn, nachts zwölf Stunden lang Kaufhäuser und Züge zu reinigen. Auch Postkontrollen, Reisesperren, Stadtarrest und zeitweise Hausarrest sind Teil der Maßnahmen. Dümmel darf Gera nicht verlassen, beispielsweise um nach Berlin zu reisen. Er muss sich an fünf Tagen der Woche bei dem Sicherheitsbeauftragten seiner Firma oder bei der Polizei melden. Tut er das nicht, wird eine Fahndung nach ihm ausgelöst. An allen staatlichen Feiertagen wie dem 7. Oktober, dem Nationalfeiertag der DDR, oder wenn politische Delegationen in der Stadt weilen, steht Dümmel für mehrere Tage unter Hausarrest: »Ich durfte das Haus nicht verlassen, um mich öffentlich zu äußern«, erinnert er sich.

Durch Isolationsmethoden versucht ihn das Ministerium für Staatssicherheit psychisch zu schwächen. Familie, Freunde und Bekannte werden von der Stasi bewusst unter Druck gesetzt, um den Kontakt zu ihm abzubrechen. Die Stasi verspricht ihnen Vorteile wie Karrieremöglichkeiten oder Studienplatzzusagen und schüchtert sie ein. »Und dann wundert man sich, wenn man beim besten Freund am Geburtstag vor der Tür steht. Man hört Musik, die beim Klingeln ausgestellt wird. Niemand öffnet die Tür, weil man zuvor unterschrieben hat, mich nicht mehr zu sehen.«

Aber dabei bleibt es nicht: Ihm werden alle bürgerlichen Rechte entzogen und sogar sein Personalausweis abgenommen. Stattdessen erhält er einen vorläufigen Ausweis, den sogenannten PM 12. »Mit der Zeit wird man immer ohnmächtiger, die Auswirkungen spürt man erst nach und nach. Die Angst nimmt zu«, sagt er. Mehrfach wird er der Untersuchungshaft zugeführt. Jedes Mal fragt er sich, ob er wieder rauskommt. »Die wissen scheinbar alles«, denkt er bei den unzähligen Vernehmungen. Daher wird er vorsichtig und versucht selbst, Menschen gezielt zu überprüfen. Er streut Informationen, um mögliche Spitzel zu entlarven und festzustellen, wem er noch vertrauen kann. Es geht sogar so weit, dass er sich komplett von seiner Außenwelt abkoppelt und mit niemandem mehr redet. Stattdessen schreibt er zahllose Briefe an seine Freunde im Ausland. »Meine Briefe wurden über Kuriere aus dem Osten geschmuggelt.«

DER LANGE ARM DER STASI

Karsten Dümmel will sich nicht einschränken lassen und bietet ab Herbst 1985 dem sozialistischen Staat die Stirn. »Wenn es die Freiheit im eigenen Land nicht gibt, muss

man so tun, als ob es sie gäbe«, sagt er. Er widersetzt sich mehrfach dem Stadtarrest, versteckt sich im Kofferraum und verlässt heimlich die Stadt. »Um die Stasi abzuwimmeln und nach Zwickau oder Leipzig zu gelangen, fuhr ich mit meinem Rennrad auf schmalen Wald- und Wiesenwegen, auf denen mich Autos nicht verfolgen konnten.«

Dümmel spielt auch mit dem Gedanken, aus der DDR zu fliehen und plant mehrfach seine Flucht in den Westen. Beim ersten Mal muss er aus gesundheitlichen Gründen seinen Versuch abbrechen. Kurz vor seinem zweiten Anlauf erfährt er über seine Westkontakte, dass er möglicherweise bald freigekauft wird. Daher geht er das Risiko nicht ein, bei der Flucht über die innerdeutsche Grenze sein Leben zu verlieren.

Im Frühjahr 1988 wird er vom Bundesministerium für innerdeutsche Beziehungen über Rechtsanwälte dann tatsächlich freigekauft. Doch auch im Westen ist der lange Arm der Stasi spürbar und die Überwachung geht weiter. In Prag möchte er sich mit Freunden aus der Initiative Frieden und Menschenrechte treffen. Die Verabredung wird verhindert, Dümmel wird als »unerwünschte Person« für 48 Stunden an der Grenze festgehalten und in den Westen zurückgeschickt.

1988 studiert Dümmel an der Universität in Tübingen Rhetorik und Germanistik – ein lang ersehnter Traum wird wahr. Ein Jahr später fällt die Mauer; Ende 1992 nimmt er das erste Mal Einsicht in seine Stasi-Akte. »Man weiß als normaler Mensch gar nicht, wie so eine Akte aufgebaut ist und ist völlig erstaunt, was man da vorfindet. Aus meinen Akten weiß ich, dass ich auch nach dem Mauerfall noch bis Dezember 1989 von der Stasi überwacht wurde.«

Die Akteneinsicht offenbart, wie die Überwachung stattgefunden hat und bringt Erschreckendes zum Vorschein. So erfährt er unter anderem, dass die Stasi damals eine Akte zu seiner fünfjährigen Tochter angelegt hat, »weil sie im ständigen Kontakt mit einer feindlichen, negativen Person steht – ihrem Vater. Der Staatssicherheitsdienst verhing eine Postsperre und verbot Besuch aus dem Westen«, berichtet Dümmel. Bislang hat er drei Mal Einsicht in seine Akte genommen. »Ein weiteres Mal werde ich das nicht tun, weil die Stasi mir bei jeder Einsicht kostbare Lebenszeit stiehlt.« Insgesamt wurden seit 1992 mehr als 7,1 Millionen Anträge auf Akteneinsicht gestellt.

Auch nach dem Ende der DDR spürt Karsten Dümmel ein gewisses Misstrauen gegenüber seinen Mitmenschen. »Ich habe lange gebraucht, um dies abzubauen. So ganz wird es aber nie verschwinden«, sagt er. Seine Heimat hat der Schriftsteller inzwischen im Ausland gefunden, in Bosnien und Herzegowina leitet er derzeit das Auslandsbüro der Konrad-Adenauer-Stiftung und lehrt als Gastprofessor an den Universitäten in Mostar, Sarajevo und Pale. Nur ungern möchte er in Deutschland, erst recht nicht in einem der neuen Bundesländer, leben. Die Erlebnisse in der DDR werden ihn nie loslassen. Dennoch stellt er klar: »Ich bin ein Gegner – kein Opfer der Stasi.« •

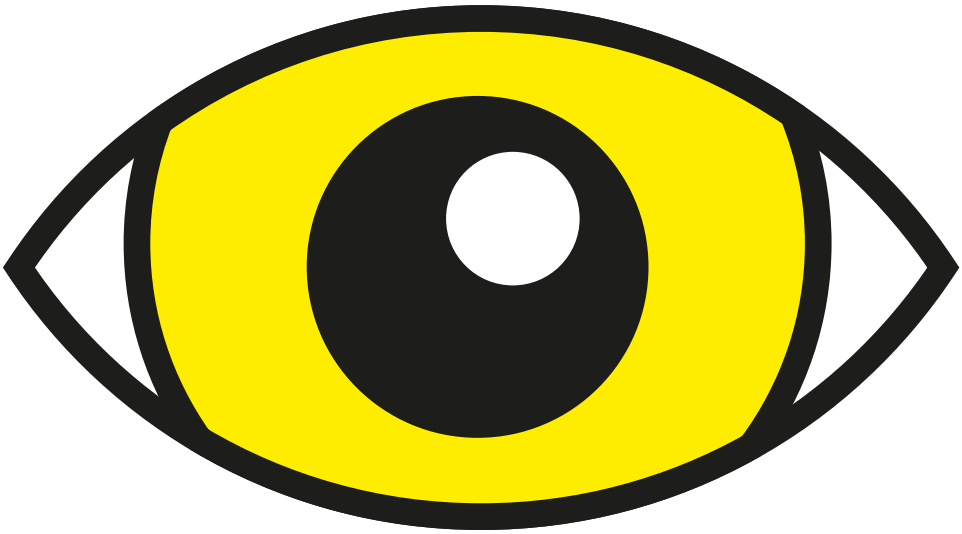
Kristina Regentrop, born and raised in Nordrhein-Westfahlen, studiert im Master Journalistik und Kommunikationswissenschaft in Hamburg. Im Rahmen eines Uni-Seminars ist sie auf Kater Demos gestoßen und freut sich, bei dieser Ausgabe mitgewirkt zu haben – trotz schlimmer Katzenhaarallergie.

WAS WURDE AUS?

FURBY

Viele Eltern erinnern sich wahrscheinlich noch mit Schrecken an diese haarigen, schnatternden Dinger, die 1998 Kinderzimmer eroberten. Furbys – irgendwas zwischen Katze, Fledermaus und Eule – sprachen anfangs nur »Furbisch« und konnten, wenn man sich mit ihnen beschäftigte, knapp 800 Wörter in der jeweiligen Sprache lernen (zum Vergleich: Eine Fünfzehnjährige benutzt etwa 12.000 Wörter). 2012 gab es eine Neuauflage der singenden und mit den Ohren wackelnden Viecher; diesmal mit digitalen Augen und dazu passender App.

Ins Visier der Sicherheitsbehörden geriet der Furby 1999 durch die National Security Agency (NSA), die eine illegale Überwachung und somit das Abschöpfen von sicherheitsrelevanten Informationen fürchtete. Die Spione wurden beschrieben als »...being less than a foot high, covered with red and orange fur, with watchful eyes and big ears«. Grund dafür war und ist noch heute der eingebaute Datenchip. Seitdem sind die kleinen Monster in allen Gebäuden der NSA streng verboten.



WAS WURDE AUS?

JOHN MILZ

DEM GEWINNER DER ERSTEN BIG BROTHER-STAFFEL

Ebenfalls 1999 wurde erstmals in den Niederlanden das Sendeformat Big Brother ausgestrahlt. Die nach dem allgegenwärtigen Überwacher aus George Orwells »1984« benannte TV-Show sollte Millionen von Zuschauern (in über 70 Ländern) selbst zum »großen Bruder« werden lassen. So konnte man, teilweise live, verfolgen, wie eine Gruppe von Menschen in ein Fernsehstudio (»Container«) eingesperrt und mehrere Wochen 24 Stunden lang durch Kameras und Mikrophone überwacht wurden.

Die damals viel kritisierte Show kam im Jahr 2000 nach Deutschland. Während sich viele heute, wenn überhaupt, eher an »Zlatko & Jürgen« erinnern, war der Sieger der ersten Staffel der damals 26-jährige John Milz; kurze Haare, dicke Augenbrauen und arbeitsloser Hausbesitzer aus Potsdam. Nach seinem Gewinn von 250.000 D-Mark hat er sich der ständigen Überwachung durch das Fernsehen allerdings entzogen. Man munkelt, er lebt heute auf einem Bauernhof nahe Krefeld. Berühmt war die Sendung übrigens auch für ihre prominenten Besucher: Besonders in Erinnerung bleibt die Stippvisite vom damaligen FDP-Chef Guido Westerwelle in der zweiten Staffel.

DER TÜRSPION

Der kanadische Filmemacher Derek Howard hat zwei Jahre lang seinen Nachbarn überwacht. Durch den Türspion seiner Wohnung filmte er all dessen Aktivitäten. Daraus entstanden ist der 30-minütige Dokumentarfilm »Doctor Korbes«. Man wird darin Zeuge bizarrer Szenen, die sich vor und in der Wohnung von Dereks Nachbarn Doktor Korbes abspielen.

TEXT ARNE SIEGMUND
FOTOS JOHANNES BERGER

Irgendjemand war in Dereks Wohnung. »Ich hatte vergessen, die Balkontür zuzumachen. Ich wusste sofort, dass er es war«, sagt er. Er, das war sein Nachbar Doktor Korbes von gegenüber, mit dem er sich vor einigen Jahren den Balkon geteilt hat. »Auf dem Fußboden im Wohnzimmer hatte er eine merkwürdige Skulptur hinterlassen: Ein Turm englischsprachiger Bücher, rundherum Zigaretten und, ganz oben, auf dem obersten Buch lag eine Euromünze.«

Derek Howard ist Regisseur und Filmemacher. Während er erzählt, sitzt er auf einem Kinderstuhl, der eigentlich viel zu klein für ihn ist. Der Stuhl gehört zum Mobiliar eines Cafés auf der Sonnenallee. Derek ist 32 Jahre alt und einen Meter 90 groß, er kommt aus Vancouver. Seine Großeltern stammen aus Koblenz. Seit 2008 lebt er in Berlin. Er trägt sein dunkelblaues Flanellhemd bis oben hin zugeknöpft und wärmt sich mit einem Chai Latte auf.

Draußen ist es kalt und nass. Über Nacht hat es geschneit. Auf der Sonnenallee ist Trubel, Lieferwagen parken mit Warnblinkanlage in zweiter Reihe vor arabischen Gemüsehändlern. Nicht weit von hier haben auch Derek und sein Nachbar Doktor Korbes gewohnt, vis-à-vis auf derselben Etage.

NÄCHTLICHER LÄRM UND KOMISCHE GERÄUSCHE

Doktor Korbes war im ganzen Haus berühmt-berüchtigt: »Nächtlicher Lärm, Kämpfe, komische Geräusche, Besuch von Prostituierten und seltsamen Leuten.« Nicht nur Derek, auch die anderen Mieter fühlten sich belästigt vom schrulligen Doktor. Nachdem dieser dann auch noch in Dereks Wohnung eingebrochen war und eine Buchskulptur hinterließ (»That freaked me out, of course!«), hatte Derek genug und erzählte seiner Vermieterin von dem Vorfall.

Es sollte der Startschuss für ein einzigartiges voyeuristisches Filmprojekt sein. »Filmen Sie ihn! Nehmen Sie mal alles auf, was der so den ganzen Tag da treibt«, so der ►

eindeutige Vorschlag der Vermieterin. »Die wollte Beweise haben, um Doktor Korbes aus der Wohnung kündigen zu können. Und das habe ich dann gemacht, ich habe ihn gefilmt«, sagt Derek und fügt mit einem Schmunzeln hinzu: »Eigentlich bin ich nicht der Typ, der seine Nachbarn ausspioniert.«

Zwei Jahre lang überwachte Derek daraufhin Doktor Korbes mit einem Camcorder durch seinen Türspion. »Erst hatte ich ein schlechtes Gewissen. Klar, das ist ein Eingriff in die Privatsphäre eines anderen Menschen. Aber ich habe mich nicht so schuldig gefühlt. Er ist ein schlechter Mensch gewesen, der ständig die Hausbewohner belästigte und mit Kriminellen zu tun hatte. Jeder wusste, dass er ein Problem war. Und es ist ja erlaubt, aus seiner Wohnung heraus zu filmen, außerdem hat er seine Tür immer stundenlang aufstehen gehabt, als ob es ihm egal war, dass man hineinsehen konnte. Es war wie eine Einladung.«

»DER KREATIVE PROZESS HAT MICH BESESSEN GEMACHT!«

Zuerst hat Derek nur ab und zu gefilmt. Immer mal wieder, hier und da fünf Minuten. »Es hat sehr beiläufig angefangen. Doch irgendwann hat mich das Projekt, der ganze kreative Prozess, besessen gemacht. Das haben Filmemacher, glaube ich, so an sich. Vor allem Dokumentarfilmer sind doch immer auch Voyeure«, erklärt Derek. »Ich hatte am Ende etwa 20 Stunden Material.« So genau weiß er es gar nicht mehr. Das Ergebnis ist der Dokumentarfilm »Doctor Korbes«, komplett durch den Türspion von Dereks Wohnung gefilmt.

»Die Geschichte hat sich von selbst erzählt. Es ist kein narrativer Film, ich habe keine Story entwickelt. Ich kannte die Schlüsselszenen, im Grunde ist alles chronologisch wiedergegeben. Mittlerweile denke ich sogar, dass es gar kein Film über Doktor Korbes ist, sondern ein Film über eine Tür. Denn das ist das, was ich am meisten gefilmt habe: Die Tür, die sich durch seine Interaktionen verändert, die auf, zu und kaputtgeht, wiederaufgebaut wird.« Der Film ist eine obsessive Dokumentation über Bizarres und Absurdes vor und in Doktor Korbes' Wohnung. 30 Minuten lang kann man in »Doctor Korbes« Szenen wie folgende miterleben und ein Stück weit an seinem Leben teilhaben:

»I love you! I want to fuck you, baby!«, ruft Doktor Korbes zwei Frauen, offensichtlich Prostituierte, zu. Er bezahlt sie auf der Schwelle seiner Wohnungstür. Die beiden Frauen gehen. »Ciao! Ciao!«

Wie fühlt sich das an, wenn man jemanden zwei Jahre lang filmt und beobachtet? »Es ist schon merkwürdig mit der Zeit, wenn du jemanden über längere Zeit dauernd observierst – eine Art abstrakte Studie.« 90 Prozent der Aufnahmen seien nachts entstanden, wenn Doktor Korbes mal wieder Stress mit irgendwem hatte. »Es war immer total aufregend, diese Keilereien mitzubekommen, während man sich durch die eigene Wohnungstür und die Kamera geschützt gefühlt hat. Im gleichen Moment dachte ich

aber auch: Ist das moralisch vertretbar, was du da gerade tust? Würde Doktor Korbes Verständnis dafür haben oder nicht?«

Ein Junge klopft an Doktor Korbes' Tür. »Sie sind doch Doktor, oder? Können Sie mir ein Attest für die Schule unterschreiben?« - »Ich unterschreibe doch keine falschen Atteste! Lügner! Betrüger! Scheißer!«, schreit Doktor Korbes. Der Junge rennt weg.

ZWEI VOM GLEICHEN SCHLAG

Derek und Doktor Korbes seien im Laufe der zwei Jahre sogar »auf eine Art Freunde geworden. Zum Ende meines Filmprojekts sind wir ab und an essen gegangen, haben stundenlang über Berlin geredet, über Neukölln, die Mauer. Er hat mir im Prinzip seine komplette Lebensgeschichte erzählt, dass er Ende 50 ist und als Arzt gearbeitet hat. Dass die englischen Bücher in meinem Wohnzimmer ein Geschenk für mich waren. Dass er jetzt von Hartz IV lebt, Sperrmüll von der Straße sammelt und in seiner Wohnung Skulpturen baut, die aber noch nie jemand zu Gesicht bekommen hat«, erzählt Derek und denkt kurz nach: »Eigentlich waren wir zwei Leute vom gleichen Schlag, die, getrennt von zwei Wohnungstüren, ihre kreativen Prozesse ausgelebt haben.«

Die Wohnungstür öffnet sich. Doktor Korbes trägt einen Rollkragenpullover und eine Kapitänsmütze, um den Hals hat er ein Amulett hängen. Er geht auf Dereks Tür zu, bückt sich und legt etwas auf den Boden, man erkennt nicht, was es ist. Dann geht er bedächtig zurück in seine Wohnung. Die Tür schließt sich.

Doktor Korbes wusste natürlich nichts von der Kamera, aber irgendwann kam er doch dahinter. Kein Wunder: Derek erzählte ihm nämlich beim Essen, dass er ein Filmprojekt über das Haus und seine Bewohner mache. »Ich habe versucht, ihn ein Stück weit wissen zu lassen, was ich mache. Ich weiß aber auch nicht genau, wie viel und was er wusste. Dazu waren sein Englisch und mein Deutsch zu schlecht – in gewisser Weise eine Grauzone«, erklärt Derek. »Es wurde zu einer Art Spiel. Er hat dann Zettel auf meiner Türschwelle mit kleinen Nachrichten hinterlassen. Auf meiner Wohnungstür stand eines Tages auch: ›Ich weiß, dass du mich beobachtest! Aber es ist mir egal!‹«

NACH ZWEI JAHREN WAR SCHLUSS

Je mehr Derek Doktor Korbes dann kennengelernt hatte, je länger das Filmprojekt dauerte, desto schlechter wurde Dereks Gewissen gegenüber ihm: »Ich habe mehr und mehr Sympathie für ihn entwickelt. Er tat mir leid. Denn er war ein paranoider, traumatisierter Mann, der mentale Probleme hatte – deswegen habe ich dann nach zwei Jahren auch aufgehört, ihn zu filmen.«

Doktor Korbes räumt nachts in seiner Wohnung herum, die Tür steht offen. Er trägt taschenweise Krempel hin und her. Irgendwo im Haus läuft laute Technomusik. »Ruhe!«, schreit er. »Go to sleep, man!«, antwortet eine Männerstimme. Doktor Korbes schreit in falschem Englisch zurück: »You destroy our privacy! You must now be silent! It is night! We'll get the police! You are against the law, understand? Criminal! Illegal!«

Derek ist sich sicher, dass der Film auch eine kritische Sicht auf Überwachung transportiert: »Man bekommt ein Gefühl dafür, wie es ist, jemanden auszuspionieren und wie es sein muss, beobachtet zu werden«, findet Derek. »Das Ergebnis ist positiv, es wirft ein gutes Licht auf dieses Thema. Du kommst, glaube ich, nicht näher ran, als mit einem Film, der zeigt, wie es ist, derjenige zu sein, der jemanden ausspioniert.«

DIE VERMIETERIN HAT DEN FILM NIE GESEHEN

Mittlerweile leben Derek und Doktor Korbes beide nicht mehr in dem Haus. Die Wohnung von Doktor Korbes steht leer, sei total zugemüllt. Und was ist aus ihm geworden? »Er wohnt nur zwei oder drei Blocks entfernt vom alten Haus. Ich sehe ihn einmal im Jahr auf dem Weihnachtsmarkt. Ich frage mich, ob er je den Film gesehen hat«, sagt Derek und lacht. Die Vermieterin hat den Film übrigens nie gesehen. »Ironischerweise hat sie nie danach gefragt. Und sie hat ja anscheinend einen anderen Weg gefunden, Doktor Korbes aus der Wohnung zu schmeißen.«

Der Film endet mit der Szene, dass Doktor Korbes' Wohnung geräumt wird. »Ich habe selbst schon gar nicht mehr in dem Haus gewohnt. Ein Freund von mir lebte aber in meiner alten Wohnung. Der hat mich nur angerufen und geschrien: ›Seine Wohnung wird geräumt! Du musst kommen! Jetzt!‹« Derek sei so schnell Fahrrad gefahren wie noch nie zuvor in seinem Leben, quer durch Berlin, um Zeuge zu werden. »Ich bin dann schnell das Treppenhaus hoch gerannt und habe alles aufgenommen.«

Männer tragen Möbel aus der Wohnung. Minutenlang. Dann sieht man Doktor Korbes über den Flur schleichen. Er geht als Letzter, knipst das Licht aus und schließt seine Tür ab. Zum letzten Mal. •

Arne Siegmund hat in Bielefeld (Heimat) und Berlin (Wahlheimat) Journalismus studiert. Er arbeitet als freier Journalist und Autor für verschiedene Medien. Auch Arne beobachtet und lauscht gerne. Beim Bus- und Bahnfahren dreht er gerne mal seine Musik leise, lässt dann aber die Kopfhörer im Ohr und hört die Gespräche der anderen Fahrgäste mit – besser als Fernsehen!

LINKS ZUM THEMA

Ein siebenminütiger Auszug von »Doctor Korbes«: https://vimeo.com/111195888

Webseite Derek Howard: http://derekhoward.ca/

DAS MITTELALTERLICHE DORF

VON JONAS IBEL

Ritterturniere und Könige in ihren prachtvollen Burgen – das ist oft das erste, was uns zu »Mittelalter« einfällt. Doch ist das schon alles? Damalige Chronisten hinterließen meist nur Schriften, die sich auf die Oberschichten der Gesellschaft konzentrierten. Aber die Mehrheit der Menschen führte ein Leben in Unfreiheit und Abhängigkeit, oft unter – nach heutigem Verständnis – elenden Bedingungen.

Einer dieser Menschen ist Jacob, geboren im Jahr 1000. Er wächst in einer ärmlichen Bauernfamilie auf und muss schon in jungen Jahren die Felder mitbestellen. Die hat der Lehnsherr, ein Fürst, Jacobs Vater zur Verfügung gestellt. Jacob ist eines von fünf Geschwistern, das sechste ist auch schon auf dem Weg. Er und seine Familie leben von der Hand in den Mund; und alles, was sie brauchen, produzieren sie selbst. Auch Werkzeuge und Alltagsgegenstände werden nicht gekauft, sondern in Eigenproduktion hergestellt. Viel mehr bleibt der Familie nicht, da Fürst und Kirche Abgaben fordern. Der Alltag ist komplett von Arbeit bestimmt, nur kirchliche Feiertage bieten Abwechslung. Die Wohnverhältnisse sind beengt: Familie und Vieh leben unter einem Dach, die Kinder schlafen nebeneinander in einem Verschlag, Butze oder Alkoven genannt. Die Eltern haben ihr Bett nahe dem Herd, wo es immer warm ist. Das Dorf mit sieben weiteren Bauernhöfen ist gemeinschaftlich organisiert – dies bietet Jacob Sicherheit, hält ihn aber auch in seiner gesellschaftlichen Position fest.

Eine private Sphäre, wie wir sie heute verstehen, gab es zu dieser Zeit nicht, da kaum Rückzugsorte existierten und es unerwünscht war, sich seiner gesellschaftlichen Rolle zu entziehen. Zeit für sich fand man selten, beispielsweise beim Schweinehüten im Wald. Doch die Freizeit, wie wir sie seit dem 19. Jahrhundert kennen, war rar – zu viel Zeit benötigten die Menschen, um ihren Alltag zu organisieren, Haus und Hof zu versorgen. Das Wort »Freizeit« gab es noch gar nicht. Eine individuelle Persönlichkeit, die Raum zur Entfaltung braucht, konnte sich nicht entwickeln, und die Idee gab es damals noch nicht wirklich. Trotzdem hatten die Menschen ein Verständnis davon, dass Gegenstände, Land und Vieh ihr Eigen – also Privatbesitz – waren. Etwas war privat, wenn es nicht der öffentlichen Macht wie Fürst oder Kirche unterstellt war.

NICHTS WIE WEG

Wer aus dem schicksalhaften Leben als Pachtbauer ausbrechen wollte, musste in die Stadt fliehen. Der Stand, in den man hineingeboren wurde, blieb ansonsten ein Leben lang Bestimmung und wurde als naturgegeben angesehen. Wie sehr die Menschen aber damals schon ihr Glück suchten, beweist die explodierende Zahl der Städte. Um das Jahr 1000 gab es gerade einmal 40, um 1400 schon 3000 Städte auf dem Gebiet des heutigen Deutschlands.

Um seinem Schicksal als Bauernknecht zu entkommen, flieht auch Rudger, geboren 1340, nach Köln. Er weiß, dass ihm als drittem Sohn kein Erbe zusteht und entscheidet sich deswegen zur Landflucht. Wie viele andere Jungen aus seinem Dorf, die dem Leitsatz »Stadtluft macht frei« gefolgt sind, möchte er ein Handwerk erlernen. Um freier Bürger zu werden und sich aus dem Herrschaftsverhältnis mit seinem Fürsten zu lösen, muss er ein Jahr und einen Tag unentdeckt in einer Stadt leben. Er nutzt die Anonymität der Stadt und taucht unter. Er hat Glück und sein Lehnsherr verzichtet darauf, ihn zu holen. Nun beginnt er seine Ausbildung zum Schmied, die ihm einen sozialen Aufstieg – in Maßen – ermöglicht. Zwar bleiben Rudgers Wohnverhältnisse beengt, aber er fühlt sich befreit. Er wohnt über der Schmiede; hinter dem Haus gibt es ein bisschen Land für Gemüseanbau und ein paar Hühner.

Die Stadt ist eng, viele Menschen leben aufeinander gedrängt. Nur vor den Stadtmauern kann Rudger wieder Luft holen. Manchmal, wenn ihm die Stadt zuviel wird, wandert er zu Jurgen hinaus, einem Fischer. Der wohnt in einer kleinen Kate am Fluss vor den Mauern und Rudger mag die Ruhe auf dem Weg. Wäre er reich, so wie der Zunftmeister, würde er sich einen großen Garten leisten und ihn mit Mauern regelrecht abschirmen, um sich vor neugierigen Blicken zu schützen. Im Gegensatz zu seinem Leben auf dem Land kann Rudger seinen Alltag stärker selbst regeln; aber noch immer bestimmen Zunftordnung, Ständebuch und die Kirche, wie er sich anzuziehen und zu verhalten hat. Anders als seine Eltern kann Rudger aber seine Braut selbst aussuchen und frei über sein Eigentum verfügen.

DIE KIRCHE UND DER BUCHDRUCK

Im Jahr 1454 erobern die Osmanen Konstantinopel mit Kanonen und Handgeschützen – für viele Historiker das Ende des Mittelalters. Viele byzantinische Gelehrte fliehen nach Westeuropa und tragen das humanistische Bild der Menschenwürde aus den antiken Schriften mit sich. Die Renaissance steht in voller Blüte. Martin Luther verkündet seine reformatorischen Thesen, der Buchdruck verbreitet sie mit nie gekannter Geschwindigkeit. Lesen und schreiben konnten aber noch immer die wenigsten.

Bruder Benedictus, Jahrgang 1490, lebt als Mönch in einem katholischen Kloster. Jeder seiner Tage besteht aus acht Stunden Arbeit, acht Stunden Gebet mit seinen Mönchsbrüdern sowie einer Stunde Freizeit, die Benedictus dem Alleinsein widmet. Er hat Geschmack an den ruhigen Momenten des Lebens gefunden und nutzt diese zum Nachdenken. Die meiste Zeit verbringt er damit, Bücher abzuschreiben oder im Klostergarten bei der Feldarbeit. Mit Misstrauen begegnet Benedictus dem neu aufkommenden Buchdruck. Er befürchtet, dass sich die Menschen von der Kirche abwenden und Luther folgen könnten. Für Benedictus ist es wichtig, dass die Menschen an den Gottesdiensten teilnehmen und genau zuhören, was der Priester ihnen zu sagen hat. Denn nur er kann die sündigen Menschen vom Pfad des Teufels abhalten. Wenn nun Häretiker wie Luther die Bibel aus dem Kirchenlatein in die Gemeinsprache übersetzen, sind falscher Auslegung und damit der Ketzerei keine Grenzen mehr gesetzt! Diesen Gedanken hängt Benedict nach, wenn er alleine in seiner Schlafzelle liegt – eine der Annehmlichkeiten seines Klosters.

AB 1000 N.CHR.
Hochzeit des Lehenswesens und damit der Leibeigenschaft in Europa

1215
Der englische König unterzeichnet die ›Magna Charta Libertatum‹ und gesteht Adeligen rechte zu – wie die Verurteilung durch Standesgenossen

UM 1450
Erfindung des Buchdrucks

1453
Eroberung Konstantinopels durch die Osmanen

1492
Kolumbus entdeckt Amerika

1500
Humanismus verbreitet sich in Europa

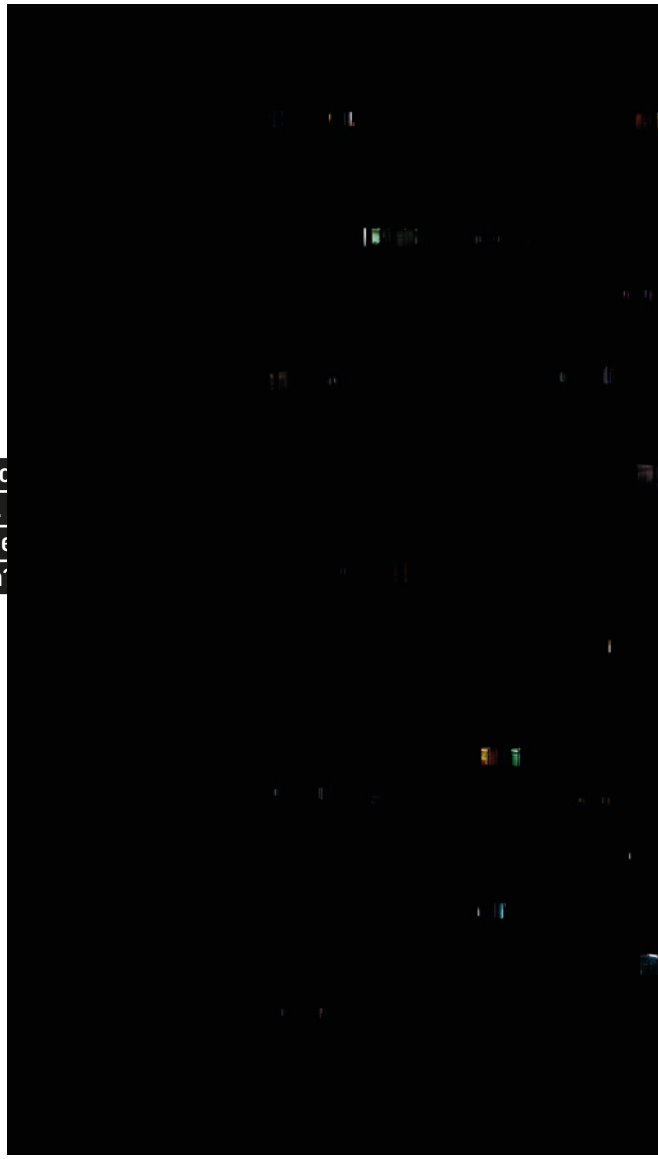
1517
Luthers 95 Thesen

DER ROTE FADEN

DER PFAD ZU EINER PRIVATHEIT

Die Menschen des Mittelalters definierten sich selten als individuelle Personen, die einen speziellen Raum zur Entfaltung – eine Privatsphäre – brauchten. Doch die gesellschaftliche Organisation verschob sich langsam von einem gemeinschaftlichen Prinzip hin zu mehr Individualismus. Als mehr Menschen lesen und schreiben lernten, eröffnete ihnen das Möglichkeiten, sich selbst ein Urteil zu bilden, Meinungen zu entwickeln und über die Welt und ihre Rolle darin nachzudenken. Auch das Gebet in Eigenregie, wie es durch den evangelisch-reformatorischen Glauben gefördert wurde, verschob den Fokus von der kirchlichen Autorität auf die individuelle Interpretation. Das humanistische Weltbild um 1500, mit Vertretern wie Erasmus von Rotterdam, rückte vom Konzept der Leibeigenschaft ab und förderte so den Gedanken der Selbstbestimmung. Tagebücher und Briefe auch von Nicht-Adeligen kamen in Mode und erweiterten die private Sphäre. Schutzmechanismen wie unsichtbare Tinte und Wachssiegel wurden genutzt, um geschriebene Geheimnisse zu bewahren. Auch in der Architektur findet sich diese Entwicklung wieder. Mehr und mehr wurden Räume als Rückzugsorte für Einzelpersonen eingerichtet, es entwickelten sich Schlafzimmer, dann Lese- und Musikzimmer oder Salons. •

IM DUNKELN IST GUT MUN



Das Darknet – unendliche Weiten: Es klingt mysteriös und gefährlic verboten und nach etwas, an das sich nur Profis rantrauen sollten. Neuland an, dabei ist es wie mit vielem im Leben: Die Realität ist vie Doch was ist das Darknet genau? Und wie kann es genutzt werden unerwünschter Überwachung entgehen? Ein Erklärungsversuch.

TEXT ELISA BILKO
FOTO FELIX HUFFELMANN

Für die meisten von uns gehört das Internet selbstverständlich zum Alltag dazu, ob am Rechner zu Hause oder unterwegs auf unserem Smart Device. Wir schauen Videos, bestellen Klamotten, chatten mit Freunden, lesen Nachrichten, bilden uns weiter oder verplempern einfach unsere Zeit. Kaum vorstellbar, kein Internet zu haben. Dabei ist unser heutiges Internet ein Hort des Konsums. Entweder kaufen wir oder sind selbst die Ware, nämlich der potentielle Kunde. Algorithmen sammeln Unmengen von Daten über uns und können mit diesen ein ziemlich genaues Bild von uns zeichnen.

Dabei ist unser Internet älter als wir glauben – obwohl wir uns ein Leben davor wahrscheinlich nicht mehr vorstellen können. Eine der frühsten Ideen dazu findet sich in dem Science Fiction Roman »A Logic Named Joe«. Der Autor Murray Leinster erzählt in seiner Shortstory aus dem Jahr 1946 von einem Personal Computer, dort Logic genannt, und beschreibt eine frühe Vision des Internets. Im Laufe der 1960er Jahre wurde aus Fiktion Realität. Das amerikanische Militär trieb die Entwicklungen voran, da es nach einem Weg suchte, im Falle eines atomaren Totalausfalls auf ein Netzwerk zurückgreifen zu können, das diesen übersteht.

Die Idee ist dabei ganz einfach: Man zerlegt Kommunikation in kleine Datenpakete, die autonom, nur mit einer Absender- und Zieladresse versehen, ihren Weg durch ein Netzwerk aus verschiedenen Knoten finden. Sie reisen dezentral, verteilen sich und sind somit weniger angreifbar. Fällt ein Knoten aus, wird einfach ein anderer Weg gewählt. In den siebziger Jahren verlagerte sich die ursprüngliche militärische Einrichtung hin zu akademischer Forschung. Freier Informationsfluss und Communitys, die auf Graswurzelbewegungen fußten, wuchsen empor. Es ging vor allem um Kommunikation von Forschern über Grenzen und Ozeane hinweg. Das Internet war schon sehr früh ein verbindendes Medium der westlichen Welt. In den neunziger Jahren erkannte dann der freie Markt und auch der Otto-Normalverbraucher das Potenzial des Netzes. Eine schöne neue Welt hatte sich aufgetan – sie schien frei und ohne Grenzen.

EIN ZWEITES INTERNET?

Doch was hat das alles mit dem Darknet zu tun? Ziemlich viel. Denn das Darknet, zumindest jenes, das die meisten meinen, wenn sie davon sprechen, ist kein unabhängiges

Internet, das auf einer eigenen Technologie basiert. Viel mehr gehört es als kleiner Teil des Internets zum großen Ganzen. Dabei kann man sich das große Ganze wie das Straßenverkehrsnetz vorstellen. Das »normale« Internet, auch Clearnet oder Surface Web genannt, das man durch Suchmaschinen wie Google erforschen kann, funktioniert wie eine Autobahn. Die Schilder sind klar zu sehen und das Navi kennt die Strecke. Man kommt also schnell von A nach B. Das Vehikel unserer Wahl sind dabei Browser wie Chrome oder Firefox: schnelle, höchstmoderne Sportwagen, die mit allem Komfort ausgestattet sind. Gleichzeitig gibt es da noch die vielen nicht gelisteten Landstraßen: Diese entsprechen dem Deep Web. Sie sind zwar theoretisch für jeden mit Sportwagen zugänglich, hier muss man sich aber auskennen und genau wissen, wo man hinwill. Ein Navi wie Google gibt es nicht. Bestimmte Inhalte des Deep Web sind nur mit Passwort oder über ein virtuelles privates Netzwerk (VPN) zugänglich. Sprich: Manche der Landstraßen sind privat und funktionieren wie eine Gated Community. Hierzu gehören zum Beispiel auch Dein digitaler Kontozugang oder Deine Lieblingsunidatenbanken.

Und dann gibt es eben noch das Darknet. Das sind holprige Schotter- und Waldwege. Um sie zu befahren, reicht der Citycruiser nicht, hier braucht man einen Geländewagen. Diese schwer befahrbaren Wege können im Prinzip von jedem genutzt werden. Ein Navi gibt es nicht, nur löchrige Straßenpläne. Über die verschlungenen Wege kommt man zwar ähnlich wie mit der Autobahn ebenfalls von A nach B, aber eben viel langsamer. Dafür gibt es nur sehr wenige Kontrollen auf den versteckten Wegen des Darknet. Die Fahrstrecke mit ihren zahlreichen Abzweigungen ist schwer nachzuverfolgen. Dabei kann der ▸

Geländewagen genau wie der sportliche Flitzer auch die Autobahn benutzten, fährt dann aber eher 80 km/h als 150 km/h.

DARKNET IST NICHT GLEICH DARKNET

Das beliebteste und bekannteste Geländewagenmodel ist dabei das sogenannte TOR Browser Bundle. TOR steht dabei für The Onion Router und basiert auf der Firefox Technologie, ist also auch für den Laien einfach zu nutzen. Die verschlungenen Waldwege sind in unserer Metapher die dazugehörigen Seiten mit der Endung .onion. Sie können nur über den entsprechenden Browser gefunden werden. Um ans Ziel zu kommen, kann man Suchmaschinen wie Torch, Ahmia oder OnionLink nutzten, kommt dabei aber nicht unbedingt dahin, wo man will. Auch zu empfehlen ist DuckDuckGo, das auch im Clearnet funktioniert und im Gegensatz zu Google keine Daten sammelt. Eine weitere, weitaus verlässlichere Möglichkeit zu navigieren sind Linklisten, die beispielsweise auf dem Hidden Wiki zu finden sind. Diese veralten aber regelmäßig. Grundsätzlich ist ein Darknet eine Art überlagernde Knoten-zu-Knoten-Kommunikation, die für bestimmte Zugänge wie im Fall des .onion-Darknets über den TOR Browser genutzt werden kann. Diese sind – wie im Clearnet – ebenfalls dezentral gesteuert. Ein Darknet ist sozusagen ein privates Netzwerk, das allein dadurch schon besser geschützt ist, weil nicht jeder dazu Zugang hat.

Entstanden ist TOR aus dem Bedürfnis des amerikanischen Militärs, seine Leute vor Überwachung dritter, meist nicht wohlgeneigter Staaten zu schützen und frei mit der heimatlichen Motherbase kommunizieren zu können. Heute wird dieses militärische Kind der späten neunziger Jahre von der linken NGO The TOR Project betreut. Allerdings spritzt das amerikanische Militär immer noch Geld in das laufende Projekt, wohl bis zu 80 Prozent der gesamten Einkünfte. Mittlerweile gibt es ein eigens TOR-Netzwerk mit über 4.000 Knotenpunkten, die das Verschlüsseln der Daten vereinfachen. Jeder mit einem Server kann hier beitragen. Und so emanzipiert sich TOR langsam durch ein Netzwerk und auch neue Geldgeber in Form von Privatpersonen, die das Projekt unterstützten. Allerdings geht man davon aus, dass auch Geheimdienste wie die NSA zahlreiche Knoten dieses Netzwerks betreiben.

DAS INNERE DER ZWIEBEL

Die Namensgeberin, die Zwiebel, kommt dabei nicht von ungefähr. Onion Routing ist eine Anonymisierungstechnik, die darauf basiert, dass man über mehrere Knoten geleitet oder, um das Bild der Zwiebel zu bedienen, durch mehrere Schichten hindurchdringen muss, um ans Ziel zu kommen. TOR nutzt hier in der Regel drei Knoten, um einen zur gewünschten Webseite zu bringen. Die Anfragen werden jeweils verschlüsselt, die Spur verschleiert, die Identität geschützt. Die Betreiber der Knoten können Ausgang und Zielpunkt nicht verfolgen, wodurch das Surfverhalten nicht nachvollziehbar ist. Je sicherer man hier surft, desto langsamer wird aber die Geschwindigkeit. Verschlüsselung und Umleitung dauern länger als ein direkter Weg über die Datenautobahn. So kann man sich auch mithilfe des TOR-Browsers im Clearnet recht unerkannt bewegen. (Checkt auch unsere Rubrik »Und jetzt kommst du!« – mit Tipps zum Umgang mit TOR – aus)

Doch nicht nur der Traffic, sondern auch die Namensauflösung läuft dabei anders als beim »normalen Internet« über drei zufällig ausgewählte Knoten des TOR-Netzwerkes. Kurzum: Der Betreiber einer .onion-Seite bleibt erstmal anonym und ist dadurch besser geschützt als im offenen Netz. Dabei kann man sich eine .onion-Domain nicht aussuchen. Sie werden softwaregeneriert und bestehen aus einer 16-stelligen Abfolge. Topplayer wie Facebook verfügen auch über eine .onion-Seite: facebookcorewwwi.onion. Hier wurde einfach solange probiert, bis der richtige Name gefunden war. Das macht es dann auch so schwierig, sich in dem Netzwerk zu bewegen: Die Namen der Seiten können größtenteils nicht antizipiert werden. Man muss sie kennen oder eben über Links verfügen.

UNENDLICHE WEITEN, KRIMINELLE TIEFEN?

Während das Deep Web extrem groß ist und exponentiell immer weiter wächst – derzeit geht man davon aus, dass es etwa 5.000 mal größer ist als das Oberflächen-Netz –, ist das Darknet nach Schätzung des TOR-Project recht klein. Die NGO bittet die Betreiber der Netzwerkknoten regelmäßig um Auskünfte, aber nur die Hälfte liefert Daten. Daraus ergibt sich eine Schätzung von etwa 60.000 Adressen im .onion-Darknet. Wissenschaftliche Studien kommen sogar noch auf geringere Zahlen: Für eine Untersuchung, entstanden am King's College in London, wurden Anfang 2015 .onion-Seiten gesammelt. Viele ließen sich gar nicht aufrufen. Lediglich 5.200 reagierten und hier fanden die beiden Forscher Thomas Rid und Daniel Moore nur etwa bei der Hälfte Inhalte. Interessanterweise wird TOR fast ausschließlich im Westen genutzt. Die Datenströme verlaufen hauptsächlich zwischen Nordamerika und Europa. Das Netzwerk breitet sich aber stetig weiter aus.

Dabei hört man immer wieder, dass das Darknet ein gefährlicher Ort und die Inhalte alles andere als jugendfrei seien. Hier wird zwar übertrieben – ganz falsch ist es allerdings nicht. Die Studie »Deeplight: Shining a Light on the Dark Web« untersuchte 13.600 .onion-Seiten und errechnete, dass nur 52 Prozent der Inhalte nach UK- und US- Recht legal sind. Die Auswertung ergab Folgendes: 29 Prozent stellen Filesharing-Dienste, 28 Prozent geleakte Daten und 12 Prozent Finanzbetrug dar. Auf 4 Prozent der untersuchten Webseiten wird mit Drogen gehandelt und nur 0,3 Prozent haben Bezug zu Waffen. Die oben genannte Studie des King's College kommt auf ähnliche Zahlen: Insgesamt seien 43 Prozent der untersuchten Seiten als legal einzustufen. Von den restlichen illegalen Angeboten entfielen 15 Prozent auf Drogen, 12 Prozent auf Finanzgeschäfte, 7 Prozent auf andere illegale Inhalte und 1,5 Prozent auf Waffen. Außerdem gilt auch hier wie im Clearnet, dass kriminellen Sei-

ten durchaus der Garaus gemacht werden kann, wenn man will. Prominentestes Beispiel ist die Seite »Silk Road«, auf der man neben Drogen auch Waffen mit Bitcoins kaufen konnte. Der Gründer Ross Ulbricht wurde zu lebenslanger Haft verurteilt. Der Schuldspruch basierte auf Drogenhandel und Geldwäsche und sollte ein Exempel für kriminelle Seiten im Internet statuieren. Die Strafe erscheint drakonisch und befeuert dadurch verschiedene Verschwörungstheorien im Zusammenhang mit der Dämonisierung des Darknet. Der ehemalige Physikstudent Ulbricht sieht sich selbst als Bauernopfer.

LET'S GO DARK

Sein ursprünglicher Nutzen jedoch, nämlich unerkannt zu kommunizieren, spielt vielen politischen Aktivisten, Whistleblowern und Journalisten in die Hände.

Beispiel Arabischer Frühling: Das TOR-Netzwerk wurde aktiv genutzt, um sich auszutauschen, zu informieren und dabei trotzdem anonym zu bleiben. Es kann einen Schutzmantel bieten, wo wachsame Augen sind. Edward Snowden hat TOR genutzt, um die Unterlagen, welche die Massenüberwachung durch den NSA belegten, an relevante Medienhäuser zu spielen. Der Guardian, die Washington Post und auch die Taz verfügen über anonyme Postfächer für genau solche Zwecke. Dabei lassen sich drei Arten der »hellen« .onion-Nutzung unterscheiden: als Infrastruktur, zum Beispiel für filesharing; als alternative Zugangstür zu Seiten von Medien wie der taz; und als originäre .onion-Inhalte wie der Auftritt der Gruppe Code:Green. Das explizit politische Kollektiv stellt hier Informationen und Tools für einen »Hacktivismus für eine bessere Welt« zur Verfügung und befeuert damit die Aufklärung der interessierten Webgemeinde.

Um sich aktiv vor verschiedentlichem Datenkrakentum zu schützen, kann jeder von uns TOR nutzen, denn der alternative Browser ist einfach zu bedienen. Ob man nun eine .onion-Seite besuchen will oder nicht, ist jedem selbst überlassen. Freiheit wird hier zu Sicherheit und umgekehrt. Nur kontrollieren lässt sich das Ganze eben schwer. Das öffnet natürlich auch Kriminellen Tür und Tor, aber eben solchen, die verbotene Güter anbieten und nicht jenen, die uns ausspionieren und schröpfen wollen. Die dunkle Seite des Darknet sind meist Marktplätze. Dabei sollte man wie mit allem im Leben auch hier die nötige Vorsicht walten lassen, und wenn man neugierig ist, lieber noch über andere Schutzmechanismen wie beispielsweise einen VPN nachdenken. Wir werden jeden Tag überwacht und nichts im Internet ist frei. Schließlich bezahlen wir jeden Tag mit unseren Daten für all die bunten kostenlosen Dienste.

Das Darknet hat für viele, die sich damit beschäftigen, ein unglaubliches Utopie-Potenzial. Es trägt noch immer die Werte des frühen Internet in sich: Freiheit und Gemeinschaft. Es hat etwas Rebellisches, es fördert die Anonymität, es hält die Privatsphäre hoch. Dadurch spiegelt es seinen Nutzern gegenüber Respekt, den unser Google-Internet längst verloren hat. Möglichst bequem sollen wir durch die Welt gehen und werden so auch entmündigt. Und spätestens hier muss sich jeder Einzelne von uns fragen, was ihm wichtiger ist: ein bequemes Leben, bei dem alles nur einen Klick entfernt ist, dafür aber überwacht wird, oder die eigene Anonymität und der Schutz vor dem großen Bruder, was aber auch bedeuten kann auf Dinge verzichten zu müssen und den Kopf etwas mehr anzustrengen. Vielleicht ist es am Ende gar nicht eine Entscheidung zwischen Diesem und Jenem, sondern ein Weg, der sich erst gabeln muss, um dann wieder zu einem zu werden. •

Wenn man will, findet man ziemlich viel über **Elisa Bilko** im Netz. Allein ihre Profile auf Xing und LinkedIn verraten einiges über ihren Werdegang. Was man allerdings nicht im WorldWideWeb findet, ist ihre Hochzeit. Sie war sieben und der Bräutigam ein Kaninchen. Gut, dass es in den Neunzigern keine Smartphones gab, sonst wäre dieser besondere Tag sicher auf Facebook gelandet. Andererseits wäre das auch ziemlich lustig.

ZUM WEITERLESEN UND -SCHAUEN

Ted Talk von Filmemacher **Alex Winter**: Er drehte eine Dokumentation zum Fall »Silk Road«.

Ted Talk von Journalist **Alan Pearce**, der sich auf Cyber-Sicherheit und digitale Gegenüberwachung spezialisiert hat.

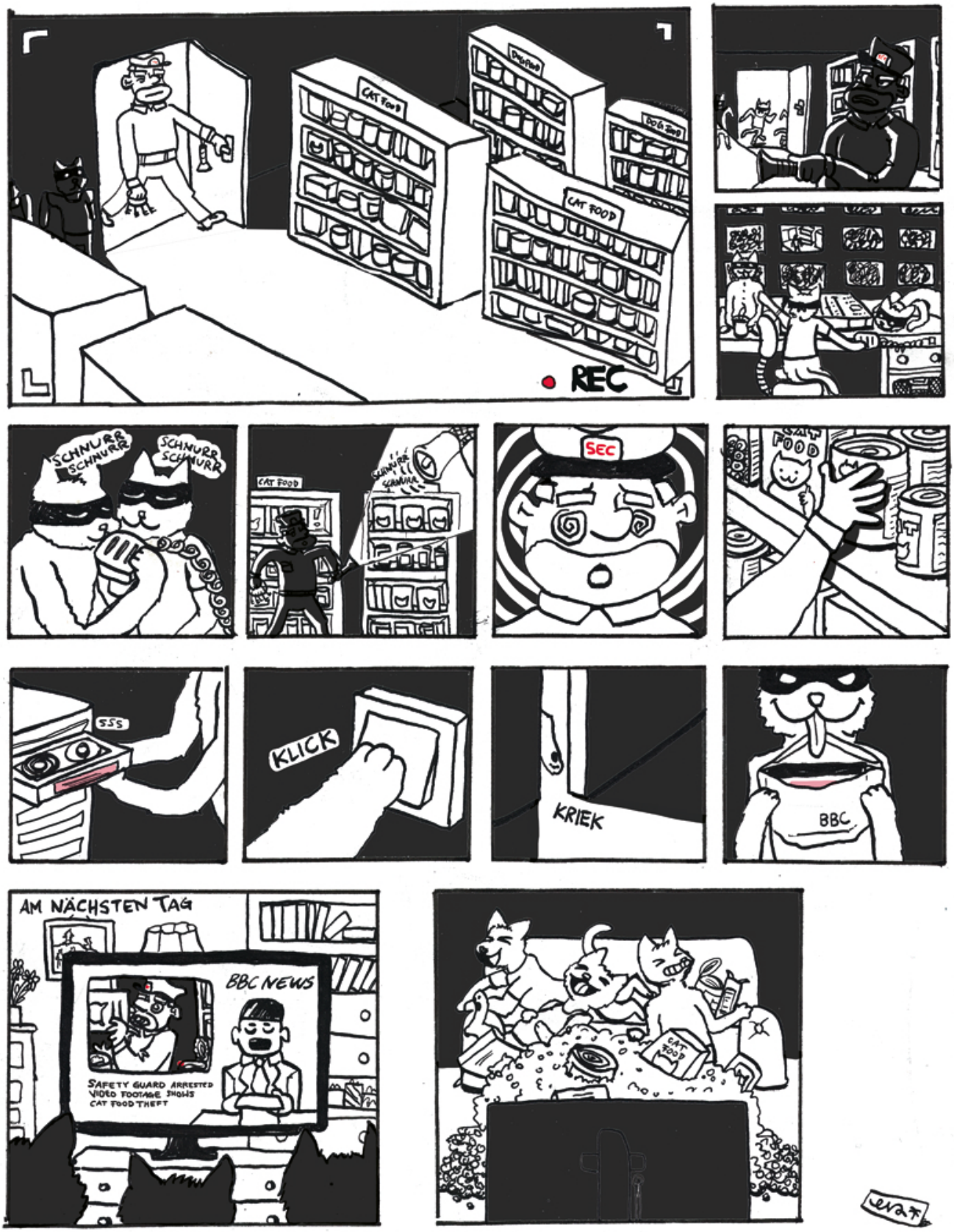
Ted Talk von Ingenieur und Computer-Historiker **Kyle Terry** mit einer Einführung in weitere Darknets.

Das Buch **Darknet** von **Stefan Mey,** dem hier besonderer Dank gebührt, da er als Experte auf dem Feld die Autorin freundlicherweise in das Thema eingeführt hat.

PET STORE
EXIT
KATER DEMOS PRESENTS:
THE PURRFECT CRIME

WÜRG
WÜRG
WÜRG

SEC


CAT FOOD
CAT FOOD
REC
SCHNURR SCHNURR
SCHNURR SCHNURR
CAT FOOD
SEC
CAT FOOD
555
KLICK
KRIEK
BBC
AM NÄCHSTEN TAG
BBC NEWS
SAFETY GUARD ARRESTED VIDEO FOOTAGE SHOWS CAT FOOD THEFT
CAT FOOD

VICTIM SURVEILLANCE CINEMA

Filme machen uns alle zu Voyeuren. Kein Wunder also, dass das Thema Überwachung auch im Kino in all seinen Facetten zur Geltung kommt. Hier sind neun, von der Kater Demos Redaktion handverlesene Filme zum Thema, die zum Grübeln, Gruseln und manchmal auch Grinsen einladen.

TEXT ROMAN OBST, JONAS IBEL UND ELISA BILKO

ILLUSTRATION EVA PALM

CITIZENFOUR

2014, USA/D

Eines Tages erreicht die Journalistin Laura Poitras eine kryptische Nachricht über ihren verschlüsselten E-Mail Account. Citizenfour – so nennt sich der Unterzeichner – stellt ihr in Aussicht, dass er bereit dazu ist brisante Informationen aus dem Geheimdienstapparat der USA an die Öffentlichkeit zu bringen. Hinter dem Pseudonym steckt Edward Snowden, der heute so bekannte Whistleblower. Er wird vom Überwacher zum Überwachten. Wohlwissend, welche Macht das System besitzt, muss nun jeder Schritt geplant und bedacht werden. Der ausgezeichnete Dokumentarfilm folgt den Protagonisten in ein Klaustrophobie auslösendes Hotelzimmer in Hongkong, in dem sie unter Hochspannung darauf warten, dass die geleakten Dokumente von der Presse veröffentlicht werden.

ALTERNATIVE: SNOWDEN

Gleiche Story im Hollywoodstil dramatisiert.

DAS LEBEN DER ANDEREN

2006, D

Gerd Wiesler ist ein Stasi-Mann wie er im Buche steht: akkurat und ordnungsliebend geht er seinem Beruf als Überwacher mit einer stoischen Leidenschaft nach. Bis er anfängt einen systemunkritsichen Schriftsteller und dessen Freundin zu überwachen. Als allsehendes Auge entwickelt er sich vom Schnüffler zum Schutzengel, kann die unmenschlichen Mühlen des Systems aber nicht aufhalten. Nicht umsonst hat dieser Film den Oscar bekommen. Einfühlsam und trotzdem dramatisch zeigt er die Pervertierung eines Systems, dem sowohl Überwachter wie auch Überwacher beide zum Opfer fallen.

ALTERNATIVE: ENGELBECKEN

Eine Doku über Paranoia, Depression und Liebe zwischen Ost- und Westberlin.

DAS FENSTER ZUM HOF

1954, USA

Alfred Hitchcocks Thriller »Das Fenster zum Hof« (engl. Rear Window) aus dem Jahr 1954 zählt zu den grandiosen Werken der Filmgeschichte: Der Fotograf L. B. Jefferies (James Stewart) kann wegen eines gebrochenen Beins seine Wohnung nicht verlassen. Als Ablenkung beobachtet er mit dem Fernglas die Fenster seiner Nachbarn und verfolgt darin deren alltägliche Geschichten. Durch seine Gehbehinderung kann er nicht eingreifen, als er glaubt, Zeuge eines Mordes in der Wohnung gegenüber zu sein. Das Fenster zum Hof ist der vielleicht meistbesprochene Film Hitchcocks: Da die Kamera nie die Wohnung verlässt, repräsentiert der zum Zuschauen verurteilte Protagonist wie kaum eine andere Filmfigur den voyeuristischen Zuschauer selbst.

ALTERNATIVE: DISTURBIA

…heißt die verstörend langweilige Neuverfilmung von 2007.

1984

1984, UK

George Orwells Klassiker des dystopischen Romans ist wieder aktuell. Nachdem die neue US-Regierung den orwellschen Begriff der »Alternativen Fakten« geprägt hatte, schaffte es das Buch aus dem Jahr 1949 kurzerhand auf die Amazon-Bestsellerliste. »So, is the age of Newspeak here?«, fragt sich der Guardian. Wem das Buch zu lange dauert, empfiehlt sich die britische Verfilmung von Michael Radford aus dem – sehr naheliegendem – Jahr 1984. John Hurt, bekannt aus Snowpiercer (Gilliam) und Harry Potter (Ollivander), spielt darin den Gedankenverbrecher Winston Smith. Die markante Ästhetik des Films hatte einen sichtlichen Einfluss auf die Produzenten des späteren Gameklassikers Half Life 2.

ALTERNATIVE: 1984

Wer trotzdem gerne schwarzweiß guckt, kann auch zur Verfilmung von 1956 greifen.

BRAZIL

1985, UK

Ein Film über den Wahnsinn der Postmoderne von Monty Python Mitbegründer Terry Gilliam (Time Bandits, 12 Monkeys) aus dem Jahr 1985. Protagonist Sam Lowry, gespielt von Jonathan Pryce (High Sparrow in Game of Thrones), ist ein kleiner Angestellter im Archiv der Abteilung für Informationwiederbeschaffung im allmächtigen Ministry of Information einer bürokratisierten und technisierten Gesellschaft. »Eine düstere, kafkaeske Dystopie, die sich der Stilmittel der grotesken Komödie bedient«, heißt es über den Film, der ursprünglich als Anspielung »1984 and ½« heißen sollte. Dieser Klassiker des dystopischen Kinos ist damit ebenso sehenswert wie 1984 lesenswert ist. War einst sogar erst ab FSK-18 zu sehen.

ALTERNATIVE: THE ZERO THEOREM

Vor vier Jahren machte Terry Gilliam einen vergleichbaren Film diesmal mit Christoph Waltz in der Hauptrolle

DRONE – THIS IS NO GAME!

2014, NORWEGEN

Was hat Call of Duty mit Drohnen zu tun? Die Verstrickungen der Computerspielindustrie sowie des Finanzwesen in Drohnenkriege sind nicht von der Hand zu weisen. Die Skills, die Computerspieler erlernen, um Pixel abzuschießen, kommen dem Militär dabei sehr gelegen. So sehr, dass es mittlerweile die Drohnensteuerung zu einem First-Person-Shooter umgestaltet hat. Der Dokumentarfilm zeigt das Geschäft rund um den Drohnenkrieg auf ruhige Art und Weise. Greifbar wird, was so schwer zu glauben ist, dass das Militär mit Computerspielen die nächste Generation an Soldaten heranzieht.

ALTERNATIVE: KRIEG UND SPIELE

Deutsche Doku zum gleichen Thema, die es etwas drastischer auf den Punkt bringt.

DIE TRUMAN SHOW

1998, USA

Die Prämisse der Truman Show ist so wahnsinnig wie beängstigend: Ein Baby wird von einem Fernsehstudio gekauft und über eine Show vermarktet. Während es zum Erwachsenen heranwächst, ist es nur von Schauspielern umgeben und jeder Tag wird live übers Fernsehen übertragen. Eines Tages aber fällt ein Scheinwerfer direkt vor die Füße von Truman, wie unseres Protagonist ironischerweise heißt. Seine Paranoia, die ja gar keine ist, treibt ihn dazu über sich hinauszuwachsen. Der Film ist natürlich Dank Jim Carrey unglaublich unterhaltsam, wirft aber neben zahlreichen anderen Moralfragen (der Mensch als Kapital; Medien, die alles Menschliche pervertieren, etc.) auch jene, nach unserem Verhalten unter Beobachtung auf. Trumans Lösung: Flucht!

ALTERNATIVE: BIG BROTHER

Wem die Truman Show nicht absurd genug ist, kann sich ja ein paar Leute im Container ansehen.

MINORITY REPORT

2002, USA

Spannungsgeladen bis zum Schluss entführt uns Steven Spielbergs Minority Report in eine nahe Zukunft, in der Morde verhindert werden, bevor sie überhaupt geschehen. Das ist einmal drei Zwillingen mit übersinnlichen Fähigkeiten zu verdanken und zum anderen einem hochmodernen System flächendeckender Überwachung. Die Iris eines jeden ist hinterlegt und wird im öffentlichen Raum automatisch gescannt, was nicht nur der Überwachung sondern auch personalisierten Bewerbung der Bürger dient. Gelobt für seinen Realismus und das trotz fantastischer Sci-Fi Elemente, setzt sich der Spielfilm mit Tom Cruise kritisch mit der Frage nach freiem Willen und dem Mehrwert von Überwachung auseinander ohne die Schattenseiten dabei zu vergessen.

ALTERNATIVE: AM ENDE DER GEWALT

Ein Wim Wenders Film mit Starbesetzung, der über Gewalt sinniert und deren Verhindern durch Totalüberwachung thematisiert.

GOOD KILL

2014, USA

Good Kill: Das ist der knappe Kommentar des Befehlshabers, wenn die Drohnen wieder erfolgreich zugeschlagen haben. Ethan Hawk spielt einen ehemaligen Soldaten der Luftwaffe, der jetzt als alles sehender Überwacher Drohnen kontrolliert – weit weg von den Einsatzorten und ohne je dem Feind ins Gesicht zu sehen. In der Wüste Nevadas führt er ein perfides Doppelleben: tagsüber ist er ein eiskalter Killer, nachts ein liebender Familienvater. Der Spielfilm zeigt uns, welche Auswirkungen der Drohneneinsatz tausende Kilometer entfernt auf die Soldaten hat, die den Schießbefehl ausführen.

ALTERNATIVE: EYE IN THE SKY

1
2
3
alexa

»ALEXA, WER IST DER MÖRDER?«

Selbstdenkende Computer waren lange Zeit eine Fiktion, direkt von Captain Kirks Brücke. Aber mit der fortschreitenden Entwicklung von Künstlicher Intelligenz sind sie greifbar nah. Das erfreut nicht nur Science-Fiction-Fans, sondern auch Hacker und Ermittlungsbehörden.

TEXT VIKTOR MARINOV & PHILIPP STEFFENS
ILLUSTRATION FLORIAN THIEMANN

Wenn James Bates vor Gericht seine Unschuld in einem Mordfall beweisen muss, könnte ein unerwarteter Zeuge auftreten: seine Lautsprecheranlage. Der 31-Jährige aus Arkansas soll den ehemaligen Polizisten Victor Collins umgebracht haben. Der Lautsprecher von Bates könnte das gehört haben. Denn er heißt »Echo«, und in ihm steckt die künstliche Intelligenz Alexa, Amazons neuestes Gadget für das eigene vernetzte Zuhause.

Echo kann vieles: Produkte bestellen, Spotify-Playlisten abspielen, die Wetterprognose heraussuchen, Einkaufslisten führen oder Witze erzählen. Die Steuerung erfolgt über Sprachbefehle, die mit dem richtigen Codewort beginnen müssen, standardmäßig Alexa, der Name der Sprachassistentin. Damit Alexa mit ihrer sanften Stimme helfen kann, muss sie immer zuhören.

ECHO IST IMMER AN UND HÖRT DICH VON ÜBERALL

»Ach, es ist immer an.« Das sind nicht etwa die mahnenden Worte eines Datenschützers, sondern Amazons Selbstdarstellung. In der ersten Werbung für Echo von 2014 präsentiert ein Familienvater stolz sein neuestes Spielzeug. »Es kann dich also von überall hören?«, fragt darauf der Sohn. »Ja. Aber jeder kann dich ohnehin von überall hören«, sagt der Vater. Die Worte sollen beruhigend wirken. Das Video wurde mittlerweile von YouTube entfernt.

Sieben permanent aktive Mikrofone sind im Inneren des zylindrischen Gehäuses eingebaut. Sie sind so ausgerichtet, dass das Gerät von jedem Punkt im Raum bedient werden kann. Amazons Gründer Jeff Bezos erklärte dazu bei einem Vortag, dass die Firma einen mechanischen Ausschalter an dem Gerät verbaut habe. Mit diesem können die Mikrofone abgeschaltet und nicht wieder über Software oder Sprachbefehle reaktiviert werden.

Ob Nutzer das wirklich tun, ist fraglich, denn ohne Sprachassistenz ist Echo nur ein gewöhnlicher Lautsprecher. Dass er deswegen meistens eingeschaltet ist, zeigte ein Fernsehbericht in den Lokalnachrichten von San Diego. Diese berichteten über ein sechsjähriges Mädchen, das beim Spielen mit Alexa ein Puppenhaus und zwei Kilogramm Kekse bestellte. Bei der Ausstrahlung des Beitrags fühlten sich in San Diego viele Alexas angesprochen und bestellten ebenfalls Puppenhäuser und Kekse – standardmäßig bestellt Alexa nämlich die Produkte sofort. Wer sichergehen will, muss erst nachträglich via Code eine Schranke aktivieren, damit nicht jeder x-beliebige Schalk ungewünschte Dinge über Amazon ordern kann.

ZEUGEN, DIE IMMER AUSSAGEN

Der Datenschutzbeauftragte der Stadt Hamburg, Johannes Caspar, nennt Alexa eine »Abhöreinrichtung«. Man hole sich mit solchen Geräten Mikrofone in die privateste Sphäre, in die eigenen vier Wände. Was mit den Aufzeichnungen geschehe, wisse der Nutzer schließlich nicht genau. Denn die Verarbeitung der Befehle erfolgt nicht lokal, ▸

sondern auf einem Server von Amazon. Dafür muss das Gesprochene übertragen werden.

Um diese Daten geht es in dem Fall Bates. Die Polizei vermutet, dass in der Nacht im Februar letzten Jahres vielleicht etwas mitaufgezeichnet wurde, das ihn überführt. Ein Streit, ein Schlüsselwort, die Stimme des ermordeten Collins allein könnte schon Aufschlüsse über den Tathergang geben. Einen weiteren mechanischen Zeugen aus Bates‹ Haushalt hat die Polizei bereits ausgewertet, seinen Wasserzähler. Dieser kann den stündlichen Wasserverbrauch anzeigen und speichern. So kann man genau sehen, wann wie viel Wasser verbraucht wurde. In Bates' Fall zeigt der Wasserzähler, dass in der Nacht zwischen 2 und 3 Uhr sehr viel Wasser verbraucht wurde. Da Collins tot im Whirlpool gefunden wurde, könnten diese Daten für die Aufklärung des Falls kritisch sein. Für den Wasserzähler gilt kein Aussageverweigerungsrecht. Und für Alexa?

Auch nicht, sagt Caspar. Seit dem »Patriot Act«, der nach dem 11. September in den USA verabschiedet wurde, müssen US-Unternehmen mit lokalen Sicherheitsbehörden und Geheimdiensten zusammenarbeiten: »Es ist anzunehmen, dass derartige Zugriffe der Ermittlungsbehörden in den USA zur Normalität werden, da dort der rechtliche Rahmen entsprechende Möglichkeiten bereithält«, so Caspar zu dem Fall Bates. Auch in Deutschland sei davon auszugehen, dass Audio-Daten zur Strafverfolgung benutzt werden können. Die Gesetzgebung in Deutschland habe hier Nachholbedarf. Doch bis dahin könnte Alexa weit verbreitet sein.

AUF DEM WEG ZUR WELTEROBERUNG

Alexa und ihre Brüder und Schwestern von Firmen wie Microsoft, Apple, Google und Samsung sind ein Teil des »Internet of Things«. Im neuen Internet der Dinge soll alles miteinander vernetzt sein. Nun bekommen viele Geräte nicht nur einen WLAN-Anschluss, sondern auch ein Ohr und eine Stimme.

Auf der diesjährigen Consumer Electronics Show (CES), eine der größten zukunftsweisenden Fachmessen für Technologie, standen Sprachassistenten im Mittelpunkt der Aufmerksamkeit, allen voran Alexa. LG präsentierte einen smarten Kühlschrank mit großem LCD-Bildschirm, Ford kündigte Autos mit Sprachassistenz an, Lenovo zeigte neue Lautsprecher, Samsung führte den Saugroboter »Powerbot VR7000« vor und First Alert versuchte Kunden für einen Sensor zu gewinnen, der Temperatur und Sauerstoffgehalt im Kinderzimmer überwacht. Alexa ist der gemeinsame Nenner dieser neuen Gadgets, denn sie alle lassen sich über sie steuern. Echo selbst wurde bereits über fünf Millionen Mal in den USA verkauft. Das US-Technologie-Magazin Wired titelte nach der Messe: »Alexa just conquered CES. The World is next.« Alexa eroberte die CES, nun ist die Welt dran.

DEIN FREUND UND HACKER

Diese rasante Entwicklung birgt Gefahren, die nicht nur davon abhängen, ob Hersteller wie Amazon Aufnahmen weitergeben müssen. Die Möglichkeit, dass Sprachassistenten von Hackern missbraucht werden, sei real, so Caspar. »Im Zweifel sind Hacker immer erfolgreicher als Produktentwickler«, warnt er weiter. Es ist einfacher, eine Sicherheitslücke zu finden, als alle zu schließen.

Das wissen auch Sicherheitsbehörden wie das FBI. Dass sie im Zweifelsfall auf externe Hilfe zurückgreifen, zeigt ein Fall von letztem Jahr. Es ging dabei um Daten auf dem iPhone von Syed Rizwan Farook, einer der Attentäter von San Bernardino. 14 Menschen wurden bei dem Terroranschlag getötet, 21 weitere verletzt. Zur Aufklärung wollte das FBI Zugriff auf das Handy von Farook, doch Apple weigerte sich, dabei zu helfen.

Apple sträubte sich, weil die Befürchtung bestand, dass dies ein Präzedenzfall sein könnte, um auch die Verschlüsselung von anderen iPhones zu legalisieren. Und tatsächlich hatte das US-Justizministerium bereits weitere Fälle zurechtgelegt, die nur auf die Entschlüsselung von Mobiltelefonen warteten. Da Apple nicht half, kaufte das FBI einen »Exploit« von der israelischen Sicherheitsfirma Cellebrite. Ein Exploit ist eine Schwachstelle im Code, die ausgenutzt werden kann, um Zugang zum Inhalt eines Telefons zu bekommen. Im Zuge der Debatte, ob Apple von Anfang an hätte kooperieren sollen, kam auch die Forderung nach staatlichen Backdoors, also bewusst eingebauten Schwachstellen in Hard- und Software auf.

Es ist nicht unmöglich, dass in absehbarer Zeit das Gleiche von Sprachassistenten-Herstellern gefordert wird. Bei Bates konnte sich Amazon noch damit absichern, dass nur Kundeninformationen preisgegeben werden, wenn es einen richterlichen Beschluss gibt.

GEFANGEN IM EIGENEN HAUS

Künstliche Intelligenz wie Alexa ist der Schlüssel zum vernetzten Haushalt. Per Sprachbefehl oder Smartphone steuerbar, verspricht das Internet der Dinge seinen Nutzern die vollkommene Kontrolle über ihr Heim. So verführerisch dies sein mag, besteht die Gefahr, dass man gleichzeitig die Kontrolle an Andere verliert. Schon heute greifen Hacker Computer an und verlangen zur Befreiung Bitcoins. Mit Sprachassistenten könnten sie bald den Kühlschrank wärmer werden lassen, ins Wohnzimmer lauschen, sogar die Tür absperren; oder eben unzählige ungewollte Puppenhäuser bestellen. •

WAS ICH EIGENTLICH SAGEN WOLLTE...

BLA BLA ÜBER BLA BLA ÜBERWACHUNGA

TEXT JOHANNES HEIM

Stell Dir vor, dass Thomas de Maizière (CDU) in Deinem Wohnzimmer sitzt und Dich beobachtet, bei allem, was Du so tust. Immer. Da sagt er dann Sachen wie: »Und die Vorratsdatenspeicherung ist ja nichts weiter, als dass der Staat den Unternehmen sagt: ›Wir zwingen euch, einige Monate die Verbindungsdaten aufzuheben, die ihr früher sowieso aufgehoben habt.‹ Um dann, wenn ein Richter es für geboten hält, bei der Aufklärung schwerster Straftaten mit der Polizei darauf zugreifen zu können. Mehr ist das gar nicht.«

So gesprochen gegenüber dem Fernsehsender Phoenix Anfang 2015. Damit machte er eigentlich klar: »Stellt euch nicht so an, das war doch eh schon immer so.« Wenn einem die Argumente ausgehen, dann kommt man immer mit dem »Das haben wir immer schon so gemacht!« Vielleicht war es aber auch vorher schon nicht in Ordnung?! Wieder einmal musste das Bundesverfassungsgericht der CDU erklären, wie das mit grundrechtskonformen Gesetzen so funktioniert. Auch ist es ein großer Unterschied, ob ein Unternehmen Daten nur speichert oder sie auch herausgibt. Und ob das mit Zustimmung des Nutzers geschieht oder auf Anordnung des Staates.

Jeder Datenschützer atmete wohl auf, als Wolfgang Schäuble (CDU) nicht mehr Innenminister war, sondern sich den Finanzen zuwendete. Denn Sprüche von ihm wie: »Den Rechtsstaat macht aus, dass Unschuldige wieder frei kommen« (Taz, 2008) sind Klassiker von »Wer nichts getan hat, hat auch nichts zu verbergen.« Aber natürlich kann man auch bei diesem Thema wieder mit »Wer hat uns verraten? Sozialdemokraten!« ankommen (übrigens ein Spruch der KPD aus dem Jahr 1930). Denn unter Sigmar Gabriels Drängen knickte Heiko Maas immer weiter ein und ging von seiner vehementen Antihaltung zur Vorratsdatenspeicherung über zu einer Variante von: »Naja, immerhin ist das alles nicht so schlimm wie damals«, wie Maas in diversen Tweets zu diesem Thema verlauten ließ.

Dabei herrschte einmal im Hause Maas die Meinung: »#VDS lehne ich entschieden ab – verstößt gg Recht auf Privatheit u Datenschutz. Kein deutsches Gesetz u keine EU-RL!« (Tweet vom 15. Dezember 2014) Wilfried Albishausen vom Bund der deutschen Kriminalbeamten fasst zwar korrekt gegenüber dem Focus im Jahr 2008 zusammen, dass »Gesetzgeber und Ermittler [...] mit der Vorratsdatenspeicherung nicht den gläsernen Bürger [wollten], sondern den gläsernen Straftäter.« Dabei macht der Staat aber, selbst wenn es unwillentlich ist, den Bürger ebenso gläsern. Das Gegenteil von ‚gut‹ ist und bleibt eben ›gut gemeint‹.

Johannes Heim wollte alles mögliche werden, an irgendeinem Punkt auch mal Journalist. Studiert hat er dann im Endeffekt Philosohie und Geschichte und jetzt überwacht er von Berufs wegen: Als Online-Marketer analysiert er wie viele was wieso kaufen und wie man das optimiert. Er duscht abends und nicht morgens.

III VIVE LA RÉVOLUTION!

VON JONAS IBEL

Im dritten Teil des Roten Fadens reisen wir weiter durch die Geschichte der Privatsphäre. Wir folgen unseren Zeitzeugen, die im 18. und 19. Jahrhundert versuchen, der Wachsamkeit der Obrigkeit zu entgehen.

Es ist Anfang Juli in Paris, wir schreiben das Jahr 1789. Steigende Brotpreise und der Kampf des Königs gegen das protestierende Volk treiben die Menschen auf die Barrikaden. In konspirativen Treffen, den sogenannten Salons, entwickelt sich die Agenda der Aufklärung. Die Aufklärer fordern, ihre Meinung frei äußern zu dürfen, werden dafür aber von Spionen verfolgt und verhaftet.

Jacques, Schuhmacher in einer Manufaktur, wohnt im Osten von Paris. Er leidet Hunger, seit Brot dreimal mehr kostet als im letzten Jahr. Frustriert geht er jeden Tag zur Arbeit, doch egal wie viel er arbeitet, er wird nie satt. Er entschließt sich am Abend des 12. Juli, seinen Freund Pierre zu treffen, um auf andere Gedanken zu kommen. Er hofft auf ein interessantes Gespräch bei einem Glas Wein in der Schänke. Doch Pierre hat andere Pläne: »Los, steck Dir das an!« sind seine ersten Worte als Jacques das Wirtshaus betritt. Jaques nimmt verwundert das Kastanienblatt entgegen, das ihm Pierre in die Hand drückt. »Das ist unser Erkennungszeichen.« Da dämmert es Jacques: Pierre ist ein glühender Anhänger von Camille Desmoulins, der den Protest gegen den König aus Paris anführt. Die beiden Freunde eilen auf die Straße, nach kurzer Strecke führt Pierre ihn zu einem Hauseingang, klopft auf eine bestimmte Weise und nennt das Passwort – sie werden eingelassen. Man ist misstrauisch, jeder könnte ein Spion der Krone sein. In der Wohnung treffen sie auf eine kampfbereite Truppe, der nur noch eines fehlt, um loszuschlagen: Waffen.

Zwei Tage später fällt die Bastille – als Foltergefängnis ein Hassobjekt der Aufklärer. Die Revolution beginnt. Die nächsten Jahre sind von der Rache am feudalen System geprägt. Die Guillotinen stehen nicht still. Aus Angst vor einer Rückkehr der royalen Macht errichten die Revolutionäre einen Terrorstaat, der paranoide Züge aufweist.

THE EMPIRES STRIKE BACK

Wie sich herausstellt, war die Angst der Aufklärer vor dem Gegenschlag nicht unbegründet. Nach Napoleons Kriegsniederlagen melden sich die Monarchen auf dem Wiener Kongress 1815 zurück, um ihre Stärke zu demonstrieren. Jeder revolutionäre Gedanke sollte von nun an ausgemerzt werden. Demokratische Pionierarbeit wird in Frankreich zunichte gemacht. Besonders repressiv erweisen sich 1819 die Karlsbader Beschlüsse. Unter dem Vorwand einer zufälligen, privaten Zusammenkunft entwickeln die Abgesandten der deutschen Höfe im Kurort Karlsbad einen Maßnahmenkatalog, der es in sich hatte. Nationalistische Burschenschaften, zu dieser Zeit fortschrittlich, werden verfolgt. Als Strafe wartet das Zuchthaus. Strenge Zensur soll verhindern, dass kritische Stimmen allzu laut werden. Ein Polizei- und Spitzelnetzwerk wird aufgebaut, um flächendeckende Überwachung auszuweiten.

Wir schreiben das Jahr 1846. Wilhelm ist Buchhalter in der Manufaktur seines Vaters; er soll nach und nach das Handwerkszeug erlernen, um sie eines Tages zu übernehmen. Berlin ist mittlerweile eine große Stadt, Menschen kommen von überall hier her. Wilhelms Lebensstandard ist auf dem Weg in die Moderne: Gaslampen beleuchten die Straßen bei Nacht und die Familie hat es nicht weit zum nächsten Brunnen. Für fließendes Wasser zu Hause braucht es aber noch ein paar Jahre, Hamburg ist zu diesem Zeitpunkt da Berlin etwas voraus. Auch sein Haus, das er mit seiner Familie bewohnt, geht mit der Zeit. Den Kindern fehlt es an nichts und sie haben ein eigenes Zimmer. Wilhelm und seine Frau schlafen in getrennten Zimmern; daneben besitzt er auch ein Arbeitszimmer, das nur ihm gehört. Zum liebsten Rückzugsort hat er für sich und die Familie eine Gartenlaube im Norden Berlins auserkoren. Dort fährt er hin, wenn ihm die wachsende Stadt zu viel wird. Besonders in letzter Zeit wird auf den Straßen Berlins wieder von Revolution gesprochen. Dabei hatte Wilhelm noch gehofft, diese Zeiten seien vorbei. Früher war er selbst einmal kurz davor gewesen, eine Revolution anzuzetteln – mit seiner Burschenschaft zu Studienzeiten. Aber das hatte er hinter sich gelassen. Statt Pamphlete verfasst er jetzt nur noch melancholische Gedichte.

Wilhelm als privilegierter Sohn eines Industriellen bekommt die Auswirkungen von Hunger und Repression nicht zu spüren und kann sich zu Hause verkriechen. Hier ist die Welt der Privatsalons und Gespräche am Kamin, der Nähkreise und Hauskonzerte mit den Kindern, die kleine Gemeinschaft aus Familie, Gouvernante, Hauslehrer und Personal. Für Systemkritiker bedeutet die Zeit von 1815 bis 1848 jedoch das Gegenteil vom gemütlichen Biedermeier; sie werden überwacht, verfolgt und mundtot gemacht: So muss unter

anderem Heinrich Heine das Land verlassen und auch die Dichter des liberalen »Junges Deutschland«. werden zensiert. Dennoch gelingt im März 1848 eine koordinierte Organisation von Aufständen, die immerhin einen Teil der Missstände adressieren kann.

DEUTSCHLAND, EINIG? VATERLAND

Doch der Kampf gegen das Volk endet nicht mit einer schönen neuen Welt. Zwar gibt es jetzt ein gewähltes Parlament, Reichskanzler Otto von Bismarck bekämpft aber die Zentrumspartei und die Sozialdemokraten. Nach wie vor ist also die freie Meinungsbildung erschwert. Wir schreiben das Jahr 1890. Friedrich, 25, ist auf dem Weg zu einem Treffen des »Berliner Vereins für Naturfreunde«. Dabei interessiert er sich nicht im Geringsten für die lokale Flora und Fauna. Der verhasste Bismarck geht schon seit zwölf Jahren derart gegen ihn und andere Sozialdemokraten vor, dass ihnen nur die Flucht ins Exil, das Gefängnis oder eben die Tarnung als Wanderburschen bleibt. Die ständige Angst vor Hausdurchsuchungen oder der Entdeckung kritischer Schriften sitzt ihm beständig im Nacken und lässt ihn misstrauisch werden. Viele seiner Freunde sind schon nach England gegangen, um von dort aus für die Klassenfrage zu kämpfen, aber er ist hier geblieben. In der Hoffnung, dass sich bald etwas ändern wird.

Tatsächlich wird Bismarck noch im gleichen Jahr entlassen, die Verfolgung der Sozialisten wird nach und nach gelockert. Die Presse erstarkt und wird zu einer bedeutenden Instanz der Gesellschaft. Innerhalb von 100 Jahren vollzieht sich ein großer Wandel: Eine Bildungsexpansion führt dazu, dass die Menschen zunehmend gebildeter und kritischer werden. Frauen dürfen endlich an die Universitäten, die erste schließt in Deutschland 1880 ihr Studium ab, und Mädchen und Jungs werden – damals revolutionär – nun oft zusammen unterrichtet. Auch die Curricula an den Volksschulen werden vereinheitlicht. Nach 1870 wird den Kirchen die Aufsicht über die Schulen entzogen und unter staatliche Obhut gestellt. Um die Kirchen weiter zu entmachten, wurden – schon unter Bismarck – Standesämter eingeführt, die die Ehe staatlich vollziehen sollten. Der Staat besitzt nun mehr Informationen über seine Bürger als jede andere Institution. 1896 tritt das Bürgerliche Gesetzbuch (BGB) in Kraft, das die Rechte von Privatpersonen untereinander regelt und erstmals Frauen die Gleichberechtigung zuspricht.

Den Beweis dafür, dass das Karma manchmal zurückschlägt, liefert das ausgehende 19. Jahrhundert ebenfalls: Bismarck, als Verantwortlicher für tausende Hausdurchsuchungen, wird selbst Opfer einer Störung der Intimsphäre. Nach seinem Tod 1898 brechen zwei neugierige Journalisten in sein Sterbezimmer ein und fotografieren seinen Leichnam. •

1789
Französische Revolution

1799
Napoleon übernimmt die Macht

1815
Napoleon verliert seine letzten Schlachten und wird abgesetzt & Wiener Kongress

1819
Karlsbader Beschlüsse

1848
Märzrevolution

1871
Gründung des deutschen Kaiserreichs

1878
Sozialistengesetze

1896
Bürgerliches Gesetzbuch

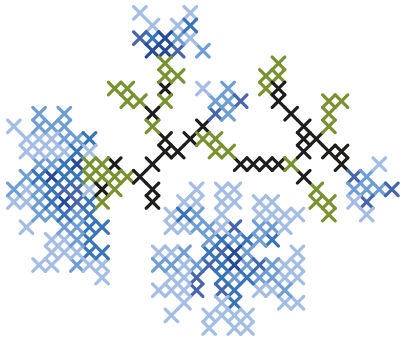
DER ROTE FADEN

TUNDMATU MAA*

*NEULAND AUF ESTNISCH

In Estland leben mit 1,3 Millionen Menschen etwa so viele wie in ganz Mecklenburg-Vorpommern. Viel weiß man in der Regel nicht über das Land: Manche kennen den Musiker Arvo Pärt, denken an Landschaften mit skandinavischem Flair oder eine Sprache mit vielen Vokalen. Seit 2008 ist Estland auch das NATO-Hauptquartier für europäische Cybersecurity und die IT- Hochburg Europas. Ein kurzer Einblick in das Land der digitalen Superlative

TEXT SYLVIA LUNDSCHIEN
ILLUSTRATION NATASCHA KORNILOWA



Die Zukunft begann in Estland am 20. August 1991 im über 1.000 Kilometer entfernten Moskau. Durch einen Putsch gegen Staatspräsident Michail Gorbatschow verlor dort die sowjetische Führung die Kontrolle über ihre Satellitenstaaten – darunter auch Estland. Der baltische Staat war seit 50 Jahren sowjetisch besetzt, 1990 erklärte man sich einseitig souverän. Der Sommer 1991 wurde durch den Putsch zur Geburtsstunde der unabhängigen Republik Estland und des Aufstiegs des kleinen Landes zur IT-Hochburg Europas. Doch den großen Bruder aus dem Osten war man damit noch nicht los.

Anfangs war von Digitalisierung noch keine Spur: Nur rund die Hälfte aller Haushalte besaß damals überhaupt ein Telefon, selbst die Regierung verfügte kaum über internationale Leitungen. Angeblich war ein Nokia-Handy, das im Garten des Außenministeriums vergraben lag, lange Zeit der einzige Kontakt zur Außenwelt. Wie praktisch also, dass die Finnen den Esten Anfang der neunziger Jahre ihr altes analoges Telefonsystem verkaufen wollten. Die Esten lehnten ab und entwarfen stattdessen eines der modernsten digitalen Kommunikationssysteme Europas.

Heute bezahlen Esten ihre Parkgebühren per SMS, unterschreiben Verträge mit ihrem digitalen Ausweis, verfolgen die Schulnoten ihrer Kinder per App und wählen seit 2005 im Internet. Kurz: Die Digitalisierung Estlands boomt nicht nur, sie hat ein völlig neues Land entstehen lassen. Vieles davon kennen wir mittlerweile auch in Deutschland: Online-Banking nutzten 2016 laut Statista 28 Prozent der Bevölkerung, Steuererklärungen werden mit dem Elster-Programm ausgefüllt, Universitäten bieten Online-Kurse an und Bewerbungen per E-Mail sind Standard. Doch in Deutschland ist man sehr viel skeptischer gegenüber dem Sammeln und Speichern von Daten. Denn was den eigenen Rechner verlässt und mit anderen ausgetauscht wird, kann potenziell von Dritten kopiert oder ausspioniert werden. Was passiert aber, wenn alle digitalen Fäden wie in Estland bei der Regierung zusammenlaufen?

GERMAN ANGST

Anto Veldre sieht das eher gelassen. Der 55-Jährige arbeitet als IT-Experte bei der Staatlichen Estnischen Informationssicherheitsbehörde RIA und vertraut als Staatsdiener seiner Regierung. Kritik an der Digitalisierung gebe es weder aus der Bevölkerung noch von Institutionen, so Veldre. Für ihn, wie auch für viele andere Esten, würden die wirtschaftlichen Vorteile überwiegen: »Die estnische Geschichte weist eigentlich keine industrielle Phase auf. Unsere Gesellschaft ist direkt von der Agrargesellschaft zur postindustriellen Online-Gesellschaft durchgerauscht.«

Die Digitalisierung wurde ab den neunziger Jahren zum Rückgrat vieler estnischer Unternehmen wie Skype oder Hotmail, die heute von Millionen Menschen weltweit genutzt werden. Der Baltenstaat überschlug sich zudem mit Rekorden: So waren bereits 1997 im Zuge des Tiger-Leap-Programmes 97 Prozent aller estnischen Schulen mit dem Internet verbunden, 2000 gab es in Estland das erste Gesetz, das das Recht auf Internet regelt. Heute ist das Land nahezu flächendeckend mit kostenlosen Wi-Fi-Hotspots versorgt und in Hunderten von Bibliotheken, Postämtern und Dorfläden können die Esten online gehen.

2005 gab es die ersten Online-Landeswahlen in Estland und seit 2015 können auch Ausländer als e-Residents ein Bankkonto eröffnen, eine Steuererklärung abgeben und eine digitale Signatur beantragen. Die estnischen Sicherheitsstandards orientieren sich dabei auch an den anspruchsvollen Empfehlungen des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI).

Hierzulande hat jedoch die große Sensibilität gegenüber Datenschutz ihre Gründe, denn zwei deutsche Diktaturen hintereinander brachten Menschen immer wieder dazu, einander auszuhorchen und zu verraten. Die Esten litten ebenfalls unter der sowjetischen Überwachung, doch eine »Estonian Angst« vor zu viel Zentralisierung und Missbrauch von Daten gibt es heute offenbar nicht. Viel eher wird ganz im Sinne der Post-Privacy die Transparenz und der gleichberechtigte Zugriff auf Daten gelobt. So kann theoretisch jeder in einer Online-Datenbank einsehen, wie viele Steuern der Finanzminister zahlt, was die letzte ärztliche Diagnose vom Ex-Partner war oder ob der Nachbar vorbestraft ist. 2012 lobte der ehemalige Präsident Toomas Hendrik Ilves das System ausdrücklich gegenüber der britischen Zeitung The Guardian: »Ich fühle mich viel sicherer mit meinem digitalen Ausweis. Wenn jemand an meine Daten möchte, hinterlässt er eine Spur. Wenn meine Akte – die es sowieso über mich gäbe – aus Papier wäre, wüsste man nicht, wer sie sich angeschaut hat.« Das System ist bei den Esten beliebt, weil es zuverlässig, transparent und bequem war – bis zum Frühjahr 2007. ►

DENIAL OF SERVICE: EIN LAND GEHT OFFLINE

Alles begann damit, als das Sowjet-Denkmal »Bronzesoldat von Tallinn« in der estnischen Hauptstadt versetzt werden sollte. Dagegen regte sich Protest – vor allem in der russischstämmigen Bevölkerung des Landes, die etwa ein Viertel ausmacht. Die Beziehung zu Russland ist angespannt, denn die Esten haben der Führung in Moskau die sowjetische Besatzung bis heute nicht verziehen. Der Großteil der russischstämmigen Bevölkerung kam zudem ab Ende der fünfziger Jahre mit einem umstrittenen Umsiedlungsprogramm der UdSSR nach Estland. Viele von ihnen blieben nach dem Zerfall der Sowjetunion, saßen aber spätestens mit dem Beitritt Estlands zur EU im Jahr 2004 fest.

Sprachlich und kulturell sind heute vor allem Ältere isoliert, politisch sind viele ethnische Russen so genannte Nichtbürger*. Dies führte immer wieder zu Konflikten und einen Tag nach Abbau des umstrittenen Denkmals wurde das digitale Rückgrat des Landes durch eine Cyber-Attacke lahmgelegt. Schuld daran waren unzählige Denial-of-Service-Anfragen durch Bot-Netzwerke. Besonders betroffen waren das Parlament, der Staatspräsident sowie zahlreiche Ministerien, Banken und Medienhäuser, was zu Ausfällen und Umsatzeinbußen führte.

2008 wurde ein russischstämmiger Este verurteilt, ein Jahr später bekannte sich die Kreml-Jugendorganisation Naschi (etwa: »Die Unseren«) zu der Attacke. Der Fall ist bis heute nicht restlos aufgeklärt und sorgte für neue Verstimmungen zwischen Tallinn und Moskau. Im Alltag gingen sich Russen und Esten bald wieder aus dem Weg, doch noch im selben Jahr mobilisierte der estnische Staat eine Art digitale Cyber-Armee aus über hundert freiwilligen Experten, die nun dauerhaft bereit sind für die nächste Cyber-Attacke. Im Mai 2008 etablierte die NATO zudem ihr Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) in Tallinn, eine Art Denkfabrik für digitale Kriegsführung in Europa. Viele IT-Kaderschmieden, wie jene der Technischen Universität Tallinn oder des Eesti IT College, banden sich nach dem Angriff enger an das Militär und die staatliche Cyber Security. Mulmige Gefühle? Fehlen heute fast genauso wie früher die Telefonkabel in den Westen.

DIGITALE PIONIERE

Vielleicht ist es die geringe Bevölkerungszahl, die Mischung von Tradition und High-Tech, die kulturelle Orientierung nach Skandinavien oder das marktliberale Klima, das die Esten so kritiklos von der Digitalisierung* überzeugt. So schreiben die Hochglanzbroschüren, dass eine Steuererklärung in Estland mit rund fünf Minuten so lange wie ein Schnäppchenkauf auf Amazon dauert. Dies führte dazu, dass heute rund 95 Prozent der Esten ihre Steuererklärung einreichen und der Staat die Belastungen sogar senken konnte. Auch für ausländische Firmen ist Estland attraktiv, denn in nur 30 Minuten könne man ein Unternehmen anmelden – natürlich ein weiterer digitaler Rekord.

*NICHTBÜRGER

Russischstämmige Bürger stellen in allen drei baltischen Staaten eine große Minderheit dar. Wer sich nicht einbürgern lässt, wird ein so genannter Nicht-Bürger, der zwar anerkannt ist, aber beispielsweise nicht die Freizügigkeit der EU genießt. Ethnische Russen können in Estland auch nicht zum Präsident gewählt werden, selbst wenn sie die estnische Staatsbürgerschaft besitzen.

Einer der größten Haken der Digitalisierung bleibt vorerst die Abhängigkeit von der Privatwirtschaft. Denn trotz aller Spitzenleistungen kann die estnische Regierung die Kosten für die Digitalisierung bisher nicht alleine stemmen. Beispielsweise wird der obligatorische digitale Personalausweis von einer Privatfirma vertrieben. Für IT-Experten ist dies kein Widerspruch. Der estnische Staat nutzte schon in den neunziger Jahren die Expertise von Privatunternehmen, um eine flächendeckende digitale Infrastruktur zu schaffen. Heute setze man diese Kooperation fort und hoffe, so Ex-Präsident Ilves 2012, »diese auch in andere Länder exportieren zu können.«

Die Esten haben offenbar großes Vertrauen in den Mix aus gesellschaftlicher Transparenz, wirtschaftlichem Wettbewerb und staatlicher Kontrolle. Mit ihrer hochdigitalisierten Infra- und Wirtschaftsstruktur ist Estland heute Vorbild für viele EU-Länder. Hier versucht man weiterhin, Verwaltungen und politische Strukturen dem 21. Jahrhundert anzupassen und Bürger von deren Vorteilen zu überzeugen. Aber wer weiß, vielleicht kommt die nächste Revolution ja aus Estland. •

*DIGITALISIERUNG

Profitiert haben von der Digitalisierung vor allem Frauen. Laut Anto Veldre zeigten Estinnen aus allen sozialen Schichten seit 2001 besonders hohe Akzeptanz im Umgang mit Hard- und Software im Alltag, während Männer zu Beginn der Digitalisierung nur Computer benutzten, wenn sie vorher eine Universität oder Fachhochschule besucht hatten. Der Frauenanteil an den IT-Studiengängen Estlands lag 2012 laut Eurostat mit rund 22,3 Prozent über dem EU-Durchschnitt von circa 16, 8 Prozent und damit neben Bulgarien, Portugal und Finnland in den Top Vier der EU. Heute rollen Frauen als Beraterinnen oder Unternehmerinnen das digitale Feld professionell auf - die einen testen in Tallinn Apps für internationale Kunden, die anderen melken auf dem Land die Kühe per selbstprogrammiertem Algorithmus.

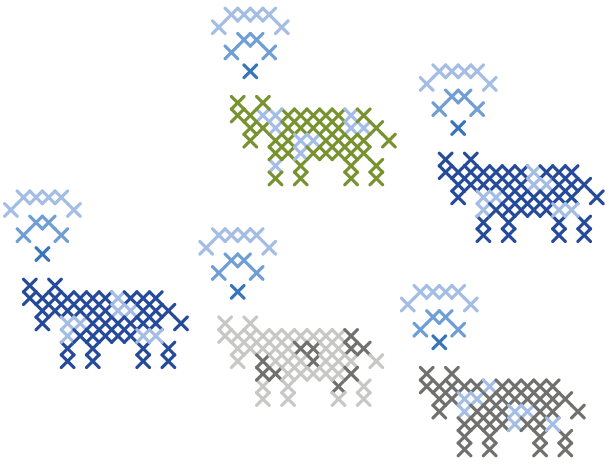
»BIG BROTHER UND SEINE KLEINEN SCHWESTERN«

Die Esten sind mächtig stolz auf ihre Digitalisierung. Daneben setzen sie auf viel Bildung vom Grundschüler bis zur Oma, sodass alle sicher online unterwegs sind. Doch wie sieht es aus in Sachen Datenschutz und kommerzieller Schnüffelei? IT-Spezialist Anto Veldre kennt das System so gut, dass er sogar weiß, wie man es umgeht.

INTERVIEW SYLVIA LUNDSCHIEN
ILLUSTRATION NATASCHA KORNILOWA

KATER DEMOS *In Deutschland herrscht oft Skepsis gegenüber der Digitalisierung von Behörden – unter anderem auch aufgrund der Erfahrungen mit staatlicher Überwachung in der DDR. Hatten die Esten ähnliche Befürchtungen nach Ende der Sowjetzeit, die die digitale Entwicklung des Landes beeinflusst haben?*

ANTO VELDRE Einer der Hauptunterschiede ist aus meiner Sicht, dass sich in Deutschland die Deutschen gegenseitig bespitzelt haben. In Estland waren es immer andere, die uns ausspionierten. Glauben Sie es oder nicht: Wir vertrauen unserem Staat und unserer Regierung. Die Zeit seit der Unabhängigkeit [seit 1991, KD] ist zu kurz gewesen, als dass die Regierung sich durch bestimmte Aktionen kompromittiert hätte. Das bedeutet aber nicht, dass wir naiv sind. Besonders die ältere Generation weiß gut genug, welche Themen nicht am Telefon besprochen oder am Computer kommuniziert werden. ▸



KD ***Heute speichern mit dem Internet verbundene Geräte wie Smartphones persönliche Daten oder tracken meinen Aufenthaltsort. Wird dies in Estland diskutiert?***

AV Das hängt vom Alter und der sozialen Gruppe ab. Im estnischen Schulunterricht wird besprochen, wie man sich schützt: Zum Beispiel, dass man intime Fotos oder Urlaubspläne nicht veröffentlicht.

Was mich betrifft – ich bin in ein paar sozialen Netzwerken aktiv, aber nur solchen, wo man anonym bleibt. Einen Facebook-Account hatte ich nie und werde ich mir auch nicht zulegen. Meine Business-E-Mails lese ich nie auf meinem Smartphone, obwohl Google theoretisch auch bei mir einige E-Mails analysieren oder Familienangehörige identifizieren könnte. Back-ups lade ich nie in eine Cloud, sondern habe sie immer in der Nähe meines Zuhauses. Wenn ich ein wirklich wichtiges Meeting habe, dann stelle ich mein Smartphone aus, noch bevor ich mich auf dem Weg zum Treffpunkt mache.

Wenn ich einen Telefonanruf zu einem sensiblen Thema erhalte, denke ich als Erstes: In welcher Funkzelle bin ich gerade und welcher Mast überträgt meine Daten? Jeder muss informierte Entscheidungen treffen, um sowohl den Staat als »Big Brother« als auch die »Little Sisters« wie große IT-Unternehmen im Blick haben.

KD ***Die ausländische Berichterstattung jubelt regelmäßig über Estlands digitale Infrastruktur. Muss man aber Nachteile befürchten, wenn man offline bleiben will?***

ANTO VELDRE

Anto Veldre war sechs Jahre lang Mitglied der Cyberabwehr für die estnische Sicherheitsorganisation CERT-EE und arbeitet heute als Spezialist für die Staatliche Estnische Informationssicherheitsbehörde (RIA). Zuvor war der 55-Jährige als Sicherheitsverantwortlicher im Finanzsektor und als Technikvorstand für den Tallinner Flughafen tätig. Veldres Schwerpunkte sind Radiotechnik und IT, er unterrichtet ebenfalls Informationssicherheit.

AV Ich glaube, so eine Entscheidung kann schwierig werden. Wenn ich jedoch selbst im Rentenalter bin, werde ich wohl einer der lautesten Verfechter dieses Szenarios. Für mich ist es ein Grundrecht, zu entscheiden, ob ich für meine Regierung digital verfügbar bin oder nicht. Allerdings sollte dieses Recht nicht dazu führen, dass man sich vor dem Staat versteckt. Wir hatten in Estland den Fall, dass das offizielle Benachrichtigungssystem der Gerichte mit den E-Mails aller Bürger verbunden wurde. Einige Leute haben sich dann bewusst bei den Behörden abgemeldet, um so einer Vorladung zu entgehen.

KD ***Wie viel Souveränität haben die Esten über ihre persönlichen Daten?***

AV Aus persönlicher Sicht glaube ich an Datenfreiheit – im Rahmen der erlaubten Gesetze. Ich scheue mich nicht davor, meine Steuererklärung zu veröffentlichen, unter der Bedingung, dass die Steuererklärungen aller anderen auch zugänglich sind. Allerdings sollte man bedenken, dass lokale Überlegungen im globalisierten Informationsraum nicht mehr so wichtig sind. Ich denke zum Beispiel daran, welchen Vorteil chinesische Unternehmen hätten, wenn alle estnischen Steuerdaten online wären.

In der Praxis definiert die estnische Gesetzgebung, über welche Daten die Bürger keine Kontrolle haben. Der Staat verfügt über bestimmte Daten, auch gegen den Bürgerwillen. Alles andere ist verhandelbar, spätestens mit Hilfe der zentralen und ziemlich mächtigen Datenschutzbehörde.

Wenn eine Verbindung zu estnischen Staatsdatenbanken aufgebaut wird, hinterlässt jeder Zugriff eine verschlüsselte Spur. Für bestimmte Datenbanken gibt es schon jetzt eine Kontrolle: Estnische Bürger können online einsehen, wer ihre Daten abgefragt oder angeschaut hat. Estland möchte diese Möglichkeit, in nahezu jede staatliche Datenbank Einblick zu erhalten, weiter ausbauen.

KD ***Gibt es überhaupt jemals Bedenken gegenüber dem digitalen Fortschritt in Estland?***

AV Es wurde sehr darauf geachtet, keine soziale Ungleichheit entstehen zu lassen. Ganz zu Beginn der Digitalisierung haben Telekommunikations-Anbieter und Banken zusammen mit der Regierung Schulungen für ältere Menschen durchgeführt. Dabei ging es um Computerkenntnisse und den Umgang mit dem digitalen estnischen Personalausweis.

Durch diese ausgewogenen Schritte gibt es keine organisierte Gegenbewegung. In Tallinn sehe ich manchmal Graffitis wie »Chipkarte = 666«, aber das ist selten. Eine unsere politischen Parteien hat wiederum mit ihren russischen Partnern angebandelt, indem sie behaupteten, Online-Wahlen seien »direkt aus der Hölle«, aber diese Initiative endete beim Europäischen Gerichtshof.

Daneben wird vor Online-Wahlen auch manchmal das so genannte Oma-Hacking diskutiert. Dabei werden ältere Wähler gezielt angesprochen, um mit ihrem Personalausweis ihre Stimme einer bestimmten Partei zu geben. Aber das ist eher ein soziokulturelles Phänomen als ein technisches Problem.

Denkbar wäre auch, dass Kriminelle über estnische Personalausweise verschlüsselte Dokumente über unsichere Kanäle senden und empfangen können und der Staat keine Möglichkeit hat, diese Nachrichten zu knacken. Aber das war bisher kein Thema.

KD ***Gibt es über die Generationen hinweg Unterschiede, wie die Esten mit Datensouveränität und digitalem Analphabetismus umgehen?***

AV Aus meiner Sicht ist diese Lücke längst geschlossen. Der Höhepunkt war 2001 erreicht: Jede Frau, die 2001 jünger als 40 Jahre war, hat wahrscheinlich das erwähnte Computer- und Ausweis-Training absolviert und surft jetzt ganz selbstverständlich im Internet. Schwieriger war es, die Männer online zu bekommen: Jene, die 2001 älter als 35 Jahre waren, sind nur ins Internet gegangen, wenn sie vorher eine Universität oder Fachhochschule besucht haben.

Esten, die jetzt älter als 60 Jahre sind, kommen gut klar – sie lesen online Zeitung, zahlen online ihre Rechnungen, sind aber kaum in sozialen Netzwerken aktiv. Ausnahmen gibt es – zum Beispiel hat meine Mutter bereits 1959 im Computerzentrum ihrer Universität programmiert und ist immer noch sehr aktiv im Internet unterwegs.

KD Vielen Dank für das Gespräch. •

Seit **Sylvia Lundschien** in einem Seminar erfahren hat, wie einfach das Auslesen von Metadaten ist und dass man fast jede Adresse beim Einwohnermeldeamt abfragen kann, macht sie sich um ihren Datenschutz noch mehr Gedanken. Wahrscheinlich ist das aber irgendwie auch typisch deutsch, wie sie in der Recherche über die estnische Digitalisierung gelernt hat. Sylvia googelt sich manchmal aus beruflichen Gründen selbst, obwohl sie ja eigentlich nichts zu verbergen hat.

13

Lichtjahre – von der Erde liegt der Planet »Kapteyns Stern« auf dem erdähnliches Leben möglich wäre

Quelle: spiegel.de

1071

operationelle Satelliten befinden sich im Orbit der Erde (die Hälfte davon von den USA ausgesendet)

Quelle: universetoday.com

374

Drohnen zur optischen Aufklärung besitzt die Bundeswehr

Quelle: de.wikipedia.org

3000

Tote durch US-Drohnen-angriffe in der ersten Amtszeit von Barack Obama

Quelle: german.irib.ir

84.372 EUR

Euro ist der Spitzen-Jahressatz, den ein Astronaut der European Space Agency verdient

Quelle: universetoday.com

2020

ist das Jahr, in dem ein Big Data Satellit für besseren Umweltschutz die Biomasse von Regenwäldern messen soll

Quelle: wired.de

5000

schiffsbrüchige Flüchtlinge rettete Seawatch 2015 mit Hilfe von Satelliten-Telefonen

Quelle: sea-watch.org

2025

will Elon Musks Unternehmen SpaceX die ersten Menschen auf den Mars fliegen

Quelle: de.wikipedia.org

TEXT HEIDI MARLEEN KUHLMANN
ILLUSTRATION NATASCHA KORNILOWA

2022

ist das Jahr, in dem die ersten BND-Spionage-Satelliten ihren Betrieb aufnehmen sollen
Quelle: sueddeutsche.de

90 cm

Mindestgröße von Objekten, die vier Google-Drohnen aus dem All erspähen können
Quelle: welt.de

3,7 MIO

Millionen US-Amerikaner wurden laut einer 1992er Studie potenziell bereits einmal von Außerirdischen entführt
Quelle: de.wikipedia.org

1

staatliche UFO-Erforschungs-Behörde in Europa: GEIPAN in Frankreich
Quelle: cnes-geipan.fr

1179

UFO-Sichtungen – in den USA im Juni 2015

6500

Mitarbeiter hat der BND
Quelle: berliner-zeitung.de

75–80 %

der Amerikaner glauben, dass ihre Regierung Wissen über Außerirdische zurückhält

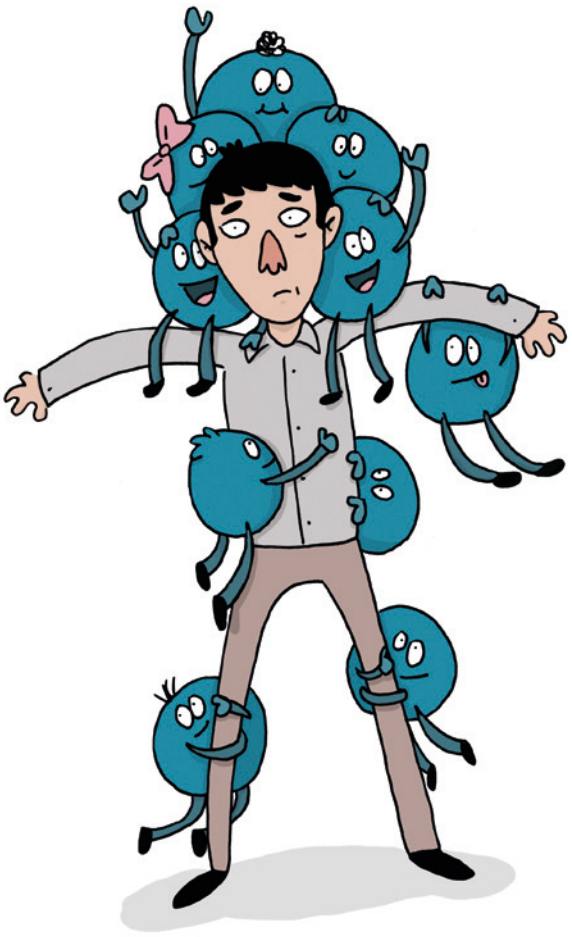
PAYBACK TIME!

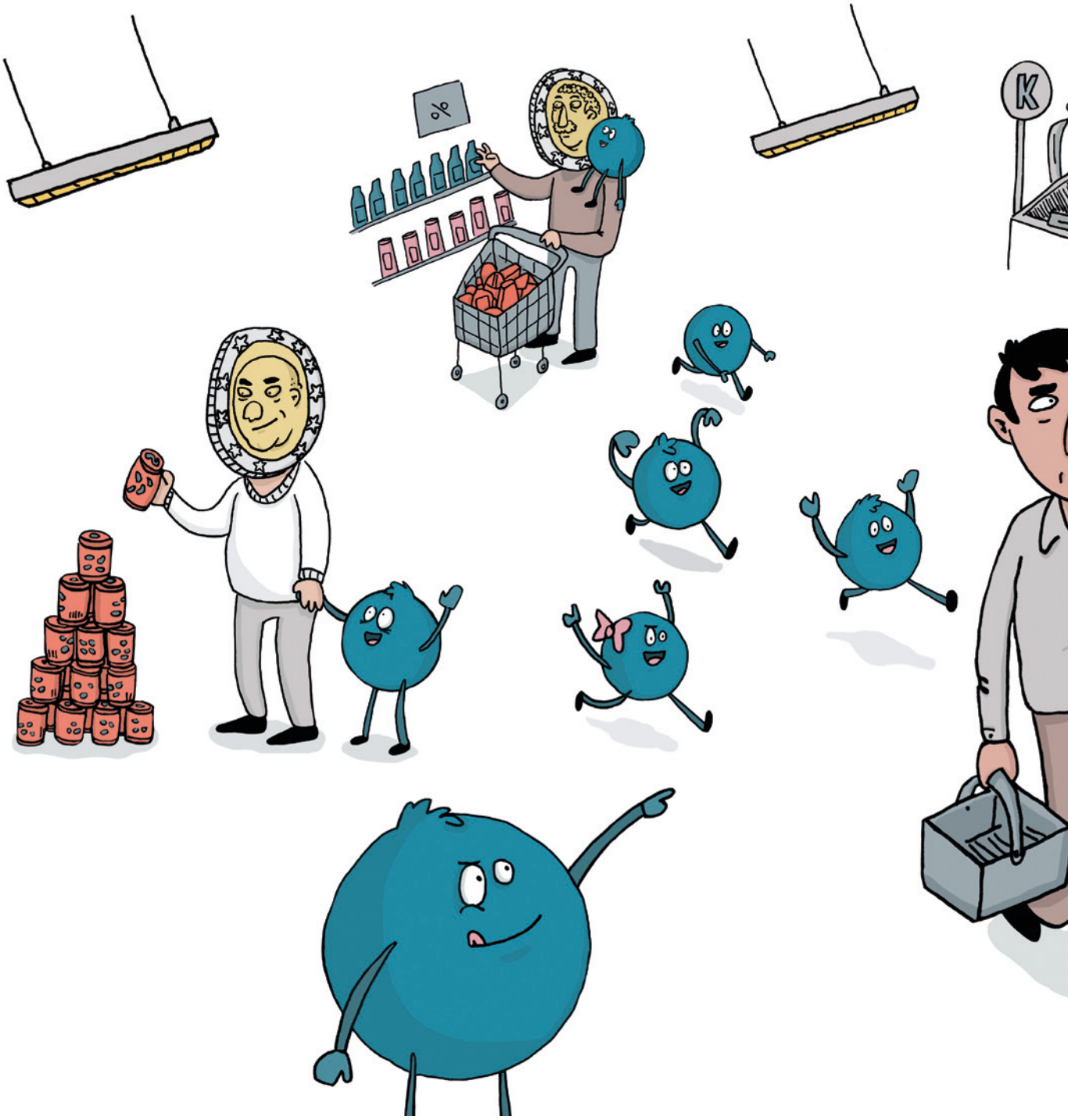
Supermärkte verfolgen ihre Kunden auf Schritt und Tritt, um ihnen die besten Angebote machen zu können. Aber haben sie dabei wirklich nur das Beste für den Kunden im Sinn?

TEXT VIKTOR MARINOV
ILLUSTRATION STEVE M. CLEMENTS

Haben Sie eine Payback-Karte?« Diese Frage wird in Deutschland täglich millionenfach gestellt. Nach Angaben von Payback gibt es bundesweit 29 Millionen aktive Kartenbesitzer. Weitere 20 Millionen haben eine Deutschlandcard im Portemonnaie. Der Kunde bekommt einen mageren Rabatt, der Supermarkt erhält jede Menge personenbezogene Daten. Mit ihnen verfolgen Unternehmen heute ein ökonomisches Ideal, das seit Ewigkeiten als unerreichbar gilt.

Ökonomen suchen nach dem perfekten Preis für jeden. Und das ist aus der Sicht eines Unternehmens der höchste Preis, den der einzelne Kunde zu zahlen bereit ist. Diese Zahlungsbereitschaft wird durch das Erkennen individueller Eigenschaften des Kunden bestimmt. »Jedem seinen Preis«, so kann man dieses ökonomische Ideal zusammenfassen. Es heißt »Total Price Discrimination« auf Englisch, »Preisdifferenzierung ersten Grades« auf Deutsch. Neu ist diese Idee nicht: Von Total Price Discrimination sprach der englische Ökonom Arthur Cecil Pigou bereits in den zwanziger Jahren des vergangenen Jahrhunderts. Sein Werk »The Economics of Welfare« gehört noch immer zur Standardlektüre in den Wirtschaftswissenschaften. Galt Pigous heiliger Gral fast hundert Jahre lang als unerreichbar, ist man ihm heute näher als je zuvor. Der Dank dafür geht an die globale und umfassende Sammlung von personenbezogenen Daten. Mit ihr können Unternehmen Antworten auf die Fragen finden, die zum perfekten Preis führen: Wo, wann, wie oft und wieviel kauft der Einzelne ein? Zu welchen Produkten greift er am häufigsten, zu welchen nur bei Rabatten? Wie hoch sollten diese Rabatte sein, damit er etwas kauft? Supermärkte versuchen diese Fragen mit Kundenkarten zu beantworten. Seit Jahren sammeln sie so Daten über ihre Kunden. Das Stück Plastik wurde allerdings nicht über Nacht der Schlüssel zum alten Wirtschaftsrätsel. ►





JE MEHR DATEN, DESTO MEHR PERSONALISIERUNG

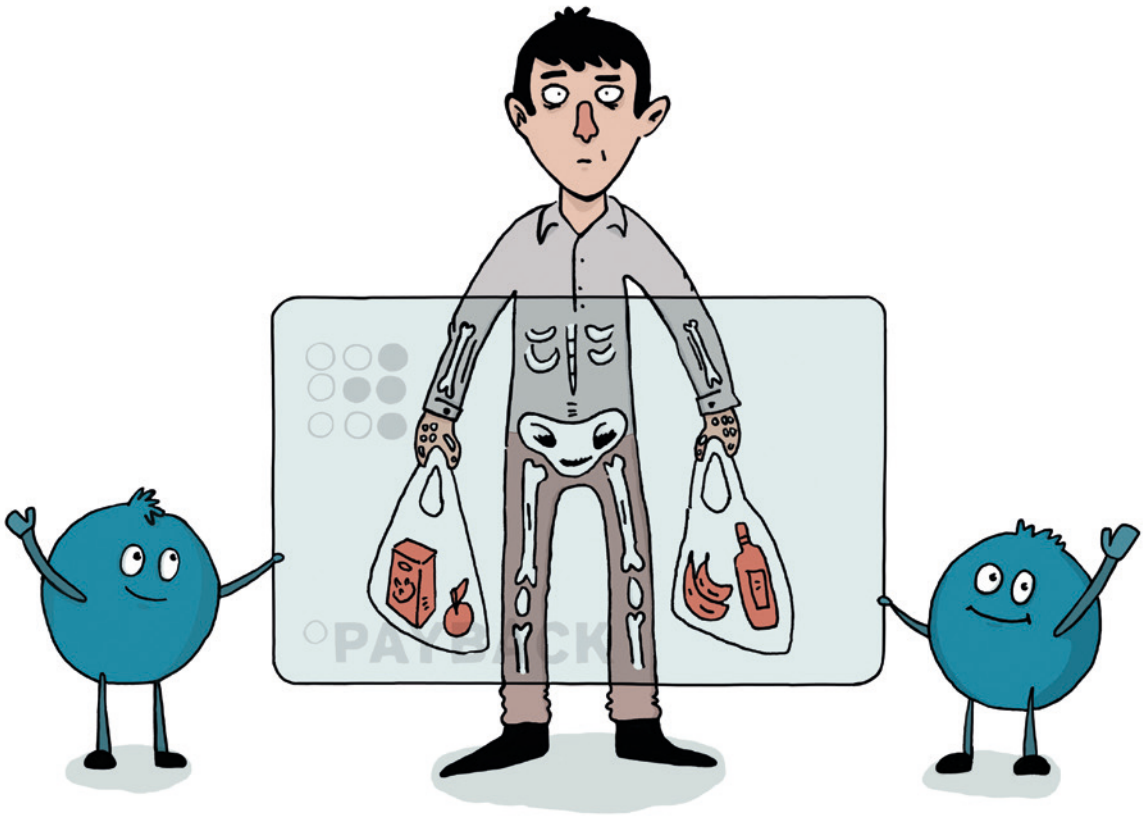
Am Anfang waren Kundenkarten ein Instrument der Kundenbindung. Sie sollten Treue erzeugen, so Karen Gedenk, Professorin für Marketing und Pricing an der Universität Hamburg. Doch die Effekte seien marginal gewesen. Einen erkennbaren Zusammenhang zwischen Ausgaben für den Einkauf und den Besitz einer Kundenkarte war kaum messbar. Das gescheiterte Treueinstrument schlug trotzdem Wellen und wurde unter anderem auch in Deutschland extrem beliebt. Für ein paar Bonuspunkte verkaufen täglich Millionen Deutsche ihre Daten: Sie lassen sich freiwillig überwachen. Dadurch kann der Traum der perfekten Preisdifferenzierung erfüllt, die maximale Zahlungsbereitschaft der Konsumenten ausgeschöpft werden. Je mehr Daten man hat, desto mehr kann man personalisieren. Durch individuelle Profilbildung gelang es der US-Supermarktkette Tesco schon 2012 herauszufinden, dass eine Minder-

jährige aus Minnesota schwanger war. Nicht einmal ihr eigener Vater wusste davon, wie das US-Wirtschaftsmagazin »Forbes« damals berichtete. Was war der Trick? Man hatte Datenanalysten gebeten aus der Masse an Daten Muster zu erkennen: So verrieten diese, dass in den ersten zwanzig Wochen einer Schwangerschaft Frauen anfingen besonders häufig Nahrungsergänzungsmittel wie Kalzium, Magnesium oder Zink zu kaufen. Genauso steigt messbar in der Schwangerschaft der Verbrauch von Bodylotion.

Dass ausgerechnet Supermärkte vor Ort und nicht etwa Online-Händler den Trend zu personalisierten Preisen vorantreiben, hat Gründe: Die Daten sind eben nicht alles. Einer dieser ist die schlechte Erfahrung, die Online-Händler schon sehr früh gemacht haben. Als Amazon im Jahr 2000 mit personalisierten Preisen experimentierte, flog der Test schnell auf. Mittels Cookies erstellte das Unternehmen persönliche Profile für Kunden und variierte die Preise für DVDs nach individueller Kaufkraft auf Basis vorangegangener Einkäufe. Kunden beschwerten sich massiv, die Medien berichteten umfassend über den Vorfall. Amazon ruderte zurück und hat sich seitdem von personalisierten Preisen ferngehalten, so zumindest der Stand aktueller Untersuchungen. So wird immer wieder überprüft, ob personalisierte Preise im Online-Handel eingesetzt werden. Der Fall Amazon hat gezeigt, was allen Unternehmen klar wurde: Bemerkt ein Kunde, dass er zum gleichen Zeitpunkt am gleichen Ort mehr für ein Produkt bezahlt als sein Nachbar, gibt es Ärger. Und das ist ein weiterer Grund, warum personalisierte Preise »offline« besser funktionieren – im Netz ist der Vergleich mit einigen Klicks schnell gezogen, unfaire Preise fallen schneller auf. Das gilt bei teuren Produkten umso mehr. Denn je teurer eine Ware, desto mehr Zeit investiert der Kunde in den Preisvergleich. Dagegen eignen sich kleine spontane Einkäufe besser für den Einsatz personalisierter Preise.

ERFOLGSKONZEPT PERSONAL PRICING IM SUPERMARKT – DAS GESCHENKEMÄRCHEN

Und wie funktioniert das nun im Supermarkt? Ganz einfach: Die Preisdiskriminierung von heute heißt »Angebot«. Mit diesem Narrativ wird von Exklusivität persönlicher Angebote gesprochen, zuweilen werden sie als Geschenke vermarktet – die mag schließlich jeder. Die Supermarktkette Migros macht es in der Schweiz vor, das Berliner Unternehmen SO1 testet das Konzept auch seit 2014 in den Filialen seiner Partner – darunter mindestens vier große deutsche Handelsketten. Und das funktioniert so: Der Kunde lässt seine Karte am Eingang einscannen und bekommt persönlich für ihn berechnete Angebote. Diese können ausgedruckt oder digital direkt am Handy übermittelt werden. Individuelle Vergünstigungen machen allerdings wirtschaftlich für einen Supermarkt erst dann Sinn, wenn Kunden das nun billigere Produkt sonst nicht gekauft hätten. Wenn jemand ohnehin viel Schokolade kauft, bekommt er dafür also keinen Rabatt. Vielleicht aber für Produkte, die zu Schokolade passen und die er sonst nicht kaufen würde. Berechnet wird die Rabatthöhe durch einen Algorithmus. Er soll den höchstmöglichen Preis ermitteln, bei dem der Kunde zuschlägt. Bereits drei größere Warenkörbe des Konsumenten reichen So1 aus, um die Kaufwahrscheinlichkeiten gut vorhersagen zu können, so der Mitgründer des Unternehmens Raimund Bau in einem Interview mit der *Welt*. 2014 war zunächst nur Kaiser's Tengelmann dabei, seitdem sind nach eigenen Angaben des Unternehmens Penny, Netto und die Hamburger ►

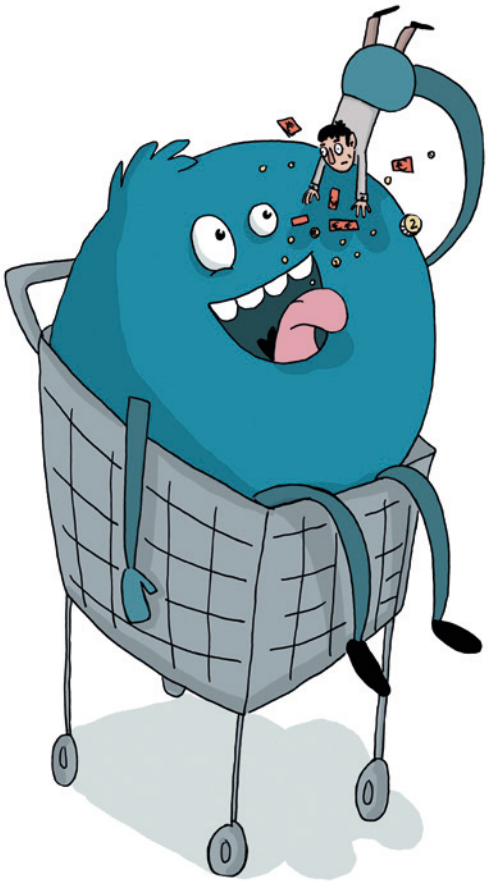


Drogeriekette Budnikowsky dazu gekommen. Es dürfte sich inzwischen um Hunderte von Filialen handeln, in denen das Personalisierungssystem von Sol eingesetzt wird. Durch den Anschein von Vergünstigungen löst Sol das größte Problem aus Sicht der Supermärkte: Der Kunde soll sich auf keinen Fall ungerecht behandelt fühlen.

Den Vorsprung seines Konzepts gegenüber dem Online-Handel betont Sol-Inhaber Bau auch gerne selbst: Online gebe es zwar auch Preisdifferenzierung, diese sei jedoch von »sehr einfachen Heuristiken gelenkt«. Diese Preismodelle seien längst gesellschaftlich akzeptiert. Dazu gehören zum Beispiel dynamische Preise, die gibt es etwa bei Fluggesellschaften. Je voller das Flugzeug, desto mehr zahlt der Kunde. Hier rechnet die Firma anhand unterschiedlicher Faktoren einen Preis aus, der sich an der Nachfrage und den Betriebskosten orientiert. Aber die individuellen Eigenschaften der Kunden spielen keine Rolle. Bei Migros, dem schweizerischen Vorreiter im Einsatz personalisierter Preise, bestreitet man eine individuelle Profilbildung. Es gehe um Gruppen von Kunden anstatt um Einzelne. Solche Preisdifferenzierung erleben wir auch im Alltag, etwa wenn Studenten oder Rentner an der Theaterkasse weniger zahlen. Das sei ein legitimer Vorgang, den wir doch alle kennen würden, so die Botschaft des Unternehmens. Die Kundschaft des Supermarkts sei jedoch mittlerweile in 154.000 »Segmente« aufgeteilt, berichtete die *Neue Zürcher Zeitung* Ende letzten Jahres. Umgerechnet sind das 18 Kunden pro Segment. Je mehr man diese Art der Preisdifferenzierung perfektioniert, desto näher kommt man dem Ideal des Personal Pricing.

VERSTOSS GEGEN DAS GRUNDGESETZ?

In Deutschland verfolgt der Sachverständigenrat für Verbraucherfragen (SVRV) die Entwicklung seit Jahren. Die individualisierte Preisbildung, wie von Sol eingesetzt, habe für Verbraucher theoretisch den Vorteil, dass für einzelne Kunden manche Produkte billiger werden, heißt es in einer wissenschaftlichen Analyse der SVRV. Die Nachteile überwögen aber deutlich, so Helga Zander-Hayat, Leiterin im



Viktor Marinov ist für sein Studium nach Deutschland gekommen und aus Lust auf die Sprache und für den Qualitätsjournalismus hier geblieben. Er schreibt derzeit seine Masterarbeit, freiberuflich für eine kleine Lokalzeitung und neuerdings glücklicherweise für Kater Demos. An langen einsamen Abenden hat er tierisch Angst vor dem Klimawandel, Überwachung und gierigen Männern mit zu viel Macht.

Markt-Bereich des SVRV: »Die Kehrseite der Medaille ist doch, dass Einzelne aufgrund ihrer Profilbildung bessere Preise bekommen, andere aber aus dem Markt gedrängt werden können.« Zwei Gruppen seien besonders gefährdet, von den Vorteilen der personalisierten Preise nicht profitieren zu können. Das seien an erster Stelle Konsumenten mit sehr geringer Kaufkraft. »Sie sind für Unternehmen nicht interessant«, so Zander-Hayat. Die zweite Gruppe bestehe aus Menschen, die sich gezielt vor dem »datensüchtigen Blick« der Unternehmen verbergen. Sie geben ihre Daten an Dritte nicht weiter und besitzen dementsprechend keine Kundenkarte. »So sind diese zwei Gruppen praktisch aus dem Markt ausgeschlossen.«

Der SVRV fordert mehr Transparenz – sowohl gegenüber Verbrauchern als auch bei den Algorithmen. »Personalisierte Preise werden als solche nicht gekennzeichnet. Dabei sollten sie ersichtlich sein, sonst kann der Einzelne nichts dagegen tun. Bei den Kriterien der Algorithmen sind der Phantasie keine Grenzen gesetzt. Es könnten die genutzten Geräte sein, aber auch die Religion, Geschlecht oder die sexuelle Orientierung«, so Zander-Hayat. Das wäre nicht minder als ein direkter Verstoß gegen das allgemeine Diskriminierungsverbot des Grundgesetzes.

Es liegt auf der Hand, dass personenbezogene Daten in Deutschland mit Kundenkarten im großen Stil erhoben werden. Sie werden zur individuellen Profilbildung eingesetzt und können zur Diskriminierung führen. Die naheliegende Lösung wäre, keine persönlichen Daten preiszugeben. Man muss also kreativ werden – Warum nicht etwa die Kundenkarte alle paar Wochen mit jemanden tauschen? Wenn mal der Mitbewohner, mal ein Elternteil und mal der ältere Herr von gegenüber dieselbe Karte nutzt, kann auch der beste Algorithmus mit dem daraus entstandenen Profil nichts anfangen. So verhindern wir nicht nur personalisierte Preise, sondern haben auch einen rebellischen Grund mehr, uns mit Freunden zu treffen – zum wöchentlichen Kartentausch! Payback time! •

ONLINE MARKETING: THE GOOD, THE BAD, THE UGLY

Werbung im Internet ist Fluch und Segen. Kunden bekommen inzwischen mehr von dem zu sehen, was sie eigentlich interessiert. Damit gehen aber auch datenschutzrelevante Probleme einher.

TEXT JOHANNES HEIM
ILLUSTRATION HEIDRUN KLEINGRIES

Disclaimer: Online-Marketing ist mein Job. Dadurch kann ich aus Erfahrung über das Thema berichten, bin aber sicherlich auch etwas voreingenommen. Beim Lesen möge man das bitte im Hinterkopf behalten.

WERBEEFFIZIENZ – DAMALS UND HEUTE

Vor den glorreichen Tagen des Internets wurde der Erfolg von Werbung mit Umfragen zur Bekanntheit derselben gemessen. Jeder konnte auch im Alltag feststellen, wie viele Mitmenschen auf einmal die Exquisa-Melodie summten oder das Zott-Sahnejoghurt-Weekend-Geschmack-Lied sangen. Dank des Internets kam zum klassischen dann das Online-Marketing dazu: Bannerwerbung, Google-Anzeigen und Rubriken wie »Kunden kauften auch« auf Amazon bereicherten das Repertoire der Werbemaßnahmen. Nun konnte man in Echtzeit feststellen, wie gut eine Kampagne oder ein bestimmtes Produkt funktionierten. Und das mit statistisch belegbaren Ergebnissen – dank Überwachung der Nutzer.

WERBEÜBERWACHUNG

Es wäre früher aufwendig und absurd gewesen, hinter jedes Plakat jemanden zu stellen, der beobachtet, wer das Plakat beobachtet, um festzustellen, wie erfolgreich eine Plakatierung ist. Im Endeffekt ist es jedoch genauso bei der Online-Werbung, nur eben in digitaler Form. Dank Pixeln und Cookies kann man heute leicht feststellen, wie ▸

viele Leute eine Werbung sehen, wie viele das Produkt dadurch anklicken und wie viele es schlussendlich kaufen. Und schon hat man bestimmt, an welcher Stelle man sein Werbebudget am besten investiert. Darunter leidet jedoch auch die Privatsphäre. Denn nur im besten Fall sind dies anonyme Daten. Häufig speichert eine Firma auch ab, bei welchem Kunden was besser funktioniert, so dass man bei einem erneuten Webseitenbesuch dem Kunden eine passende, persönliche An- und Bildsprache zeigt. Bei dieser Form der Nutzer-Überwachung ist nicht alles einfach abzulehnen und zu verdammen. Die Grenze zwischen problematisch und heilsbringend ist aber fließend und schwer zu erkennen.

TRICK 17

Was geschieht-, wenn man geneigt ist, einen Kauf zu tätigen und man entscheidet sich während des Kaufprozesses gegen das Produkt? Kurze Zeit später bekommt man gegebenenfalls eine E-Mail, dass es ein technisches Problem beim Bestellen gegeben hätte, was der Webseitenbetreiber sehr bedauert. Zur Wiedergutmachung erhält man kurz darauf einen Gutschein. Aber man hat doch ganz bewusst abgebrochen, wundert man sich. Das weiß der Web-Shop auch. Hat man aber bereits seine E-Mail-Adresse eingegeben, obwohl man kurz darauf den Kauf abbricht, kann diese vom Webseitenbetreiber per Script im Code der Webseite ausgelesen und eine sogenannte Remarketing-E-Mail an den potentiellen Kunden abgesetzt werden.

Angespornt von dem vermeintlich versehentlich zugesendeten Gutschein, wird der Einkauf dann häufig doch noch getätigt. Das ist doch sicher verboten, könnte man jetzt denken. In Deutschland ist das tatsächlich so. Man erhält im Endeffekt ungefragt Werbung, auch wenn die Betreiber dieser Rückholaktionen eine Menge juristische Kniffe anwenden, damit sie nicht gleich abgemahnt werden. Will man sich aber als genervter Verbraucher wehren, so hat man zumindest hierzulande gute Chancen. Denn im Gegensatz zu beispielsweise den USA ist in Deutschland schon das Erhalten einer E-Mail ohne die ausdrückliche Erlaubnis des Empfängers unerlaubter Wettbewerb und damit leicht straf- und abmahnbar. Bereits das Speichern von Daten, ohne dass sie für irgendetwas verwendet werden, ist laut Telemediengesetz strafbar, wenn keine Einwilligung des Nutzers vorliegt. Daher muss man auch überall irgendwelche AGBs annehmen, bevor man etwas online kauft oder auch nur einen Dienst wie Facebook nutzen möchte – was man viel zu oft ohne Nachdenken tut.

WE NEED TO GO DEEPER

Wer hat sich nicht schon mal online kurz vor Abschluss des Kaufs gegen einen Schuh entschieden, nur um dann von eben jenem Kleidungsstück über viele Webseiten hinweg innerhalb eines Werbebanners verfolgt zu werden? Denn von findigen Marketern betreute Webseiten merken sich per Werbepixel, welchen Schuh oder welches Katzenfutter jemand sich anschaute, und versuchen dann durch sogenanntes »Retargeting«, den eigentlich willigen Käufer durch wiederholtes Zeigen des begehrten Objektes zur nachträglichen Kaufentscheidung zu bewegen. Kauft man, so teilt die Webseite dem Pixel mit, dass ein weiteres Ausspielen der Werbung an diese Person nicht mehr nötig ist.

Nun hat sich jeder schon mal über nervige Werbeblöcke im Fernsehen aufgeregt. Hier sehe ich vor allem einen Vorteil bei der Online-Werbung, auch wenn diese auf mein digitales Verhalten reagiert. In der Regel erhalte ich Angebote von Sachen, die mich interessieren. Ich will nicht ständig Auto- oder Bierwerbung anschauen, sondern erhalte durchaus gerne Anzeigen, die meinem Interesse entsprechen. Und solange eine Firma meine Daten nur benutzt, um mich besser bewerben zu können, kann ich mit etwas Datenkrakentum gut leben. Lieber werde ich von einem hübschen Schuh verfolgt als von Bierflaschen.

FACEBOOK ALLWISSEND

Wenn man aber, wie so oft, die Schattenseiten des Online-Marketings erlebt, dann fragt man sich schon, wie weit Werbung im Netz eigentlich gehen darf. Man bucht einen Flug zum Ziel X mit der Fluggesellschaft Y und bekommt kurz darauf auf Facebook weitere Ziele angeboten, die Y so ansteuert. Welches »Nein«-Häkchen zur Verwendung meiner Daten habe ich beim Bordkartenkauf da denn nicht gesetzt? Manchmal wird so ein übergreifendes Marketing mit technischen Tricks auf Seiten des ursprünglich werbenden Unternehmens vorgenommen. Manchmal aber, und gerade im Fall von Facebook, laden Unternehmen gesammelte E-Mail-Adressen ihrer Kunden in ihr Facebook-Adverts-Konto – gerne auch ohne Wissen des Kunden. Damit zielen sie dann die Werbung treffgenau auf diese User, sobald sich die zum Anmelden bei Facebook genutzte E-Mail mit der von den Werbenden hochgeladenen E-Mail deckt.

WIN-WIN-WIN-SITUATION?

Facebook greift dabei die für sich wichtigen Informationen über seine Nutzer ab, während die Firmen so sehr gezielt werben können. Handelt es sich dabei dann sogar um eine Win-Win-Win-Situation? Immerhin profitieren davon

*ZÄHLPIXEL

Sogenannte Tracking-Pixel oder Zähl-Pixel sind kleine Codezeilen in Webseiten und Newslettern, die zur Erhebung von statistischen Daten genutzt werden. Damit werden sowohl banalere Zahlen wie die Besuchermengen auf Homepages erhoben, aber auch speziellere Informationen wie von Kunden angesehene Produkte in Webshops übermittelt.

Facebook und die werbende Firma und der Kunde eventuell auch? Aber vielleicht will ich die Hoheit über meine Daten haben und finde es grenzwertig, auf welche Art und Weise mit meinen Informationen umgegangen wird? Oftmals geht es bei dieser Form der Überwachung ja nicht darum, dass sie geschieht, sondern wie sie geschieht. Dass ich bestimmte Informationen über mich freigebe, wenn ich etwas online kaufe, sollte mir bewusst sein. Dass damit die Firma, von der ich kaufe, etwas anfangen kann und mir zumindest einen Newsletter schicken darf, wenn ich nicht widerspreche, auch noch. Aber es müsste ebenso selbstverständlich sein, dass außer mit ausdrücklicher Zustimmung des Kunden keinerlei Informationen an Dritte weitergegeben werden. Was aktuell in den USA passiert, wo Kundendaten von Internet Service Providern einfach (weiter)verkauft werden dürfen, ist in Deutschland zum Glück nicht absehbar. Aber wie so oft gilt: Wehret den Anfängen. •


OK

FREIHEIT FÜR SOFTWARE!

WIE VIEL KONTROLLE HABEN WIR ÜBER UNSERE PROGRAMME?

Wer hat Lust, sieben Seiten Lizenzbestimmungen zu lesen? Richtig, niemand. Das führt aber dazu, dass wir als Verbraucher gar nicht wissen, was wir den Programmen, die wir auf unserem Computer haben, so alles erlauben. Zeit, sich zu fragen, was in diesen Nutzungslizenzen eigentlich drin steht.

TEXT HAJO MOEBIUS
ILLUSTRATION HEIDRUN KLEINGRIES

Es klopft an meiner Zimmertür: Meine Mitbewohnerin Philomena hat ihren Laptop in der Hand und bittet mich, ihr zu helfen. Ihr alter Computer hat den Geist aufgegeben und sie installiert auf einem neuen Rechner gerade die wichtigsten Programme. Ob ich noch eine Version von Microsoft Office übrig hätte? Klar hab' ich das, und gebe Philomena meine CD mit der Software.

Doch als sie die Programme installiert, wird sie nicht nur nach dem Produktschlüssel gefragt, sondern auch nach einer Identifikationsnummer. Als ich ihr meine gebe, protestiert Office: Das Programm sei bereits auf einem anderen Rechner installiert, das verstoße gegen die Nutzungsbedingungen.

Philomena und ich schauen uns an. Nutzungsbedingungen? Das sind doch diese schrecklich komplizierten, langen und unverständlich geschriebenen Textwüsten, die man ganz schnell wieder wegklickt, damit die Installation weitergeht. Tatsächlich steht in der sogenannten End User Licence Agreement, kurz EULA, von Microsoft Office 365 Personal Folgendes:

»Unter unserer Lizenz gewähren wir Ihnen das Recht, diese eine Kopie der Software auf einem lizenzierten Gerät [...] zur Verwendung durch jeweils eine Person zu installieren und auszuführen, jedoch nur, wenn Sie alle Bestimmungen dieser Softwareergänzung einhalten.«

In den knapp sieben Seiten dieser EULA wird in Juristendeutsch oder -englisch beschrieben, was wir mit der Software tun dürfen, was nicht, was völlig verboten ist und welche Daten die Macher des Programms von uns haben wollen. Eigentlich sollten wir uns diese Texte alle durchlesen. Nur hat niemand dafür Zeit.

Nimmt man die Nutzungslizenz für Apples iTunes, dann enthält diese rund 3.800 Wörter in der deutschen Version. Geht man von 250 Wörtern Lesefähigkeit pro Minute aus (für geübte Leser, die meisten würden wohl länger brauchen), so kommt man auf einen Wert von 15 Minuten – nur für eine Softwarelizenz.

Philomena schaut panisch auf die Uhr. Sie muss heute noch unbedingt einen Text abgeben, das hatte sie mit einem Kunden vereinbart. Im Prinzip müsste sie für alle ►

Teile des Office-Pakets die Lizenz lesen. Also für Word, Excel, Outlook, Powerpoint… Dafür hat doch niemand Zeit! Was hat es mit diesen EULAs auf sich?

Im Prinzip sind EULAs rechtlich bindende Verträge zwischen dem Softwarevertreiber und dem Käufer. Meist sind diese Lizenzen aber erst bei der Installation komplett zu lesen. Wirklich widersprechen kann man ihnen zumeist nicht: Entweder klickt man auf »Akzeptieren« oder bricht die Installation ab und gibt die gekaufte Software zurück. Aber wer macht das schon? Schließlich bleibt einem ja sonst das Programm versperrt – und damit, beispielsweise bei Messengern wie WhatsApp, auch gleich der Kontakt zu Freunden und Familie.

Darauf spekulieren vielfach auch die Hersteller und verstecken in ihren EULAs einige Klauseln, denen wir als Verbraucher normalerweise nicht zustimmen würden. So steht bei Facebook:

»Du erteilst uns deine Erlaubnis zur Nutzung deines Namens, Profilbildes sowie deiner Inhalte und Informationen im Zusammenhang mit kommerziellen, gesponserten oder verwandten Inhalten (z. B. eine Marke, die dir gefällt), die von uns zur Verfügung gestellt oder aufgewertet werden.«

Sehr beliebt ist ebenfalls der Hinweis auf eine automatische Weitergabe von Daten an Dritte über das Internet. In der Lizenz zu Microsoft Office 365 Home Personal steht zum Beispiel:

»Wenn Sie Ihr Gerät mit dem Internet verbinden, stellen einige Features des Dienstes oder der Software möglicherweise eine Verbindung mit Computersystemen von Microsoft oder von Serviceprovidern her, um Daten zu senden oder zu empfangen. Sie erhalten womöglich nicht immer einen gesonderten Hinweis, wenn die Verbindung hergestellt wird.«

Allerdings: In Deutschland ist das Recht auf Verbraucherseite. Denn eine EULA gilt in der Bundesrepublik nur dann als rechtlich bindender Vertragsbestandteil, wenn der Text der Lizenz bereits zum Kauf vereinbart wurde – also der Käufer weiß, welchen Sachen er da zustimmt. In der Form, in der die meisten EULAs dargeboten werden, nach dem Kauf also, sind sie rechtlich eigentlich ungültig.

Das Bürgerliche Gesetzbuch regelt in den Paragraphen 305 bis 310 die sogenannten Allgemeinen Geschäftsbedingungen. Im Grunde sind Lizenzbestimmungen Allgemeine Geschäftsbedingungen, die in Deutschland tendenziell Verbraucher schützen. Deshalb gelten für sie auch bestimmte Regeln: Sie sollen verständlich formuliert sein, keine überraschenden Klauseln enthalten und somit die Verbraucher auch nicht benachteiligen. Wenn ein Käufer allerdings erst nach dem Bezahlvorgang die Lizenz lesen kann, so ist das schon eine ziemliche Benachteiligung des Verbrauchers.

Nur dann wären plötzlich alle kommerzielle Softwarelizenzen ungültig. Daher befinden sich viele Softwareprogramme in einer rechtlichen Grauzone: Zwar gelten die Nutzungsbedingungen nicht, aber da eine einheitliche Rechtsprechung fehlt, kann man sich als Verbraucher nicht darauf verlassen, dass die eine oder andere Klausel der Lizenz nicht doch greifen kann.

Eine Gemeinsamkeit vieler EULAs: Sie gewähren den Käufern nur eine Nutzungserlaubnis, kein Eigentum. Zwar habe ich meine Office-Version selbst gekauft, Philomena aber darf sie nicht nutzen, weil das gegen die Bedingungen der Lizenz verstößt. Das steht so in der EULA von Microsoft Office 365 Home Personal:

»Wir verkaufen unsere Software oder ihre Kopie davon nicht, sondern lizenzieren sie nur.«

Dass die meiste Software, die wir so tagtäglich benutzen, aus den unterschiedlichsten Ländern, allen voran aber den USA stammt, macht es nicht einfacher. Zwar könnte man meinen, nur deutsche Lizenzverträge seien wirklich gültig, da nur sie verständlich für deutsche Kunden sein könnten, doch die Rechtsprechung ist da anderer Meinung: Das Landgericht in München hat bereits 2004 eine Softwarelizenz für wirksam erklärt, obwohl sie nur in Englisch vorlag. Die Begründung: Englisch sei nun mal die gängige Sprache im Softwarebereich. Nach dieser Logik sind anderssprachige Lizenzen dann wirksam, wenn man sie von einer Seite aus dem Ausland herunterlädt – erst wenn der Anbieter seine Seite auch auf Deutsch anbietet, müsse er seine Lizenzen auch in dieser Sprache zugänglich machen.

Trotzdem ist man als Verbraucher nicht machtlos, wie der Fall Electronic Arts, kurz EA, zeigt. Der große, internationale Videospielherausgeber hat einen eigenen Webdienst für seine Spiele gegründet. Origin heißt das Programm und nur darüber sind die bekannten PC-Titel wie »Battlefield« oder »Fifa« spielbar.

Als Origin aber 2011 zusammen mit »Battlefield 3« eingeführt wurde, leistete sich EA einen Fauxpas: Man übersetzte damals die US-amerikanische EULA einfach ins Deutsche. Demnach sollten Nutzer der Spielefirma ziemlich weitreichende Rechte einräumen. So nahm sich EA heraus

- automatisch Lizenzrechte für die eigenen Produkte zu prüfen
- Daten über den Computer, seine Hardware, abgespielte Medien aufzuzeichnen und gegebenenfalls deren Lizenzrechte zu überprüfen
- und gab seinen »Partnern« einen Blankoscheck darin, Daten wie die IP-Adresse und andere technische Daten über die Software-Nutzung zu sammeln, zu nutzen und zu speichern.

Durch diese weitreichenden Rechte, die das Unternehmen sich selbst eingeräumt hat, wurde Origin schnell als Spyware betitelt, was wiederum den Datenschutzbeauftragten des Landes NRW alarmierte. Nach vielen Entschuldigungen seitens EA wurde die EULA von Origin branchenüblichen Standards angepasst und entschärft. Allerdings: IP-Adressen werden noch immer gespeichert und EA merkt sich auch noch immer, welcher PC da gerade welchen Titel abspielt. Allerdings dürfen diese Daten nicht mehr automatisch für Werbezwecke genutzt werden.

Philomena ist inzwischen der Verzweiflung nahe. Ein eigenes Office-Paket kann sie sich nicht wirklich leisten, aber irgendwie muss ihr Artikel fertig werden – damit verdient sie schließlich ihr Geld. Bei der Recherche zum Li-

zenzenkram stoßen wir jedoch noch auf eine interessante Sache. Etwas, das Philomena ihre Arbeit retten könnte.

Zum Glück gibt es nämlich auch eine ganze Reihe von Programmierern, die Knebellizenzen doof finden und deshalb ihre Software »frei« setzen – also für alle zugänglich. Das heißt nicht zwingend, dass sie kostenlos ist. Viel eher geht es darum, dass die Nutzer Freier Software ein paar grundlegende Freiheiten haben:

- Freiheit I: Nutzer dürfen das Programm für jeden Zweck nutzen.
- Freiheit II: Nutzer dürfen die Funktionsweise des Programms untersuchen und ihren eigenen Bedürfnissen anpassen.
- Freiheit III: Nutzer haben das Recht, das Programm weiterzuverbreiten und damit Menschen zu helfen.
- Freiheit IV: Nutzer dürfen das Programm verbessern und dieses dann wieder der Öffentlichkeit zur Verfügung stellen.

Damit steht Freie Software im Gegensatz zu kommerzieller Software, deren Käufer ihre Programme eben nicht weitergeben dürfen, wie Philomena und ich schmerzlich erfahren haben.

BITTE NICHT VERWECHSELN:

FREEWARE

ist kostenfrei, unterliegt aber Copyright-Bestimmungen, sodass keine Änderung und Weitergabe der Software möglich ist.

FREIE SOFTWARE

bezieht sich auf die vier Freiheiten, ist nicht unbedingt gratis und Benutzer können den Quellcode verändern und das Ergebnis veröffentlichen.

OPEN SOURCE SOFTWARE

ist oft gratis, hier wird aber meist von einer Expertengruppe oder einem Komitee bestimmt, was am Quellcode geändert werden soll. Ein Einzelner könnte den Code zwar für sich selbst anpassen, darf dieses Ergebnis dann aber nicht unbedingt auch veröffentlichen.

Die Idee von Freier Software, deren Code allen zugänglich ist und von der Allgemeinheit verbessert werden kann, geht zurück auf den Programmierer Richard Stallman. Der gründete 1985 in den USA die Free Software Foundation und zeichnet sich verantwortlich für die GNU-Lizenz, auf der beispielsweise das alternative Betriebssystem Linux aufbaut.

Zugegeben: Derartige Software ist wenig benutzerfreundlich und richtet sich eher an Menschen mit Programmierkenntnissen. Um dies zu kompensieren, haben sich Open-Source-Projekte gegründet, die einer anderen Philosophie folgen als Freie Software. Viele bekannte Projekte sind daraus hervorgegangen, zum Beispiel der bekannte Browser Firefox.

Ebenfalls ein Produkt dieser alternativen Software-Bewegung: Pakete wie Libre Office oder Open Office, kostenlose Programme, die eine ähnliche Funktion bieten wie das Angebot von Microsoft. Das kann sich Philomena auf ihren Computer herunterladen und mit dem Tippen beginnen.

Derweil recherchiere ich weiter. Es gibt eine ganze Menge an Angeboten in der freien und offenen Software-Szene. Programme wie der VLC Player spielen fast alle Medien ab, mit Audacity lassen sich Audioaufnahmen schneiden, Gimp und andere Grafikprogramme ermöglichen es, Fotos zu bearbeiten. Zwar punkten die großen Namen wie Adobe, Microsoft oder Google mit Benutzerführung, schlanker Optik und zuverlässiger Kompatibilität, aber ist es das Wert, dass wir unsere Daten an diese Unternehmen geben?

Wie man an Philomena sieht: Wir sind von Programmen und damit auch von ihren Herstellern abhängig. Da diese Software so essentiell für unser modernes Leben ist, sollte sie auf eine Art und Weise entstehen, die auch unserer Gesellschaft entspricht: einer freien, demokratischen. Momentan aber beherrschen Software-Riesen wie Google, Apple und Microsoft den Markt und zwingen Nutzer dazu, sich in den eng abgegrenzten Gärten der Programme zu bewegen.

Während Philomena fleißig tippt (und hin und wieder flucht), überlege ich mir, vielleicht einen Programmierkurs zu besuchen. Schließlich möchte ich langsam wissen, was im Code steckt, der mein Leben mitbestimmt. Vielleicht kann ich dann den Spieß umdrehen und diesen Code selbst schreiben. •

HaJo Möbius heißt eigentlich **Johannes Hahn**, und wenn er nicht gerade schreibt oder liest, spielt er Videospiele. Nach seinem Studium der Politik und Medien unterstützt Johannes die Crew von Kater Demos schon zum zweiten Mal. Nebenbei arbeitet Johannes als Redakteur, Autor und Podcaster. Wegen des Spiels »Dark Souls« hat er schon zwei Schreibtische demoliert.

HILFE, DER STAAT SCHNÜFFELT!

Dass der Staat uns überwacht: geschenkt! Der Clou – wir können ihn auch zurückü̈berwachen! Oder zumindest: ihm Fragen stellen; der Demokratie und dem Informationsfreiheitsgesetz sei Dank. Die Plattform *FragDenStaat.de* hilft dabei.

TEXT ALEXANDER SÄNGERLAUB
FOTOS SIMA EBRAHIMI

ARNE SEMSROTT

Zwischen spröden, charmebefreiten Plattenbauten, nicht weit vom Berliner Alexanderplatz entfernt, steht ein kleines Backsteinhaus versteckt, das in seinem Inneren nicht nur ein gewaltiges, wunderschönes Atrium und ein Hostel verbirgt, sondern auch die Open Knowlegde Foundation. Die hat eine Menge guter Projekte im Ärmel, darunter FragDenStaat.de. Wir trafen uns mit Arne Semsrott – dem Projektleiter.

KATER DEMOS ***Was ist FragDenStaat.de und was kann ich als Bürger damit machen?***
ARNE SEMSROTT FragDenStaat.de ist die Online-Plattform für Informationsfreiheit in Deutschland. Über FragDenStaat.de lässt sich sehr einfach jegliche Art von Anfrage transparent an eine Behörde stellen: Man kann nämlich alle möglichen Informationen anfragen, die beim Staat liegen. Das kann zum Beispiel ein Schriftwechsel zwischen zwei Behörden sein, aber auch Fotos oder Videos, welche die Polizei bei Demonstrationen macht. Alle gestellten Anfragen sind dann wiederum auf FragDenStaat.de einsehbar. Jede einzelne Anfrage befreit also die Information für die gesamte Öffentlichkeit.

KD ***Und wer nutzt das hauptsächlich – außer vielleicht Journalisten und Anwälte?***
AS Journalisten, das könnte man meinen – die sind es aber nicht unbedingt, weil sie häufig nicht offenlegen wollen, wie sie an Informationen kommen. Die nutzen für ihre Recherchen eher die Infos, die schon offenliegen. Hauptnutzer sind politisch interessierte Leute. Die fragen alles mögliche, von »In meinen Dorf wird ein Schwimmbad gebaut und ich möchte wissen, was der Dorfrat dazu beschlossen hat und wie das Budget ist« bis hin zu »Das Ministerium XY plant dieses und jenes Gesetz. Mich interessiert, mit welchen Lobbyisten sich das Ministerium getroffen hat.« Hier sind natürlich auch viele NGOs neugierig.

KD ***Bleiben wir mal beim Schwimmbad. Ich würde jetzt gerne wissen, wie es um die finanzielle Situation des Schwimmbads in meinem Ortsteil steht. Wie kommt ihr ins Spiel?***
AS Du gehst auf FragDenStaat.de. Entweder weißt du schon, welche Behörde diese Information hat, vielleicht das Bezirks- oder das Ordnungsamt, oder du fragst uns beziehungsweise die Community. Dann gibst du den Namen der Behörde ein, die Mailadressen sind hinterlegt, und schreibst in einem Satz deine Anfrage. FragDenStaat.de versendet das dann für dich mit möglichen legalen Hinweisen, zum Beispiel: »Dies ist ein Antrag nach dem Informationsfreiheitsgesetz Nordrhein-Westfalens, nach §3 haben Sie nach drei Tagen zu antworten«. Gibt es eine Ablehnung, helfen wir auch.

KD ***Worüber muss der Staat denn eigentlich Auskunft geben und worüber nicht? Welche Bereiche sind ausgeschlossen vom Informationsfreiheitsgesetz?***
AS Grundsätzlich sind alle Informationen zugänglich. Es sei denn, einer oder mehrere von 30 Ausnahmetatbeständen treffen zu. Das deutsche Gesetz ist im internationalen Vergleich tatsächlich relativ schlecht, in den USA gibt es zum Beispiel nur neun Ausnahmetatbestände. Die am meisten vom Staat genutzten Ausnahmetatbestände sind »Betriebs- und Geschäftsgeheimnisse«. Das heißt, wenn der Staat mit einem Unternehmen einen Vertrag schließt, dann müssen die Passagen nicht herausgegeben werden, die Geschäftsgeheimnisse berühren. Ein anderer beliebter Grund ist der »Schutz der öffentlichen Sicherheit«, wenn der Staat beispielsweise verhindern möchte, dass spezifische Details zu Atomkraftwerken den falschen Leuten in die Hände geraten.

KD ***Ist das in Anbetracht der ganzen Private Public Partnerships zwischen Staat und Unternehmen nicht ein Riesenproblem, wenn ich da nicht alles einsehen kann, zum Beispiel bezogen auf Unternehmen wie VW oder Toll Collect?***
AS Das ist ein Riesenproblem! Es ist eines der zentralen Probleme mit diesem Gesetz – daher auch unsere tolle Kunstaktion. In sehr vielen kritischen Dokumenten geht es um Betriebs- und Geschäftsgeheimnisse. Volkswagen ist ein Topbeispiel dafür. Das Verkehrsministerium hat mutmaßlich schon vor der Bekanntwerdung des VW-Skandals davon gewusst. Aber alle Dokumente, die es dazu gibt, betreffen Betriebs- und Geschäftsgeheimnisse von Volkswagen, sind also für Journalisten oder NGOs nicht einsehbar. Das führt dann zur Herausgabe von Dokumenten, wie wir sie bekommen haben, wo einfach die ganze Seite geschwärzt wurde; in diesem Fall vom Bundeswirtschaftsministerium.

KD ***Amerika hast du schon erwähnt. Wo stehen wir denn nun international betrachtet in Sachen Informationsfreiheit?***
AS Es gibt das Global Right to Information Rating, wo 111 Informationsfreiheitsgesetze auf der Welt miteinander verglichen werden. Deutschland ist auf Platz 105 von 111.

Dennoch ist es ein unterschätztes Gesetz, weil man an viel mehr Informationen rankommt, als man glaubt. Nur nutzen es noch nicht allzu viele Menschen. Wir haben zum Beispiel gerade die Gesprächsvorbereitung des Innenministers zu seinem Treffen mit dem Facebook-Chef Mark Zuckerberg bekommen. Ich denke, dass viele nicht wissen, dass man das Recht hat, diese Information zu bekommen.

KD ***Das klingt spannend! Wer hat das denn angefragt, warum und was steht drin?***
AS Diese Anfrage haben wir tatsächlich selbst gestellt. Hier haben wir genau nach allen Dokumenten zur Gesprächsvorbereitung von Thomas de Maizière gefragt und als Antwort darauf einen Vermerk des Pressereferats des Ministeriums bekommen, das den Briefverkehr zwischen verschiedenen Referaten des Ministeriums enthält. Die 20 Seiten zeigen, worauf sich der Minister vorbereitet hat. Er macht sich zum Beispiel Sorgen über zu viel Hate Speech auf Facebook. Praktisch, da meist das konkrete Gespräch nicht protokolliert wird oder nur ausgesuchte Versatzstücke an die Öffentlichkeit dringen. Das alles ist auch bald online für alle einsehbar. ►

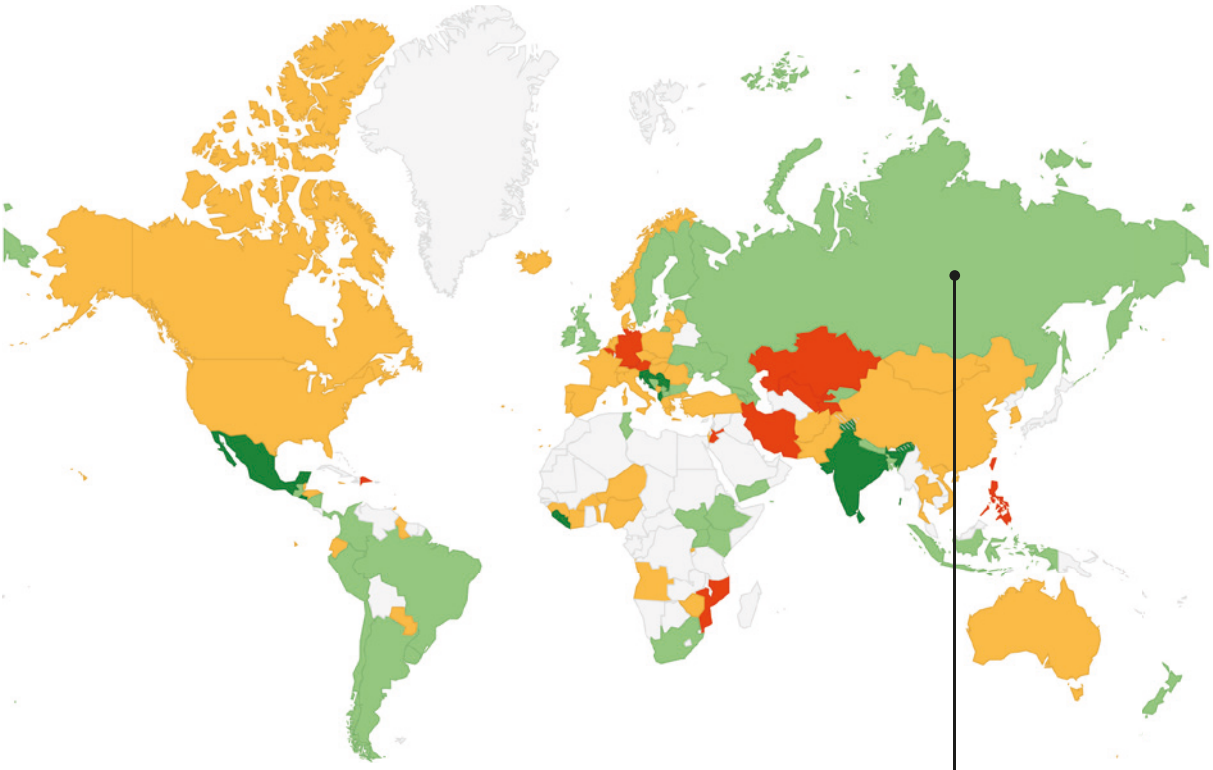
KD ***Welche Behörden sind denn besonders auskunftsunwillig?***
AS Es ist das Innenministerium, das leider auch die Verantwortung für das Gesetz hat. Das hat aber auch Ressorttradition: Das Innenministerium lässt sich besonders ungern in die Karten schauen, ebenso das Bundeskanzleramt oder der Bundestag. Das Umweltministerium ist da vergleichsweise völlig anders. Es strebt viel eher Koalitionen mit der Zivilgesellschaft an. Hier bekommt man dementsprechend recht schnell Informationen und muss in der Regel auch keine Gebühren dafür bezahlen.

KD ***Das Umweltministerium macht das ja auch schon seit 1994, die anderen Ministerien erst seit 2006. Versteht ihr euch als Vorreiter einer neuen politischen Kultur, damit die Ministerien sich so langsam öffnen wie die Austern?***
AS Absolut! Spannend ist auch, dass die Grenze der Auskunftsfreudigkeit weniger zwischen den Ministerien, als zwischen den Generationen der Menschen verläuft, die dort arbeiten. Wir merken, dass jüngere Mitarbeiter im Innenministerium beispielsweise viel offener sind. Manchmal sind wir erfolgreicher, wenn wir ein Ministerium einfach antwittern, statt den offiziellen Weg zu gehen. Wenn das der Trend ist, stehen uns gute Zeiten bevor.

KD ***Ihr zieht aber zuweilen auch vor Gericht, wenn bestimmte Behörden überhaupt nicht auskunftswillig sind.***
AS Wir klagen selbst oder finanzieren auch Klagen von anderen, meist vor dem Verwaltungsgericht. Das entscheidet am Ende dann oft, dass man die Informationen bekommen darf.

KD ***Ihr habt bestimmte Schwesterplattformen gegründet, wie FragDenBundestag.de oder FragDasJobcenter.de. Warum braucht es diese spezifischen Seiten?***
AS Solche Kampagnen fahren wir in den Bereichen, wo wir das Gefühl haben, dass da besonders viel im Argen liegt. Das Bundesverwaltungsgericht hat den Bundestag dazu verurteilt, gewisse Ausarbeitungen des Wissenschaftlichen Dienstes herauszugeben.

Der Wissenschaftliche Dienst des Bundestages erarbeitet jedes Jahr Tausende Gutachten zu allen möglichen Themen, sei es der Finanzmarkt in China oder die Drogenpolitik in Berlin. Diese Ausarbeitungen, von denen sie nun gezwungen waren, einzelne herauszugeben, dienen als Grundlage für Gesetze. Wir haben dem Bundestag vorgeschlagen, doch einfach direkt alle Ausarbeitungen auf ihrer Online-Plattform freizugeben. Der Bundestag antwortete: »Vielen Dank, wir melden uns!«, und hat sich daraufhin nie wieder gemeldet. Zusammen mit Abgeordnetenwatch.de haben wir dann eine Datenbank mit einer Liste von 5.000 Gutachten angelegt, die von unseren Nutzern automatisch beim Bundestag angefragt werden konnten. Das führte dazu, dass der Bundestag mit Anfragen regelrecht geflutet wurde. Bedeutet: Beim Bundestag mussten sie entscheiden, ob sie Tausende von Anfragen einzeln ausdrucken, Aktenzeichen vergeben, Bearbeiter-Namen schwärzen, an den Vorgesetzten geben, Empfangsbestätigung mit der Post rausgeben – oder ob sie die Gutachten einfach online stellen. Drei Wochen später geschah genau letzteres und das gilt jetzt für alle zukünftigen Ausarbeitungen. Das ist genau unser Weg, solche Wissensschätze zu befreien.



KD ***Was war denn die skurrilste aller Anfragen, die bisher über eure Seite lief?***

AS Meine Lieblingsanfrage ist, glaube ich, auch die berühmteste aller Anfragen: die Anfrage eines Schülers nach den Abiturfragen. Der dachte sich beim Lernen: »Halt mal! Das sind doch Informationen, die beim Staat liegen!«Also hat er vor den Prüfungen beim Ministerium die Aufgaben angefragt. Das ging dann durch die internationale Presse. Das Ministerium musste erst einmal herausfinden, wie sie das ablehnen können. Letztlich haben sie aber einen Ausnahmetatbestand gefunden: »Schutz des behördlichen Entscheidungsinteresses«. Immerhin haben sie ihm dann einen Tag nach dem Abi die Aufgaben zugeschickt. Hat ihm zwar nicht mehr geholfen, aber vielleicht den Schülern im nächsten Jahr zum Lernen.

KD ***Arne, vielen Dank für das Gespräch.*** •

GLOBAL RIGHT TO INFORMATION RATING MAP, 2015

Die Karte zeigt, welche Länder gut (grün) und welche schlecht (rot) abschneiden. Unerwartet: Mexiko hat das beste Informationsfreiheitsgesetz, Österreich das schlechteste. Grund dafür ist die österreichische Verfassung, die in Artikel 20.3 quasi eine Art Verschwiegenheitsklausel für alle staatlichen Organe beinhaltet.

www.rti-rating.org

EMPFEHLUNGEN ZUM THEMA

Wie man FragDenStaat.de helfen kann:

- Selber die Seite besuchen und seine Informationsauskunftsrechte nutzen.
- Spenden! Empfänger:
  Open Knowledge Foundation Deutschland e.V.
  IBAN: DE18830944950503009670,
  Verwendungszweck: FragdenStaat

SHARING IS CARING – OFFENE DATEN ZUM NUTZEN ALLER

Wie bei (fast) jeder anderen Technologie kommt es auch bei Überwachung auf die Motivation dahinter an. Denn es gibt durchaus Formen moderner Überwachung und Big-Data-Sammelwut, die einen Mehrwert bringen und uns im Alltag helfen. Sinnvolle Nutzung statt Missbrauch und Panoptikum. Zeit für einen kurzen Perspektivenwechsel.

TEXT SASKIA SELL
ILLUSTRATION VOLKER STRÄTER

Das Kind von Yodit Stanton hat Asthma, häufig ein Resultat schlechter Luftqualität. Die englische IT-Spezialistin macht sich auf die Suche nach frei zugänglichen Informationen zur Luftqualität in ihrem Londoner Wohnumfeld, ohne Erfolg. Frustriert darüber, dass lediglich Statistiken auf Makroebene zugänglich sind, beginnt Stanton mit eigenen Messungen in ihrem Block. Kurze Zeit später beschließt sie, das Start-up OpenSensors.io zu gründen: Heute ist ihr soziales Netzwerk für Sensordaten, die in unterschiedlichsten Kontexten verknüpft werden können, die größte Open-Data-Plattform in der Internet of Things-Welt.

An den Komplexen »Wohnen« und »Arbeiten« zeigt sich beispielhaft, wie wir von Stantons Idee einer offenen und miteinander vernetzten Sensorüberwachung profitieren können. OpenSensors.io hat mit der »Flood Map« einen Service entwickelt, der Wasserstandsdaten von Privatgrundstücken an Flussläufen in Echtzeit übermittelt und verarbeitet. Dies funktioniert über Crowdsourcing: Jeder Hausbesitzer, der in der Nähe eines Flusses wohnt, kann auf seinem Grundstück einen Sensor installieren. Die erhobenen Daten werden übermittelt und in einer Datenbank gespeichert. Sollte der Wasserstand steigen oder entlang des Flusslaufs der Pegel absehbar eine kritische Grenze überschreiten, werden die Anwohner darüber umgehend benachrichtigt. Die relevante Karte ist im Netz frei einsehbar.

Das andere Anwendungsbeispiel nennt sich »evidenzbasierte Arbeitsplatzgestaltung«. Was heißt das? Um Arbeitsplätze sinnvoll gestalten zu können, müssen Architekten wissen, wer welche Räume in einem Unternehmen wie nutzt. Zum einen können sie dabei über OpenSensors.io öffentliche Wetter- und Verkehrsdaten bei ihrer Planung berücksichtigen. Zum anderen installieren Unternehmen selbst Sensoren: Die Gewohnheiten ihrer Mitarbeiter werden temporär überwacht und auch diese Daten in den Dienst integriert. Wer legt welche Wege zurück, wer schaut in welchem Winkel auf seinen Bildschirm, wer braucht wo mehr Licht, wie wird der Besprechungsraum genutzt, welches Gerät ist wann an- oder ausgeschaltet? Die Raumgestaltung kann somit dank Sensordaten des Unternehmens sowie der offenen Daten aus dem Umfeld des Gebäudes an die Bedürfnisse der Angestellten architektonisch angepasst werden.

Open-Data-Projekte laufen auch hierzulande. Die Deutsche Bahn etwa baut derzeit einen frei zugänglichen Datenbestand zu Infrastruktur und Mobilität auf. Neben dem Monitoring von Luftqualität und Schadstoffausstößen werden bisher Daten zum Streckennetz, zu Bahnsteigen, Servicestellen und Frachtverkehr zur Verfügung gestellt. Auch zu Aufzügen werden offene Datensätze angeboten – hilfreich, wenn man mit Kinderwagen, schwerem Gepäck oder im Rollstuhl auf selbige angewiesen ist.

Das Sammeln und Speichern muss also nicht per se problematisch sein, der Umgang mit den ermittelten Daten zählt. Wenn der Supermarkt an der Ecke speichert, was wann gekauft wird, kommt es seltener zu Versorgungsengpässen, weil bedarfsgerecht beim Großhändler bestellt werden kann. Dass Krankenakten anonymisiert ausgewertet werden ist sinnvoll, um dank Mustererkennung Rückschlüsse über Umweltfaktoren zu ziehen, die möglicherweise krank machen. Pikanter wird es bei der Erhebung von Zensusdaten durch das Anwohnermeldeamt: Wer die Zusammensetzung der Anwohnerschaft kennt, kann den Bedarf an Schulen, Krankenhäusern oder Altersheimen feststellen. In den 80ern gab es allerdings starke Proteste gegen diese Form der Volkszählung, es ging damals bis zur Klage beim Verfassungsgericht. Kritiker mahnten an, dass selbst bei anonymisierten Datensätzen eine Re-Identifizierung des Einzelnen nicht ausgeschlossen war. Die Missbrauchsgefahr wäre also gegeben. Hier kommen Datenschützer ins Spiel, die dafür sorgen wollen, dass wir Informationen aus großen Datensätzen sinnvoll nutzen, ohne individuelle Freiheits- und Privatrechte zu gefährden. Öffentliche Daten nützen, private Daten schützen – sagt auch der CCC. Das klappt heute so mittelmäßig gut.

Wir schießen uns bei sukzessiver Digitalisierung und Vernetzung auf einen neugierigen und gefährlichen Big Brother ein. Kann Überwachung stattfinden und die Privatsphäre gewahrt bleiben? Kann die Gesellschaft von einer Big-Data-Sammelwut profitieren, oder können das nur private Unternehmen? Kann die Dystopie einer Utopie weichen, bei der Transparenz allen Menschen dient statt nur wenigen? Yodit Stanton und die Deutsche Bahn zeigen, was möglich ist.

LINKS ZUM THEMA

OpenSensors.io: https://www.opensensors.io/
Open Data Portal der Deutschen Bahn: http://data.deutschebahn.com/
Flutnetzwerk: https://flood.network/

ICH SEHE WAS, WAS DU NICHT SIEHST (UND NOCH VIEL MEHR)

In kaum einem anderen Land wird so viel überwacht wie im Vereinigten Königreich. Die Diskussion darüber, wie und ob das alles etwas bringt, dauert bis heute an.

TEXT JOHANNES HEIM
ILLUSTRATION ANNI STELKE

Wir kommen nicht umhin, uns in einer Ausgabe über Überwachung ab und an George Orwells »1984« zu erinnern. Denn in keiner Dystopie ist die konstante Beobachtung so vorherrschend wie in diesem Buch. Ähnlich wie bei den allgegenwärtigen Telescreens des Buches ist die britische Kameraüberwachung Closed Circuit Television (CCTV) oft nicht mal versteckt, sondern weithin sichtbar, allein aus Gründen der Abschreckung.

Und wenn nicht offensichtlich, dann muss zumindest in Ländern mit überwältigend vielen Kameras wie dem Vereinigten Königreich darauf hingewiesen werden, dass man gefilmt wird. Das hilft aber dem nicht viel, dem diese Praxis ohnehin sauer aufstößt. Voranstellen muss man an dieser Stelle aber, dass die Überwachungswut der Untertanen von Elisabeth II. allgemein ziemlich groß ist. Zwischen 11 und 32 Einwohner kommen auf eine Kamera. Überwachung ist hier kein Privileg des Staates: Viele der Aufnahmegeräte sind in privater Hand oder in der von Firmen.

Es wird nach wie vor heiß diskutiert, ob die Kameras Straftaten und Terrorismus verhindern. Prävention scheint jedenfalls wichtiger als die Aufklärung eines bereits geschehenen Verbrechens zu sein. Fälle wie der des »London Nail Bombers« oder der verwirrten Mörderin Nicola Edgington zeigten, dass Kameraüberwachung die Täterermittlung oft erleichtert.

Zwei Probleme gehen daher mit der Effizienz von Überwachung einher. Erstens: Ist es das wert? Dann kann man aufschreien, wenn vermeintlich ein Preis an ein Menschenleben beziehungsweise an dessen Unversehrtheit geheftet wird. Die Herstellung von Sicherheit hat eine Grenze – finanziell wie moralisch. Nur wo sind diese? Und zweitens: Was hilft uns die Ermittlung des Täters, wenn aber im Allgemeinen die Straftaten durch die Überwachung nicht bedeutend zurückgehen?

In TV-Serien wie »Broadchurch« und »The Fall« sieht man, wie alltäglich Kameraüberwachung bei (britischer) Polizeiarbeit inzwischen ist. Verhindert aber haben sie im Fernsehen nichts und in der Realität, so scheint es bisher, verlegen sie eher den Ort des Verbrechens in zwielichtige Ecken. Viele Studien verweisen darauf, dass es in spezifischen Fällen wie Parkhäusern signifikant weniger Straftaten gab, so zum Beispiel eine Veröffentlichung zur Verbrechensprävention von den Kriminologen Brandon Welsh und David Farrington aus dem Jahr 2009. Aber gerade bei eher impulsiven Straftaten wie Gewaltverbrechen scheint Überwachung keinerlei messbare, positive Effekte mit sich zu bringen, jedenfalls nicht in der Prävention.

Überwachung kostet die Gesellschaft aber zweimal. Einmal materiell, weil durch die Technik, die bezahlt werden muss, automatisch andernorts Geld fehlt. Zudem schaffen die Menschen hinter der Kamera keinen wirtschaftlichen Wert, der die ungeheuren Ausgaben für großflächige Überwachung rechtfertigt.

Und zum Zweiten ist da der moralische Preis, den die ganze Gesellschaft bezahlt. Freiheiten und individuelle Rechte des Einzelnen werden aufgeben, weil man aus diffuser Angst vor dem Nächsten lieber jeden überwachen lässt, auch sich selbst. Das trägt dann zuweilen recht absurde Früchte, wie Juli Zeh und Ilija Trojanow in ihrem Buch »Angriff auf die Freiheit« beschreiben: Darin wird das Anti-Terror-Gesetz »RIPA« (Regulation of Investigatory Powers Act) unter anderem dafür eingesetzt, um mit Hilfe der Kameras Hundehalter zu stellen, die die Hundehaufen ihrer Kläffer nicht richtig entsorgen. Wenn wir keinen Polizeistaat wollen, dann müssen wir eine gewisse Unsicherheit akzeptieren. Eine Unsicherheit, die auch mit Kameras an jeder Ecke nie ganz verschwinden wird.

DER ÜBER-WACHUNGSSTAAT UND ICH

Das Tückische an der Überwachung ist, dass sie unsichtbar ist. Deswegen können wir sie so leicht verdrängen, obwohl sie uns im Alltag ständig begleitet und persönliche Daten über uns gesammelt werden. Aus dieser digitalen Spur entsteht eine zweite Identität unserer selbst – und wir wissen nicht, ob diese verdächtig ist. Was weiß der Staat eigentlich über uns?

TEXT JULIA STÜRZL
ILLUSTRATION RICHARD KLIPPFELD

Nach jedem Terroranschlag nutzt der Staat die Gelegenheit, die Überwachung im öffentlichen und privaten Raum weiter auszubauen – im Namen der Sicherheit. Im Jahr 2008 erhielt beispielsweise das *Bundeskriminalamt* (BKA) mit der Neufassung des »Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus« weitreichende Befugnisse, die vorher nur der Landespolizei zustanden. Dies betrifft Online-Durchsuchungen, Rasterfahndung, Einsatz von verdeckten Ermittlern, akustische und optische Überwachung von Wohnungen und Telekommunikationsüberwachung. Die Kritikpunkte daran sind, dass seitdem präventive Ermittlungen ohne konkreten Tatverdacht und in eigener Regie durchführbar sind und das BKA im Rahmen von Vorfeldermittlungen nicht mehr der Staatsanwaltschaft untersteht. Ob solche Maßnahmen zur Kriminalitätsbekämpfung effektiv sind, ist zwar keineswegs sicher. Aber der Staat handelt, um irgendetwas zu tun und angesichts der unberechenbaren, terroristischen Bedrohung nicht hilflos zu wirken.

Die gleiche Ohnmacht ist bei uns Bürgern zu finden – wir wissen zwar, dass diese neuen Abhör- und Überwachungsaktionen uns ebenfalls betreffen, aber wir setzen uns damit kaum auseinander. Laut einer Studie des *Deutschen Instituts für Vertrauen und Sicherheit im Internet* (DIVSI) aus dem Jahr 2014, also ein Jahr nach den Snowden-Enthüllungen, geht zwar jeder Zweite davon aus, dass er von Geheimdiensten abgehört wird – aber nur knapp jeder Vierte gab an, beim Telefonieren, Mailen und Surfen im Internet nun vorsichtiger zu sein. Wozu auch? Wir werden schließlich vorher nicht nach Erlaubnis gefragt und außerdem gewinnen wir doch durch diese Einschnitte in unsere Grundrechte mehr Sicherheit – so wird es uns zumindest vermittelt. ▸

DIE SELBSTÜBERWACHUNG

Heute könnte der *Bundesnachrichtendienst* (BND) auch unsere E-Mails und Telefonate abhören, ohne dass er dafür öffentlich Begründungen liefern müsste – wir würden von dieser Überwachung nie erfahren. Und wer weiß schon, ab wann er sich verdächtig macht. Vielleicht schon mit dem Kauf dieser *Kater-Demos*-Ausgabe via Kreditkarte? Kaum ein Bürger wird wahrscheinlich die rechtlichen Grundlagen und gelebte Praxis kennen, ab wann eine generelle Überwachung stattfindet und ab wann man ins Visier der Behörden gerät. Ab dem Zeitpunkt, an dem man merkt, dass man in einem Überwachungsstaat lebt, ist es schon zu spät, sich dagegen zu wehren. Die *Bundeszentrale für politische Bildung* (bpb) beschreibt den Überwachungsstaat als »Staat, der in alle privaten Lebensbereiche des Einzelnen vordringt und eine nahezu unbegrenzte Macht entwickelt, weil er alles über seine Bürger weiß«. Wir merken nicht, dass unsere Freiheit im beruhigenden Wattebausch der Sicherheit langsam zu ersticken droht. Sind wir also auf einem Weg zum Überwachungsstaat?

DIE WANZE IN MEINER HOSENTASCHE

Wir in Deutschland können immer noch frei unsere Meinung äußern, aber ein großer Teil unserer Kommunikation wird dennoch gespeichert: Bis zu 220 Millionen Metadaten werden jeden Tag vom BND gesammelt – vor allem Informationen darüber, wer, wo, wann und mit wem telefoniert, chattet oder schreibt. Die Plattform für digitale Freiheitsrechte *Netzpolitik.org* zeigt, dass der BND mit seinen Programmen zur Überwachung der weltweiten Datenströme (SIGINT) und der Analyse dieser Daten (AIDA) insgesamt 90 Prozent seiner Mittel in die Internetüberwachung investiert. Die Zeiten, in denen Geheimdienstler heimlich einbrechen mussten, um Wohnungen zu verwanzen, sind vorbei.

Heute geht das Spionieren bequemer; die Technik übernimmt den Hauptteil der Arbeit: Steueridentifikationsnummer, Bundesmelde- und Ausländerzentralregister, biometrischer Personalausweis und Gesundheitskarte sind nur einige Möglichkeiten, bei denen uns der Staat nicht heimlich, sondern hochoffiziell überwachen kann. Denn diese Dokumente können bei der Erstellung von Bewegungsprofilen helfen, zum Beispiel durch Videoüberwachung mit biometrischen Identifikationsmethoden, Ortung von Mobiltelefonen, Maut und – nicht zu vergessen – RFID. Dieses Kürzel steht für *radio-frequency identification* und ist eine Technologie

VERSCHIEDENE ÜBERWACHUNGSMASSNAHMEN

INDECT

Zwischen 2009 und 2014 investierte die EU über vier Milliarden Euro in ein Überwachungsprojekt namens INDECT, das über Videoüberwachung »abnormales Verhalten« im öffentlichen Raum aufspüren und melden soll. Wie funktioniert das? Eine automatisierte Analyse der Überwachungskameras und unserer Daten aus sozialen Netzwerken und Telekommunikationsüberwachung bewertet, ob unser Verhalten verdächtig ist.

CAPER

Eine Art Internetscanner ist das EU-Projekt CAPER, das Daten von sozialen Medien und Suchmaschinen semantisch auswertet und mit Polizeidaten kombiniert. Auch die Universität der Bundeswehr hilft fleißig mit: Sie sammelt Social-Media-Daten, um eine Studie zur automatisierten Beobachtung von Internetinhalten zu erstellen.

PROACTIVE

Da uns in Zukunft nicht nur unser Handy überwacht, sondern auch unsere digitalisierten Autos, Kühlschränke und Lichtanlagen, wird das 4,7 Millionen Euro teure Forschungsprojekt Proactive die Sensordaten aus vernetzten Geräten mit Polizeidaten kombinieren. So sollen typische Verhaltensmuster definiert und darauf basierend bereits erwähntes »abnormales Verhalten« erkannt und Gewalttaten präventiv verhindert werden. Es wird also alles das gesammelt wird, was nicht verschlüsselt ist.

ZERBERUS & VISTA

Der Geheimdienst will bestehende Abhör-Fähigkeiten ausbauen und neue schaffen: Satelliten und Glasfaser-Kabel, sprich, der Erweiterung von so genannter G-10-Kabelerfassung (Inland) und regionaler Kabelerfassung (Ausland). Vor allem durch G-10, das Abhören des Internetverkehrs an Knotenpunkten, wird die Macht des BND gestärkt und er wird zum wichtigsten Pfeiler der Cybersicherheitsarchitektur der Bundesregierung. Mit VISTA investiert der BND in die Selektion und Verarbeitung von Massendaten, vor allem der Metadaten.

ANTI-TERROR-RICHTLINIE

Das im Februar 2017 neu beschlossene Gesetz ist starker Kritik ausgesetzt, da es wegen teils unscharfer Bestimmungen auf Bereiche ausgedehnt werden könnte, die bisher nicht als Terrorismus gelten – etwa öffentlichkeitswirksame Proteste von Polit- und Ökoaktivisten oder Reisen, die als zu terroristischen Zwecken fehlinterpretiert werden könnten. Zudem wird den EU-Mitgliedstaaten unter anderem die Möglichkeit eingeräumt, Netzsperren zu errichten.

zum berührungslosen Identifizieren und Lokalisieren von Objekten mittels Radiowellen.

Viele von uns kennen sie bereits: sie sind in Transpondern vieler Firmen als Türöffner eingebaut. Diese im Ausweis oder der Kreditkarte eingebauten Chips sind nur so groß wie ein Sandkorn und wir tragen sie wie Wanzen jederzeit mit uns herum – teils sogar freiwillig, Stichwort kontaktloses Bezahlen mit Kreditkarten. Im Unterschied zum Handy, mit dem wir ebenfalls leicht lokalisierbar sind, können wir RFID-Chips aber nicht einfach ausschalten oder entfernen. Sie begleiten uns überall hin, ob wir wollen oder nicht. RFID-Chips sind vielfältig für die Identifizierung von Objekten einsetzbar, in der Industrie oder als Fälschungsschutz von Dokumenten. Das Problem daran ist, dass die Hersteller der Chips beständig Informationen über uns sammeln können.

DIE FREMDÜBERWACHUNG

Viele dieser neuen Bestimmungen kommen unter dem Tarnmantel des technischen Fortschritts, der Digitalisierung und der Sicherheit angeschlichen. Sie mögen uns einen praktischen Nutzen bringen, aber sie beinhalten gleichzeitig die Möglichkeit, uns zu überwachen. Überwachungsmaßnahmen sollen in erster Linie Sicherheit verschaffen: Neben Behörden, die unsere Daten sammeln, gibt es aber auch solche, die sie schützen wollen. Zum Beispiel die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) Andrea Voßhoff und auch Landesdatenschutzbeauftragte für jedes Bundesland, die die öffentlichen Stellen in Fragen des Datenschutzes beraten und kontrollieren sollen.

Für den IT-Schutz von Bürgern und Unternehmern existiert mit dem *Bundesamt für Sicherheit in der Informationstechnik* (BSI) bereits eine zuständige Bundesbehörde – nur genießt diese einen zweifelhaften Ruf. Erstes Problem: Sie ist dem *Bundesinnenministerium* (BMI) unterstellt und somit nicht unabhängig, was zu Interessenskonflikten führen kann: Beispielsweise entwickelte das BSI in der Vergangenheit mit dem BKA einen Staatstrojaner zur besseren Datenerfassung, hielt parallel dazu aber einen mit Steuergeldern finanzierten Leitfaden zur IT-Sicherheit für Bürger zurück. Darüber hinaus wird der neue BSI-Chef Arne Schönbohm von Medien wie der *Welt* und dem *Tagesspiegel* stark kritisiert, da er weder ausreichend technische Kompetenzen, noch eine vertrauenswürdige Vita vorweisen könne. Der Grünen-Politiker Konstantin von Notz nennt ihn gar »IT-Lobbyist« und Constanze Kurz, die Sprecherin des Chaos Computer Clubs, erzählt, in der Branche werde er als »Cyber-Clown« verspottet.

Die Cyber-Abwehr scheint jedoch das Steckenpferd vieler Behörden zu sein: Neben BSI, BND und Bundeswehr konkurrieren diverse weitere Einrichtungen um Befugnisse und Ressourcen in diesem Bereich, was ein riesiges Kompetenzchaos verursacht. Denn das *Bundesamt für Verfassungsschutz* (BfV), das *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe* (BBK), der *Militärische Abschirmdienst* (MAD), das BKA, das *Zollkriminalamt* (ZKA) und diverse Landesbehörden kümmern sich ebenfalls um gewisse Teilbereiche der Cyber-Abwehr. Und hier fängt bereits ein großes Problem der Überwachung an: Wenn wir nicht wissen, wer was überwacht – wie soll das dann kontrolliert werden? Es gibt mit dem parlamentarischen Kontrollausschuss zwar ein formales Kontrollgremium, doch der unübersichtliche Kompetenz-Föderalismus macht eine umfassende Kontrolle der Datensammlung und -verwertung schlichtweg unmöglich. Was hier fehlt, sind klare Strukturen. Doch das bisherige Fehlen ebenjener untergräbt das Vertrauen der Menschen in die Regierung. Es gibt also keine einheitlichen Regeln für die Analyse und Verwendung unserer Daten und dies hat direkte Folgen für uns.

BIS ZU 220 MILLIONEN METADATEN WERDEN JEDEN TAG VOM BND GESAMMELT

WIR FILMEN SIE ZU IHRER SICHERHEIT: DIE FOLGEN DER ÜBERWACHUNG

Ein Facebook-Kommentar unter Freunden wie: »Ich bin heute so mies gelaunt, ich lauf gleich Amok«, bleibt in Deutschland noch folgenlos – zumindest meistens. Daniel Bangert ist eine der Ausnahmen dieser Regel, seine Geschichte ist die Verkörperung der Überwachungs-Dystopie. Eines Morgens vor vier Jahren klingelten plötzlich Polizeibeamte und der Staatsschutz an seiner Haustür im hessischen Griesheim. Sein Verbrechen? Er hatte sich etwas zu sehr für den NSA-Abhörskandal rund um den ▸

Whistleblower Edward Snowden interessiert und auf Facebook gemeinsame Besuche des in Griesheim ansässigen *Dagger Complex*, der angeblichen Europazentrale der National Security Agency (NSA), initiiert. Doch die NSA steht ganz offensichtlich überhaupt nicht auf öffentliche Aufmerksamkeit. Das bekam Bangert mit diesem Besuch der deutschen Staatsmacht zu spüren. Er ließ sich jedoch nicht einschüchtern, sondern gründete auf diesen Vorfall hin den Verein *NSA-Spion-Schutzbund*, der sich jede Woche »zum Spazieren, gemeinsamen Studieren und Erforschen der sehr scheuen NSA-Spione und deren Lebensraums« trifft. Mit diesen Aktionen will Bangert gegen die staatliche Vorratsdatenspeicherung in Deutschland protestieren.

Denn um die Sicherheit der Bürger zu gewährleisten und Verbrecher online sowie offline zu verfolgen ist zwar immer ein gewisser Zugriff auf Daten notwendig, aber dies sollte nur im begründeten Ausnahmefall geschehen. Vor 30 Jahren demonstrierten die Einwohner der BRD noch vehement gegen eine Volkszählung, weil sie sich dadurch in ihren Grundrechten eingeschränkt fühlten. Und heute? Laut einer FORSA-Studie von Januar 2017 sprachen sich ganze 80 Prozent der Berliner sogar für mehr Überwachungskameras aus – das subjektive Sicherheitsgefühl, welches Überwachung vermitteln will, scheint uns zu beruhigen. Die Message der gelben Sticker-Hinweise »Video – zu Ihrer Sicherheit« in den Berliner U- und S-Bahn-Stationen und den Zügen scheint anzukommen.

VERHÄLTST DU DICH DA ETWA KRIMINELL?

Dabei vermitteln Kameras schnell ein falsches Sicherheitsgefühl: Sie helfen beim Aufspüren von Tätern, können aber keine Straftaten verhindern. 2015 führte bei einem Drittel der Festnahmen in Berlin eine Videoaufzeichnung zum Täter: »Der abschreckende Effekt wird aber stark überschätzt«, warnte Berlins früherer Datenschutzbeauftragter Alexander Dix. Von insgesamt 14.765 Kameras im öffentlichen Raum der Hauptstadt filmen 13.643 das Geschehen in U- und S-Bahnen, laut Berichten von Netzpolitik.org sind das 30 Stück pro Bahnhof. Dennoch stieg die Anzahl der Kriminalitätsdelikte in Nahverkehrszügen von 2.201 in 2015 leicht auf 2.241 Delikte im Jahr 2016 an. BKA, BMI, die *Deutsche Bahn* (DB) und die *Bundespolizei* wollen jedenfalls diesen Weg weitergehen und setzen in Zukunft »intelligente« Überwachung auf Bahnhöfen ein.

An der Berliner S-Bahn Station Südkreuz wird im Herbst 2017 ein sechsmonatiges Pilotprojekt dazu gestartet, inklusive Gesichts- und Verhaltenserkennung. Zur Probe gleichen die Videokameras ihre Aufnahmen mit Fotos und Verhaltenstests von Freiwilligen ab – zum Beispiel deutet ein häufiges Hoch- und Runterlaufen einer Treppe auf Taschendiebe hin. Ist etwas auffällig, löst die Kamera einen Alarm aus und die Polizei kann sofort einschreiten. Die *Berliner Morgenpost* berichtet zudem, dass sich die Bahn erhofft, Graffitisprayern auf die Spur zu kommen. Auf eine Datenbank wird bei diesem Test noch nicht zurückgegriffen, denn das Bundesinnenministerium prüft noch, ob die intelligente Videoüberwachung mit den Grundrechten vereinbar ist. Normale Passanten am Südkreuz können laut offiziellen Angaben der intelligenten Videoüberwachung leicht aus dem Weg gehen, da die einzelnen Stellen gekennzeichnet sein werden.

WO WERDEN WIR EIGENTLICH ÜBERWACHT?

ÖFFENTLICHE PLÄTZE

Videokameras gibt es in den meisten öffentlichen Verkehrsmitteln, an Bahnhöfen und an öffentlichen Plätzen. Darüber hinaus natürlich in Läden, Banken und oft auch in Häuserkomplexen und Tiefgaragen.

INTERNET

Browserverlauf, Social-Media-Bilder und E-Mail-Verkehr. Es gibt kaum einen Bereich im Internet, der nicht Daten sammelt, sie analysiert und sogar verkauft. Diese Daten sind heiß begehrt von Unternehmen, Meinungsforschungsinstituten, BND, LKA und NSA.

HANDY

Dein Handy ist wie eine Wanze, die Du ständig mit Dir trägst. Über GPS weiß man, wo Du wie lange warst. Apps können oft auf Deine Telefonkontakte, Deine Speicherkarte oder Deine Fotos zugreifen und kennen darüber hinaus Deine Interessen, zum Beispiel Meditation und Deinen Fitness-Status über Health-Apps.

ONLINE-SHOPPING UND BARGELDLOSES ZAHLEN

Welche Lebensmittel und Kleidung wir kaufen, wie viel Alkohol wir in einer Bar konsumieren – all das kann theoretisch gesammelt, gespeichert und ausgewertet werden. Sehr interessant wären diese Daten natürlich für Krankenkassen und Kreditinstitute.

SMART HOMES

Kühlschränke, Mikrowellen, Türsensoren, Kameras, Kaffeemaschinen, Fernseher, Drucker – fast alle Deine Einrichtungsgegenstände könnten Dich überwachen, sobald sie WLAN haben.

ICH WEISS, WAS DU TUN WIRST

Präventive Sicherheitspolitik ist scheinbar das übergreifende Ziel der massenhaften Datenspeicherung und Überwachung von *CAPER* & Co. Wird eine Dystopie, wie man sie bisher nur aus Science Fiction Filmen wie »Minority Report« kannte, bald Wirklichkeit? Dreht sich die rechtliche Unschuldsvermutung um und jeder Bürger gilt per se

als potentieller Gefährder, der vorsorglich überwacht werden muss? In diesem Szenario muss der Einzelne erst durch regelkonformes Verhalten, das keine Anomalien aufweist, seine Unschuld beweisen – und zwar nicht nur einmal, sondern in einem fortlaufenden Prozess. Mit intelligenter Videoüberwachung werden in Zukunft Algorithmen und keine Menschen mehr entscheiden, wer verdächtig ist: Das individuelle Verhalten wird damit gleichgeschaltet, denn Abweichungen von der Norm sind suspekt.

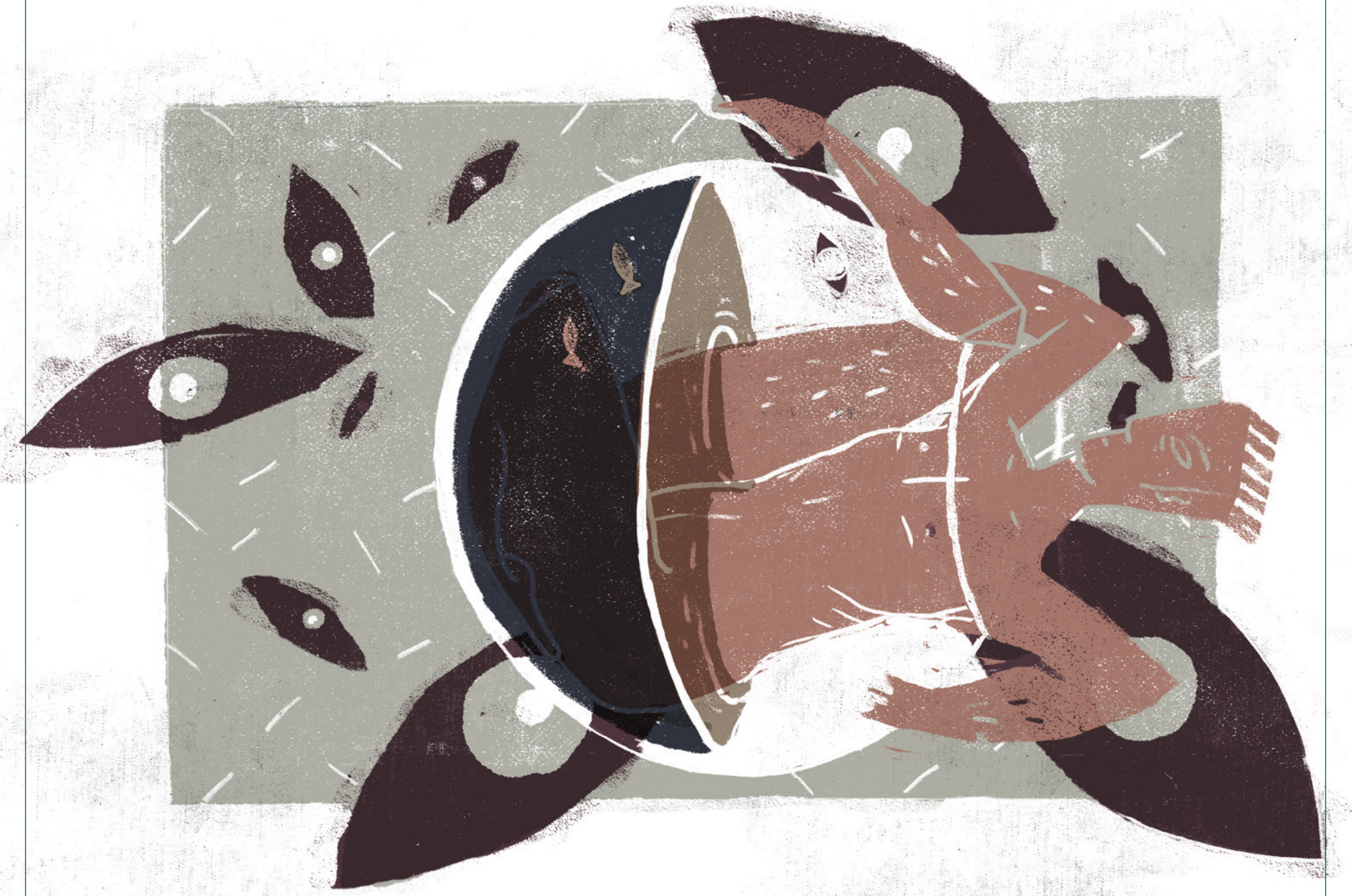
WENN UNSER STAAT WILL, IST ER JEDERZEIT IN DER LAGE, ALLES ÜBER UNS HERAUSZUFINDEN.

Von dieser Dystopie scheinen wir heute in Deutschland noch weit entfernt. Denn dass der deutsche Staat alles über uns weiß, ist – angesichts der reinen Datenmenge – noch nicht möglich. Die Strategie der Nachrichtendienste, alle Bürger vorsorglich unter Generalverdacht zu stellen, indem sie ihre Daten sammeln und auswerten, geht aber in eine bedenkliche Richtung. Festzustellen bleibt: Wenn unser Staat *will*, ist er jederzeit in der Lage, alles über uns herauszufinden. »Wenn in diesem Land jemals ein Tyrann an die Macht käme, dann könnten die technologischen Möglichkeiten, die die Geheimdienste der Regierung bieten, ihr zugleich ermöglichen, uns eine totale Diktatur aufzuzwingen und es gäbe dann keine Möglichkeit mehr, dagegen zu kämpfen«, warnte der amerikanische Senator Frank Church schon im Jahr 1975. Wir vertrauten bisher auf den Rechtsstaat, der uns vor dieser Dystopie beschützt. Aber warum sollten wir einem Staat vertrauen, der uns, jedem einzelnen, ohne Anlass misstraut? •

Julia Stürzl wollte als kleines Mädchen Journalistin werden – also noch unrealistischer als Bundeskanzlerin. Nach ein paar Irrungen & Wirrungen im Agenturleben hat sie aber den Notausgang gefunden und macht heute ein Volontariat bei QIEZ.de, schreibt einen eigenen Blog (Rucksack-pack) und für Perspective Daily. Ihr gefällt es, das Haushaltsbudget ihrer Freunde zu überwachen: »Dafür willst Du Geld ausgeben?!«.

ZUM WEITERLESEN

Rufin, Jean-Christophe: Globalia (2004)



VON PARANOIA BIS VERFOLGUNGSWAHN

ANGST IM ZEITALTER GLOBALER ÜBERWACHUNG

Edward Snowden hat nicht nur die Überwachungsmaßnahmen westlicher Geheimdienste verraten, er hat auch unsere Sicht auf den klassischen Verfolgungswahn verändert. Wir sind Subjekte einer Angstgesellschaft geworden, in der wir irrationale Ängste wahrnehmen und tatsächliche Bedrohungen ignorieren. Wie wirkt sich die allgegenwärtige Überwachung auf unser tägliches Denken und Handeln aus?

TEXT ROMAN OBST
ILLUSTRATION ANNE SELLING

Im Sommer letzten Jahres sorgte *Facebook*-Gründer Mark Zuckerberg unfreiwillig für einigen Spott, löste aber gleichzeitig eine Diskussion zu privater Netzsicherheit aus. Eigentlich wollte er mit einem Selfie an seinem Schreibtisch lediglich die 500 Millionen *Instagram*-Nutzer feiern. Im Hintergrund des Bildes war jedoch Zuckerbergs Laptop zu sehen – mit eindeutig erkennbaren Klebestreifen über Kamera und Mikrofon. Vor allem die *Twitter*-Gemeinde spottete über Zuckerbergs Maßnahmen zum Schutz seiner Privatsphäre, fragte sich aber auch, ob an der Gefahr allgegenwärtiger Überwachung nicht etwas dran sei, wenn selbst Zuckerberg solche Vorkehrungen treffe. Einige Wochen später unterstützte der damalige Direktor des Federal Bureau of Investigation (FBI) James Comey in einer Rede zu »Encryption and Surveillance« Zuckerbergs Maßnahmen und nannte sie eine prima Idee: »Weil ich gesehen habe, dass eine Person, die schlauer ist als ich, die Kamera abgeklebt hat.« Darüber hinaus, so ließ er wissen, sei das in US-Regierungsbüros längst üblich. Natürlich ist es verständlich, dass Leute wie Zuckerberg und der Chef des FBI zu allen Mitteln greifen, um sicherzustellen, dass ihre Gespräche im Büro nicht abgehört werden. Dabei bieten sich mit deren vorhandenen Ressourcen sicher noch ganz andere Möglichkeiten als das Abkleben von Kameras. Aber was ist mit uns?

SIND WIR NICHT ALLE EIN BISSCHEN PARANOIA?

Erstaunlich viele meiner Bekannten, darunter auch die Mehrzahl der Kater-Demos-Redakteure, kleben ihre Laptopkameras ab oder schalten den Ortungsdienst auf ihren Smartphones grundsätzlich aus. Hinter diesem Verhalten steckt häufig die Befürchtung, jemand könnte unsere digitalen Geräte hacken und uns mit der eigenen Kamera während privatester Momente beobachten. Zumindest wurde dies von meinem Bekanntenkreis als signifikant häufigste Erklärung angebracht. Dabei ist die Wahrscheinlichkeit, dass sich ein global agierendes Hackerkollektiv für unser Privatleben interessiert, vergleichsweise gering. Immerhin schätzt die relative Mehrheit der Befragten dies genauso ein. Mit den Szenen unseres häuslichen Alltags lässt sich eben weniger Geld verdienen als mit der Erpressung multinationaler Konzerne und der Bedrohung ihrer Netzinfrastruktur. Statt uns darüber Gedanken zu machen, sollten wir uns eher fragen, wann wir zuletzt das Passwort für unser Online-Banking geändert haben. Eine irrationale Angst oder Überzeugung wird umgangssprachlich auch als Paranoia bezeichnet. Dabei sind sich die Menschen bewusst, dass ihre Ängste nur teilweise begründet sind. Im Zusammenhang von Überwachung und Digitalisierung kann man also auch von Überwachungsparanoia oder digitaler Paranoia sprechen. ▸

Diese irrationalen Ängste gegenüber Netztechnologien und ihren impliziten Möglichkeiten des Ausspähens beziehen sich für die meisten auf persönliche Endgeräte wie Laptop und Smartphone. Wir fürchten, jemand könnte in unseren privaten Raum eindringen, uns beobachten und ausspähen, ohne dass wir Kenntnis davon haben. Doch obwohl wir in unserer unmittelbaren Umgebung zu Vorsichtsmaßnahmen wie Klebestreifen greifen, haben die meisten verhältnismäßig wenig Bedenken gegenüber anderen Überwachungsmethoden – insbesondere vor jenen im öffentlichen Raum. Das Ganze ist vergleichbar mit den irrationalen Ängsten aus unserer Kindheit wie zum Beispiel der Angst, aus dunklen Ecken von Monstern und Ungeheuern beobachtet und belauert zu werden – sei es beim Einschlafen oder beim Gang in den Keller. Später haben wir gelernt, mit solchen Ängsten umzugehen. Als Erwachsene lassen wir uns nicht mehr so leicht von unserer eigenen Fantasie einschüchtern. Mit unserer digitalen Paranoia sind wir offensichtlich noch nicht so weit, uns auf die wahrscheinlicheren Bedrohungen zu konzentrieren. Dass wir als Erwachsene aber ebenso irrationale Ängste spüren, ist nicht ungewöhnlich.

DIE DEUTSCHE ANGSTGESELLSCHAFT

Den Soziologen zufolge leben wir in der westlichen Welt gegenwärtig in einem Zeitalter der Angst. Heinz Bude, Professor für Makrosoziologie an der Universität Kassel, hat über »Die Gesellschaft der Angst« 2014 ein lesenswertes Buch geschrieben. Angst, so sagt er mit den Worten von Niklas Luhmann, sei heutzutage »vielleicht das einzige Apriori, auf das sich alle Gesellschaftsmitglieder einigen können«. Sie kenne keine sozialen Grenzen und erstrecke sich über alle Lebensbereiche. Alles sei offen, aber nichts ohne Bedeutung. Der moderne Mensch mit Internetanschluss und Smartphone glaube daher in jedem Moment, mit dem ganzen Leben zur Disposition zu stehen.

Und unsere Angst wird immer schlimmer – mit einem Anstieg um zehn Prozent im letzten Jahr! Denn »2016 war das Jahr der Angst« – zu dieser effektvollen Schlussfolgerung kamen die Autoren der letzten Befragungsrunde der Langzeitstudie »Die Ängste der Deutschen«. Seit 25 Jahren befragt das Infocenter der R+V Versicherung einmal im Jahr rund 2.500 Menschen aus Deutschland zu ihren Ängsten. Demnach dominiert seit den Anschlägen in Paris und Brüssel in unserer Gesellschaft die Angst vor Terrorismus und Zuwanderung. Drei Viertel aller Deutschen (73 Prozent) fürchten sich davor, Opfer eines Terroranschlags zu werden. In den Jahren davor waren es noch die EU-Schuldenkrise und steigende Lebenshaltungskosten. Der Angstindex, also der Durchschnitt aller abgefragten Themen, stieg 2016 um besagte zehn Punkte. Es ist bemerkenswert, dass die Studie bisher keinerlei Fragen zu Digitalisierung, Vernetzung und Freiheitsrechten stellt. Dabei wäre es zumindest wissenswert, ob neben der zunehmenden Terrorangst beispielsweise auch eine Furcht vor zu viel staatlicher Kontrolle besteht. Schließlich sollten wir wissen, welches von beiden Übeln uns mehr stört, wenn wir unsere Freiheitsrechte zur Abwehr von Terrorgefahren einschränken.

DIGITALE SELBSTZENSUR

Einen ersten Eindruck, was Überwachungsangst mit unserer Fähigkeit zur Meinungsbildung anstellen kann, liefern die Ergebnisse einer Studie aus dem letzten Jahr: Demnach sind Menschen, die den Eindruck haben, bei der Internetnutzung von staatlichen Sicherheitsbehörden überwacht zu werden, weniger bereit, ihre Meinung zu äußern, wenn sie der wahrgenommenen Mehrheit widerspricht. Zu dieser Folgerung kommt Elizabeth Stoycheff von der Wayne University in Detroit in ihrer Studie »Under Surveillance« (2016). Die US-amerikanische Kommunikationswissenschaftlerin bat die Teilnehmenden ihrer Online-Studie um deren Meinung zu einem US-amerikanischen Bombenangriff auf Ziele der Terrororganisation des sogenannten Islamischen Staates (IS) im Irak. Der Hälfte der Befragten gab sie den zusätzlichen Hinweis, es könne nicht gewährleistet werden, dass die sonst vertraulichen Antworten nicht von der National Security Agency (NSA) registriert würden. Die Mehrheit dieser Personen artikulierte ihre Meinung daraufhin deutlich zurückhaltender.

In einem Podcast-Interview sagte die Autorin, ihrer Ansicht nach sei die gesamte Debatte um Terrorabwehr und den Schutz unserer Freiheitsrechte in eine Schieflage geraten. Das Thema Terrorismus werde ständig mit besorgniserregenden Statistiken und Zahlen präsentiert und Überwachung dabei als einfache Lösung angeboten. »Wir müssen beginnen, uns zu fragen, welche grundlegenden psychologischen Auswirkungen es auf unser politisches Denken und Handeln hat, wenn Regierungen diesen unbegrenzten Zugang zu all unseren Daten haben«, fordert Stoycheff. Die Studie zeige, dass Selbstzensur in unserer Gesellschaft stattfindet, sogar »wahrscheinlich in weiten Teilen der Bevölkerung«. Staatliche Überwachung kann also dazu führen, dass Menschen von ihrer Meinungsfreiheit nur noch eingeschränkt Gebrauch machen. Besonders stark war dieser Effekt übrigens bei Befürwortern der Internetüberwachung. Diese verhielten sich konformistischer und übten vorauseilende Selbstzensur aus, während die Minderheit der ausdrücklichen Überwachungsgegner vom Meinungsklima und der Überwachungsdrohung vergleichsweise unbeeindruckt blieb.

DIGITALE PARANOIA

»Die Ergebnisse dieser Studie stehen im Widerspruch zu der Behauptung, das Internet trage zu einer Demokratisierung der Gesellschaft bei«, urteilt auch der Berliner Psychiater Jan Kalbitzer. Er forscht am »Zentrum für Internet und seelische Gesundheit« der Berliner Charité und arbeitet als Psychotherapeut in seiner eigenen Praxis. Kalbitzer veröffentlichte Ende letzten Jahres ein Buch mit dem Titel »Digitale Paranoia«. Darin beschreibt er aus psychiatrischer Sicht, wie es uns gelingen könne, »online zu bleiben, ▸

ohne den Verstand zu verlieren«. Durch die Arbeit mit seinen Patienten bildete er den Begriff der »Digitalen Paranoia« heraus. Dieser beschreibt unser irrationales Verhältnis zum Internet, dem Kalbitzer oft bei ratlosen Patienten begegnete. Wenn man bedenkt, dass das Internet nur eine Erscheinung der digitalen Vernetzung ist, lassen sich einige von Kalbitzers Überlegungen durchaus auf unsere Überwachungsparanoia übertragen.

Die umgangssprachliche Paranoia, die unsere irrationalen Ängste beschreibt und die Kalbitzer in seinem Buch hauptsächlich behandelt, müssen wir abgrenzen von der Paranoia im psychiatrischen Sinne. Diese psychiatrische Paranoia ist eine wahnhafte Überzeugung, die häufig mit einer Psychose oder Schizophrenie einhergeht. Kalbitzer zufolge liegt die Grenze zwischen irrationaler Angst und einer wahnhaften Psychose dort, wo die realistische Einschätzung nicht mehr richtig funktioniert. Solange wir also noch mitbekommen, dass unsere irrationalen Ängste zumindest teilweise unbegründet sind, können wir von einer umgangssprachlichen Paranoia sprechen. Was aber geschieht mit uns, wenn wir irgendwann nicht mehr wissen, was richtig und was falsch ist, und unsere Überwachungsangst zum Überwachungswahn wird?

DIE PARANOIA DES PSYCHIATERS

Gregor S. (Name der Redaktion bekannt) kann den Moment noch genau beschreiben, als die Psychose über ihn hereinbrach – vor drei Jahren an einem malerischen Strand in Südostasien, fernab von allen vernetzten Geräten und Kameras, die in den darauffolgenden Wochen seine Wahnvorstellungen beherrschen sollten. Gregor ist ein fröhlicher Kerl, der bisweilen recht lange überlegt, bevor er einen einfachen Satz ausspricht. Er reist sehr gerne und hätte damals, vor drei Jahren, eigentlich immer so weitermachen können. Doch zu Hause war sein Leben vor allem von Erwartungshaltungen und ständiger Erreichbarkeit geprägt. Genau davor hatte er Angst. »Auf dem Rückweg war es dann einfach passiert«, erinnert sich Gregor. »Plötzlich war die Psychose da. Ich habe es körperlich gespürt und ich wusste, dass ich krank bin.« Aber kontrollieren konnte er es nicht. Die Heimreise sollte für ihn rückblickend zum Alptraum werden.

»Ehrlich gesagt interessiere ich mich nicht besonders für Politik«, gibt er zu. Dennoch checkt er selbst auf längeren Reisen jeden Morgen die Nachrichten. Ihm sei es wichtig, informiert zu sein. So auch 2013, als nach den Enthüllungen von Edward Snowden auf dem Höhepunkt des NSA-Skandals immer weitere Informationen zum Ausmaß der Internetüberwachung bekannt wurden. »Ich war plötzlich überzeugt davon, von allen Seiten überwacht und beobachtet zu werden. Vor jeder Kamera habe ich versucht, mich so normal wie möglich zu verhalten. Ich dachte, die Behörden wären ständig über jeden meiner Schritte informiert.« Selbst Menschen, die einfach mit ihren Handys auf der Straße telefonierten, waren für ihn verdächtig. Wovor er Panik hatte? »Dass man mich eines Verbrechens beschuldigen könnte, das ich nicht begangen habe. Ich hatte vor allem Angst, dass man meine Situation ausnutzt. Das wirklich Verrückte war, dass ich wusste, ich habe eine Psychose, die ich aber für keinen Augenblick mit dieser irren Verfolgungsangst in Verbindung bringen konnte.«

Diese wahnsinnige Flucht vor den unsichtbaren Sicherheitsbehörden dauerte zwei Wochen, in denen er teilweise sogar auf der Straße lebte. Schließlich gelang es ihm in einem geistig klaren Moment, eine E-Mail an seine Angehörigen und Freunde abzusetzen, die ihn in einer abenteuerlichen Aktion aus Bangkok abholten und zurück nach Deutschland zur Behandlung in eine psychiatrische Klinik brachten. Heute sagt Gregor mit gesundem Abstand: »Ich habe in der Klinik viele Menschen getroffen, die an einem ähnlichen Verfolgungswahn gelitten haben wie ich und dabei von der Angst vor Geheimdiensten und Überwachungstechnik getrieben wurden.« Er versucht das Erlebte rückblickend mit einer modernen »medialen Urangst« zu erklären, die ihn damals verfolgt habe. Schließlich hätte er auch Angst vor Außerirdischen haben können, vor seinem eigenen Schatten oder dem Allmächtigen. Aber in seinem Wahn wählte er als »Thema« seiner Psychose die Sicherheitsbehörden und die allgegenwärtigen Überwachungstechniken. »Die Überwachung und das Politische dahinter formen unser Denken bis ins Unbewusste«, resümiert er nachdenklich. Es ist wichtig festzustellen, dass Gregor kein Anhänger kruder Verschwörungstheorien ist und niemals war. Er ist seit dem Vorfall gesund und versorgt sich über das Internet weiterhin kritisch, aber unaufgeregt mit Informationen – wie die meisten von uns.

DIE WIRKLICHKEIT KOMMT

Anders geht es den Menschen, die der Filmemacher Niels Bolbrinker in seiner Dokumentation »Die Wirklichkeit kommt« aus dem Jahr 2014 begleitet hat. Darin lässt er Menschen mit Verfolgungswahn und Verschwörungstheoretiker sprechen und beobachtet, wie sich ihre Ängste zu unserer gegenwärtigen Realität verhalten. Da ist der legendäre »Sendermann«, der bereits in den 1970er-Jahren auf den Straßen Berlins vor der Totalüberwachung durch die Central Intelligence Agency (CIA) warnte. Oder die ältere Frau, die ihr Leben ausschließlich auf Reisen verbringt, weil sie glaubt, man könne sie mit einem heimlich implantierten Mikrochip überall hin verfolgen. In einer Szene sagt sie angesichts der heutigen technischen Möglichkeiten fassungslos: »Es geht in die Richtung totaler Paranoia.« Dabei ist sie schon längst davon vereinnahmt. Die Psychiater nennen dieses Verhalten »paranoiden Technikwahn« – das Gefühl von unbekannten Kräften, Mächten und Technologien kontrolliert, manipuliert und terrorisiert zu werden. Bolbrinker gibt diese offensichtlich an Psychosen leidenden Menschen nicht der Lächerlichkeit preis. Doch je mehr er in der Nebenhandlung über die gegenwärtigen Überwachungsmethoden berichtet, desto weniger verrückt erscheinen ihm die zuvor geschilderten paranoiden Erzählungen. Wohl ein Grund, weswegen dem Film über weite Strecken die Distanz fehlt.

DIE ANGST VOR DER ÜBERWACHTEN GESELLSCHAFT

Eines wird dabei jedoch deutlich: Edward Snowden – da sind sich auch zahlreiche weitere Autoren einig – hat unser gesellschaftliches Verständnis gegenüber Verschwörungstheorien und Wahnvorstellungen verändert, zumindest soweit sie sich auf das Internet und Überwachungstechnologien beziehen. Hätte sich vor zehn Jahren jemand von ausländischen Geheimdiensten beobachtet gefühlt, wären wahrscheinlich Wahnvorstellungen vermutet worden. Heute ist das normal. Seit Snowdens Enthüllungen wissen wir, dass nicht nur ein enormer kommerzieller Datenhandel betrieben wird, sondern dass personenbezogene, zurück verfolgbare Daten auch an staatliche Geheimdienste weitergegeben, dort gesammelt, miteinander abgeglichen und auf Verdachtsmomente analysiert werden. Wir wissen, dass nicht nur radikale Tätergruppen abgehört werden, sondern wir alle. Der bereits erwähnte Soziologe Heinz Bude gehört zu den Initiatoren der »Charta der Digitalen Grundrechte der Europäischen Union«, die Ende November 2016 veröffentlicht wurde. Er sagt: »Aus dem Unbehagen über die ungebetene Werbung ist die Angst vor einem Großen Bruder geworden, der ununterbrochen aufzeichnet, was ich von transportablen Rechnern so alles von mir gebe« – eine Angst, die wir heute alle mehr oder weniger zu teilen scheinen.

WIE UNSERE PARANOIA IM DIGITALEN ZEITALTER ENTSTEHT

Wie Paranoia und ernst zu nehmender Verfolgungswahn im digitalen Zeitalter entstehen, hat sehr viel mit der Unübersichtlichkeit einer immer komplexeren Welt zu tun. Für die menschliche Psyche, so schreibt Psychiater Kalbitzer, gibt es kaum etwas Bedrohlicheres als das Gefühl »frei flotierender Angst«, also eines Zustandes ungerichteter Panik und haltloser Unsicherheit. Damit liegt er auf ganzer Linie mit Bude und dessen »Gesellschaft der Angst«. Eine zunehmend komplexe Welt versetzt uns in einen Zustand tiefer Verunsicherung. Die uns gebotenen Antworten sind naturgemäß komplizierter als die ihnen zugrunde liegenden Fragen. Für viele Menschen ist dies gleichbedeutend damit, gar keine Antwort zu bekommen. Die Psyche einiger Menschen flüchtet sich angesichts dieser Unsicherheiten – gleichsam eines Ventils – in Phobien und paranoide Überzeugungen. Der NSA-Skandal hat viele gesunde Menschen paranoid und zu Anhängern politischer Verschwörungstheorien werden lassen. Auf keinen Fall ist abschließend geklärt, was eine dauerhafte und allgegenwärtige Überwachung mit der Psyche des Menschen anstellt. Selbst die gut analysierten totalitären Regime des 20. Jahrhunderts hatten nicht die umfassenden Möglichkeiten, die den zahlreichen Geheimdiensten der modernen westlichen Demokratien heutzutage zur Verfügung stehen.

Wir müssen uns jedoch eingestehen, dass hinter unserer eigenen, eher harmlosen digitalen Paranoia sehr ähnliche Motive stecken wie hinter den paranoiden Ideen von Verschwörungstheoretikern. »Aus dieser Paranoia heraus verhalten wir uns irrational und verdrängen, dass die digitale Zukunft ein Gestaltungsprojekt ist, bei dem wir alle mit anpacken müssen, wenn wir wollen, dass sie unseren Bedürfnissen gerecht wird«, sagt Psychiater Kalbitzer. Wer aus Sorge vor einer Überwachung ausländischer Geheimdienste online keine Kochrezepte mehr suche, weiterhin als übermäßig ängstlich, so Kalbitzer weiter, wenn auch nicht unbedingt als wahnhaft. Was für Kochrezepte gilt, kann jedoch auch für eine kritisch reflektierte politische Teilnahme gelten. Wer nun nachts nicht mehr ruhig schlafen kann, weil er oder sie befürchtet, vom eigenen Mac beobachtet zu werden, dem empfiehlt sich das kleine Gratis-Tool »Oversight«, das der Ex-NSA-Mitarbeiter Patrick Wardle im Netz bereitstellt. Es überwacht die Nutzung von Webcam und Mikrofon und warnt, sobald eine Anwendung versucht, darauf zuzugreifen. Zumindest für den Mac konnte noch keine Malware dieser Art nachgewiesen werden. Das ist doch durchaus beruhigend. •

Roman Obst klebt seine Laptopkamera nicht ab. Das heißt natürlich auch nicht, dass er von jenen irrationalen Ängsten frei ist, die er in seinem Beitrag beschreibt. Er findet es nur schlimmer, ständig von einem kleinen Streifen Klebeband symbolisch daran erinnert zu werden, wie wenig Privatsphäre und Bürgerrechte in der digitalen Welt bisweilen wert sind.

ZUM WEITERLESEN UND -SCHAUEN

Jan Kalbitzer: Digitale Paranoia – Online bleiben, ohne den Verstand zu verlieren (2016)

Heinz Bude: Gesellschaft der Angst (2014)

Niels Bolbrinker: Die Wirklichkeit kommt (2014)

Elizabeth Stoycheff: Under Surveillance (2016)

IV IM SCHATTEN DER FREIHEIT

VON SYLVIA LUNDSCHIEN

Im vierten Teil des Roten Fadens geht es um schnüffeln, beschatten und abhören – denn das gab es doch nur in der DDR, oder? Aber auch die Bundesrepublik Deutschland griff seit 1950 massiv in die Privatsphäre ihrer Bürger ein und öffnete ausländischen Geheimdiensten Tür und Tor. Eine historische Skizze.

Privatsphäre? Da kann Joschka nur mit den Schultern zucken. Geboren 1948, verbringt er seine Jugend in einer engen Wohnung in der Nähe von Stuttgart. Mitte der sechziger Jahre kommt Joschka an die Frankfurter Universität. Fast überall wird gestritten, debattiert und demonstriert – über Abrüstung, Frauenrechte oder Atomkraft. Seine WG teilt er mit einem Dutzend Menschen. Hier kann jeder schlafen, wo er will und oft wird stundenlang im Hausplenum diskutiert. Besitz ist verpönt: Man »borgt« sich die Dinge – und manchmal auch den Partner. Joschka ist glücklich, denn allen geht es um die Befreiung von steifen Rollen hin zu mehr Selbsterfahrung.

Wer in den sechziger und siebziger Jahren in der BRD heranwächst, erlebt eine Zeit, in der immer mehr Menschen Zugang zu Bildung und die Möglichkeit zu reisen haben. Vieles, was lange als »tabu« oder »privat« galt, wird nun offen diskutiert und politisiert: Sexualität, Familie, Psychologie und Besitz. Getreu dem Motto »das Private ist politisch« werden Stereotype und moralpolitische Entscheidungen hinterfragt, die für viele heute Privatsache sind – wie zum Beispiel Homosexualität oder Abtreibung. Neue Interessengruppen debattieren sich die Köpfe heiß, zeigen sich demonstrativ in der Öffentlichkeit, fordern Transparenz und wollen dauerhaft verändern und mitbestimmen. Dabei geht es den meisten schlichtweg um die eigene Zukunft: Etwa ein Drittel der Bevölkerung ist Anfang der Siebziger jünger als 20 Jahre, 1990 ist es nur noch ein Fünftel.

»AUF GOTT VERTRAUEN WIR, ALLE ANDEREN HÖREN WIR AB«

Christopher McLarren, von 1973 bis 1975 US-Army-Geheimdienstmitarbeiter in der Abhöranlage auf dem Berliner Teufelsberg

Während die deutsche Nachkriegsgesellschaft ihre Tabus allmählich hinterfragt, ist das Bundesamt für Verfassungsschutz (BfV) jedoch längst aktiv. Gegründet 1950, befasst es sich mit der Verfolgung von verfassungsfeindlichen und terroristischen Aktivitäten auf dem Gebiet der BRD. Die Kanzler der BRD erlauben den amerikanischen, britischen und französischen Alliierten, die deutsche Bevölkerung zu überwachen, wovon heute noch die verfallenen Abhörkuppeln auf dem Berliner Teufelsberg zeugen. Sie sind Teil eines der vielen Geheimprojekte, die im Westteil Deutschlands auch heute noch existieren und zum so genannten Spionagenetzwerk Echelon* gehören. Echelon war lange eine Legende, bis das europäische Parlament 2001 seine Existenz nachweisen konnte.

IM RASTER DER BEHÖRDEN

Durch das Abhören versprach man sich einen Wissensvorsprung gegenüber links- und rechtspolitischen Gegnern. Gleichzeitig wurde die Privatsphäre der BRD-Bürger eingeschränkt. Auch im westlichen Deutschland wurden massenweise Briefe geöffnet, Telegramme abgeschrieben und Telefongespräche mitgeschnitten – besonders wenn sie von der anderen Seite des Eisernen Vorhangs kamen.

*ECHELON

Das Echelon-Spionagenetzwerk wird den Nachrichtendiensten der USA, Großbritanniens, Australiens, Neuseelands und Kanadas zugeschrieben und soll die Satellitenkommunikation für Telefone, Faxe und das Internet überwachen. 2004 wurde eine von der NSA geführte Anlage im bayerischen Bad Aibling geschlossen. Das Netzwerk steht im Verdacht, über seine Anlagen Wirtschaftsspionage zu betreiben.

Die siebziger Jahre waren auch die Zeit der Rasterfahndung. Entwickelt wurde sie im Zuge des so genannten »Roten Herbst« 1977, als die linksextreme Rote Armee Fraktion (RAF) die Bundesrepublik durch Überfälle, Entführungen und Mord in eine Krise stürzte. Damals wie heute galt Terrorgefahr als Rechtfertigungsmittel, um Bürger zu durchleuchten. Die Rasterfahndung bedeutete, den Täterkreis anhand von bestimmten Personenmerkmalen systematisch zu verkleinern. Diese Methode führte zu Fahndungserfolgen und ist bis heute in Gebrauch – trotz Fehlschlüssen, Beschwerden sowie Skandalen um V-Personen und mangelhafter Behördenführung.

ZWISCHEN RELIGION UND VOLKSZÄHLUNG

Für Maxi spielt das in den Achtzigern kaum eine Rolle. Sie ist 1985 ein Teenager, lebt mit ihren Eltern in der Nähe von Hannover. Politik interessiert sie nicht. Das ändert sich im Frühling 1986, als im ukrainischen Kernkraftwerk Tschernobyl ein Reaktor explodiert. Wilde Spekulationen machen die Runde, schließlich lebt die Welt noch immer im Kalten Krieg. Anstatt sich politisch zu vernetzen, sucht Maxi Antworten im Spirituellen: Den Sommer verbringt sie beim ökumenischen Jugendtreffen im französischen Taizé, wo ein Brüderorden seit den 1960er Jahren eine Mischung aus Sommer-Festival und religiösem Dialog anbietet.

Die achtziger Jahre sind durch inneren Rückzug geprägt. Demonstrierten ehedem Hippies und Alt-Linke öffentlich und gemeinschaftlich, zieht sich der Protest jetzt zunehmend ins Private zurück. Esoteriker, Punks und Skinheads prägen die Zeit ebenso wie auch »Normalos«, die für Frieden und Umweltschutz protestieren. Seit Ende der siebziger Jahre sind gut zwei Drittel der BRD-Bevölkerung gegen den Einsatz von Atomkraft und den Bau neuer Kernkraftwerke.

1987 wird schließlich die Volkszählung in der BRD durchgeführt, denn der Staat will wissen, wie viele Kindergärten, Buslinien oder Trinkwasserleitungen die Bevölkerung braucht. Eigentlich ganz praktisch. Doch die Volkszählung ist aufgrund unvollständiger Anonymisierung der Daten umstritten. Bereits 1983 wurde zunächst zu Boykott und Sabotage der damaligen Volkszählung aufgerufen, später erfolgreich geklagt: Das Bundesverfassungsgericht fällt erstmals eine Grundsatzentscheidung in Sachen informationeller Selbstbestimmung. Die Bürger haben fortan gegenüber dem Staat ein Grundrecht auf Anonymität und Datenschutz.

DER ROTE FADEN

DIE DIGITALE SCHNÜFFELEI BEGINNT

Melanie hat als Zwölfjährige nichts von der damaligen Volkszählung mitbekommen. 1996 ist das längst vergessen und die Welt hat sich verändert: Die Mauer ist weg, Melanie studiert Politik an der Freien Universität Berlin und absolviert gerade ein Praktikum beim Kiez-Politiker Joschka Bäcker. Überwachung? Gibt's doch nur noch in alten Filmen und Erzählungen über die Stasi. Der Staat muss sich jetzt an Gesetze halten, und was sollte man schon über einfache Bürger herausfinden wollen? Zum Geburtstag bekommt Melanie von ihren Eltern ein Nokia-Handy geschenkt, damit sie sich öfter meldet. An der Uni hat sie auch zum ersten Mal eine eigene E-Mail-Adresse, was ziemlich praktisch ist, wenn man mit den Dozenten und Erasmus-Studenten aus Frankreich in Kontakt bleiben will.

In den nächsten 25 Jahren wird die Welt vernetzter und internationaler. Verletzung der Privatsphäre durch Geheimdienste klingt für viele bis heute wie ein Horrormärchen aus dem Kalten Krieg: Man denkt an verwanzte Wohnungen oder Ermittler im Trenchcoat. Doch derartige Methoden sind oft nicht mehr nötig, denn die Bevölkerung hilft zunehmend selbst dabei mit, sich überwachen zu lassen: Grund dafür ist der Einzug von PC, Handy und E-Mail in fast allen Haushalten. Dass sich damit immer neue Möglichkeiten zur Überwachung der Bürger durch in- und ausländische Geheimdienste ergeben, wird spätestens mit der NSA-Affäre 2013 deutlich, deren Aufarbeitung und Auswirkungen bis heute nicht restlos geklärt sind. Doch der Schock war auch heilsam: Selten wurde so häufig über Datenschutz und -sicherheit gesprochen wie in der Gegenwart. •

ZUM WEITERLESEN

Josef Foschepoth: Überwachtes Deutschland. Post- und Telefonüberwachung in der alten Bundesrepublik (2013)

FUNKSENDER IN TEDDYBÄREN

Unter ihrem Pseudonym Ruth Werner ist Ursula Beurton (geb. Kuczynski) in der DDR mit »Sonjas Rapport«, dem Bericht über ihre Zeit als sowjetische Top-Spionin, zu großer Berühmtheit gelangt. Ihre Übergabe der Baupläne für die US-amerikanische Atombombe an die Sowjets hat entscheidenden Einfluss auf den Verlauf des Kalten Krieges genommen. Drei Kinder zieht sie während ihres geheimen Wirkens auf. Eines davon ist Michael Hamburger – mein Großvater.

TEXT EVA PALM
FOTOS AUS DEM PRIVATBESITZ VON MICHAEL HAMBURGER

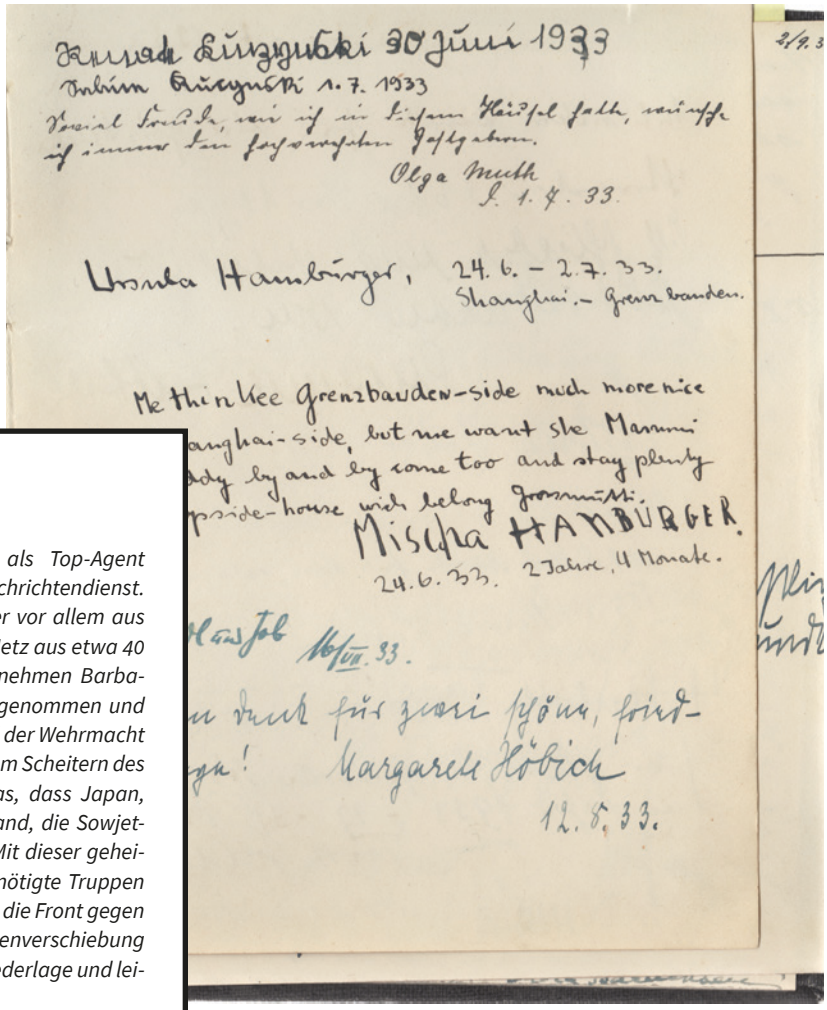
Meine Urgroßmutter, die sowjetische Agentin ›Sonja‹, wäre in diesem Jahr 110 Jahre alt geworden. Am 15. Mai 1907 wird sie als Ursula Maria Kuczynksi in Berlin-Schöneberg geboren. Als Tochter von progressiv eingestellten jüdischen Intellektuellen wächst sie in einer Villa am Schlachtensee auf – dennoch in relativ bescheidenen Verhältnissen und mit engem Kontakt zum Arbeitermilieu. Schon früh entwickelt sie einen starken Sinn für Klassengerechtigkeit, liest voller Begeisterung Bücher von kommunistischen Ideengebern und tritt dem Kommunistischen Jugendverband bei. Es folgt eine sich rasch entwickelnde Karriere im Geheimen – als Agentin im Auftrag des damals sowjetischen, heute russischen Militärnachrichtendienstes GRU.

Ihr Sohn Michael, mein späterer Großvater, erfährt von ihrem besonderen Lebenslauf erst kurz vor der Veröffentlichung ihres ersten Buches »Ein ungewöhnliches Mädchen«. Dabei ist er bereits seit seiner Geburt mitten im Geschehen: Ursula Maria Kuczynksi heiratet 1929 den deutschen Architekten Rudolf Hamburger. In Shanghai, wo sich seine Eltern seit Anfang der 1930er Jahre aus beruflichen Gründen aufhalten und er zur Welt kommt, ist die kommunistische Partei illegal und ihre Anhänger werden erbarmungslos verfolgt. In den chinesischen Provinzstädten hängen Köpfe auf Pfählen neben den Stadttoren, um vor umstürzlerischen Aktivitäten abzuschrecken. Parallel dazu werden im oberen Stockwerk des Hauses der Familie Hamburger illegale Treffen von Richard Sorge* und seinen Genossen abgehalten. Für deren Geheimhaltung trägt die junge Mutter Sorge, während der kleine ›Micha‹ nebenan in der Wiege liegt. In den frühen Jahre ihrer Spionagetätigkeit wirkt die kommunistische Agentin mit dem Decknamen »Sonja« zwischen Windeln wechseln und Hausarbeit.

Die Treffen in dem Haus in Shanghai finden zwischen 1930 und Ende 1932 statt. Richard Sorge traut Kuczynski im Laufe dieser Zeit mehr und mehr Aufgaben zu: von Wache halten während der Treffen, über Abtippen geheimer Dokumente, bis zu Botengängen. Von einem Mitglied der Gruppe wird das Nachrichtenmaterial in einem Fotoladen auf Kleinfilme kopiert. Was heute unspektakulär klingt, ist damals die hohe Kunst der Spionage. Alles dreht sich um geheime Dokumente, Berichte, Analysen und deren Übermittlung. Wer im Spiel der politischen Mächte die geheimen Informationen zuerst in seinen Händen hält, kann auch als erstes handeln.

Auch Sohn Michael und ihr erster Mann Rudolf Hamburger lernen die Genossen kennen – allerdings als Freunde, Lehrer und Bekannte der Familie. Schließlich kennen sich die meisten Europäer in der asiatischen Großstadt ohnehin.

Heute erzählt mir mein Großvater mit Blick auf seine ungewöhnliche Kindheit: »Ich habe relativ früh schon be-



*DR. RICHARD SORGE

Dr. Richard Sorge arbeitet ab 1933 als Top-Agent »Ramsay« beim sowjetischen Militärnachrichtendienst. Getarnt als deutscher Journalist funkt er vor allem aus Japan. Durch ein von ihm aufgebautes Netz aus etwa 40 Informanten kann er vor Hitlers »Unternehmen Barbarossa« warnen, wird jedoch nicht ernst genommen und es kommt zum verhängnisvollen Überfall der Wehrmacht auf die Sowjetunion. Als Richard Sorge vom Scheitern des Antikominternpakt erfährt, bedeutet das, dass Japan, entgegen der Abmachung mit Deutschland, die Sowjetunion doch nicht anzugreifen gedenkt. Mit dieser geheimen Nachricht kann Stalin dringend benötigte Truppen aus dem weiten Sibirien abziehen und an die Front gegen die Wehrmacht schicken – diese Truppenverschiebung führt 25 km vor Moskau zur deutschen Niederlage und leitet somit die Kriegswende ein.

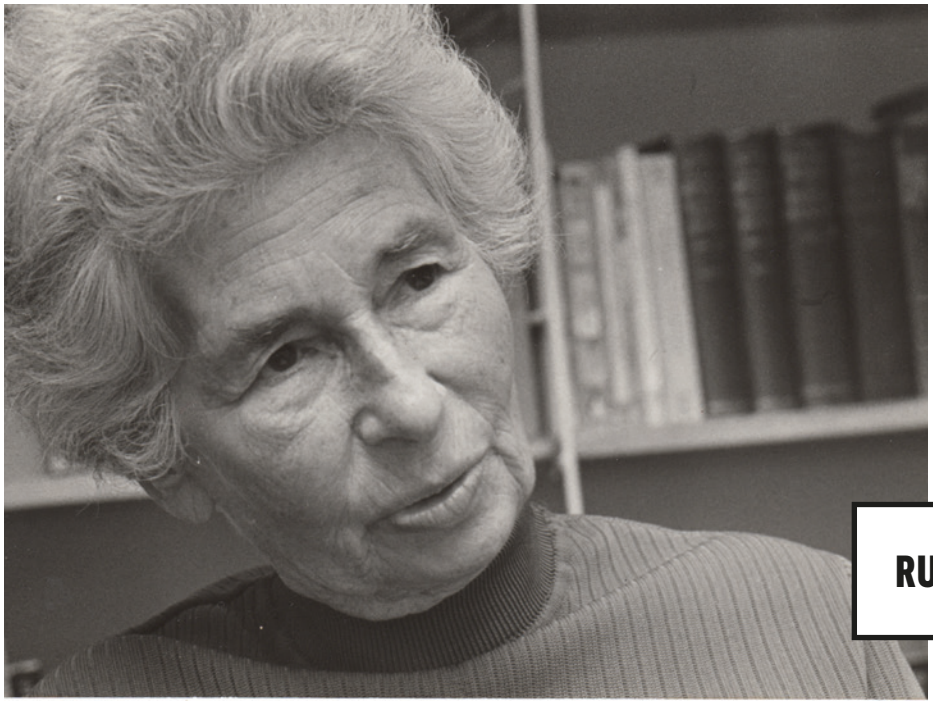
merkt, dass ich aus einem Teil des Lebens meiner Mutter völlig ausgeschlossen war. Wenn Bekannte kamen, musste ich irgendwann immer den Raum verlassen. Ich hätte gern noch weiter mit denen geredet oder gespielt, doch ich wurde weggeschickt. Dann wurde im Wohnzimmer gesprochen und diskutiert und ich durfte nicht mitmachen.«

Dieses Verhalten der Mutter erweist sich später als begründete Sorge um das Kind: Einmal empfiehlt ihr Richard Sorge, vorsichtshalber die Koffer zu packen, denn es könne sein, sie müssten jeden Augenblick fliehen. Ein anderes Mal bringt sie Tee ins obere Stockwerk und überrascht die Männer bei der Inspektion etlicher Waffen. Die Gefahr entdeckt zu werden ist damals allzeit gegenwärtig. Seine Mutter trinkt keinen Kaffee oder Alkohol und härtet sich körperlich ab – auf eine drohende Verhaftung will die Agentin »Sonja« jederzeit vorbereitet sein.

Scheinbar ganz nebenbei meistert sie ihre Rolle als Mutter: Selbst als der Krieg zwischen Japan und China auch Shanghai erreicht und viele verfolgte Kommunisten und Flüchtlinge im Hause Hamburger unterkommen, wird Michas erster Geburtstag gefeiert.

Schon kurz darauf steht der erste Umzug für den kleinen Michael an. Seine Mutter bringt ihn zu den Großeltern, die im Riesengebirge in der Tschechoslowakei leben. Denn »Sonja« beginnt auf Empfehlung Richard Sorges eine Ausbildung zur Agentin – an einer Spionageakademie in Moskau. Dorthin darf ihr Sohn nicht mitkommen, schließlich könnte er fortan bei dem Aufenthalt in der Sowjetunion ausreichend Russisch aufschnappen, um anschließend mit einem unbedachten Wort kritische Informationen oder die wahre Identität seiner Mutter auszuplappern.

Fortan gehören ständig neue Begegnungen und wechselnde Abschiede zum jungen Leben meines Großvaters. »Ich hielt das lange für relativ normal«, sagt er heute. »Aber ich habe dann auch entdeckt, dass es gewisse Spuren an mir hinterlassen hat, dass ich keine kontinuierliche Entwicklung nehmen konnte. Denn ich fasste nie richtig Wurzeln oder konnte mich als Teil von festen sozialen Gruppen fühlen.« ►



RUTH WERNER

Und während Michael und der Rest der Familie denken, es ginge um einen gesunden Klimawechsel, lernt seine Mutter Funksender zu bauen, das Morsealphabet kennen und weitere Kenntnisse des Spionagehandwerks, die für ihre Arbeit notwendig sein werden. Im Februar 1934 beginnt die erste Mission: Sie soll gemeinsam mit einem deutschen Genossen nach Mukden, in die Mandschurei im Norden Chinas, gehen – und diesmal mit Michael. Die Agentin »Sonja«, geborene Kuczynski, verheiratete Hamburger, willigt pflichtbewusst ein. Doch der junge Michael ist davon gar nicht begeistert, aus der Geborgenheit der Großeltern für eine Reise ins Ungewisse entrissen zu werden. Das Vertrauen zwischen Mutter und Kind hat gelitten und auch die Strapazen der langen Fahrt verträgt der Junge nicht gut. »Nach dem Aufenthalt in der Tschechoslowakei sind wir mit dem Schiff gefahren, ich hatte eine Riesenangst, dass wir untergehen und bekam Keuchhusten.«

Während eines kurzen Zwischenstopps in Shanghai beschließen Ursula Kuczynski und ihr erster Mann sich voneinander zu trennen. Doch zum Schutz beider lassen sie sich nicht offiziell scheiden. Während mein Urgroßvater, der deutsche Architekt Rudolf Hamburger, in Shanghai zurückbleibt, fahren Kuczynski, der gemeinsame Sohn Michael und ein die beiden begleitender Genosse weiter in die Mandschurei. Doch noch bevor sie in Nordchina ihre geheime Arbeit aufnehmen können, entgehen sie nach der Ankunft nur knapp den Grenzkontrollen, als Teile für einen Funksender beinahe aus einem Sessel fallen, den sie in ihrem Hausrat dabei haben.

Am Zielort beginnen sie chinesische Widerstandsgruppen zu Partisanengruppen auszubilden und zu Aktionen anzuleiten. Kuczynski funkt mehrmals wöchentlich aus ihrem Zuhause mit der Zentrale in der Sowjetunion – immer nachts, während nebenan der ahnungslose Michael schläft. Dabei nimmt sie die geheimdienstlichen Anweisungen entgegen, um die Abläufe mit den verschiedenen Gruppen vor Ort zu koordinieren. Oft ist mein Großvater das Alibi der Harmlosigkeit. Als der Sender kaputtgeht und seine Mutter neue Teile besorgen muss, wird sie diese beim Transport in einem seiner Teddybären verstecken. Ein anderes Mal müssen sie und ihr Genosse in der Apotheke kiloweise Chemikalien besorgen, die in Kombination später den Sprengstoff ergeben, mit dem die Partisanen Bahngleise japanischer Militärzüge in die Luft jagen.

Mit ihrem Vorgesetzten beginnt sie während der Zeit eine Beziehung und wird erneut schwanger. Die Umstände für das Paar sind mehr als schwierig. Mit der neugeborenen Tochter Janina ziehen sie schließlich 1936 nach Polen. In Warschau und Danzig arbeitet Kuczynski am Aufbau von Widerstandsgruppen gegen die Nazis. Zu dieser Zeit wird ihr feierlich der Rotbannerorden verliehen – vom Vorsitzenden des Obersten Sowjets der UdSSR Michail Iwanowitsch Kalinin persönlich.

Ende 1938, noch vor dem deutschen Überfall auf Polen, hat die Geheimdienstzentrale in Moskau bereits neue Aufträge. So geht es nach einem weiteren Agententraining für »Sonja« in Moskau anschließend in die Schweiz. Michael ist jetzt sechs Jahre alt und hat bereits in fünf Ländern gelebt, spricht Chinesisch, Englisch, Deutsch, Polnisch, lernt in der Schweiz Französisch. Ein Leben, das sich für den Jungen nicht immer als einfach erweist. »Wenn man überall mal ist, mal zwei, mal fünf Jahre, trägt man eine

ständig wechselnde Vergangenheit mit sich herum. Diese Vergangenheit passt dann nicht zur Gegenwart. Und diese Gegenwart passt dann wiederum nicht zur nächsten Gegenwart. Du kannst also im Grunde nichts richtig lernen, was dir dann später wieder von Nutzen ist.«

In der Schweiz arbeitet Kuczynski mit zwei englischen Agenten zusammen, die aus Hitlerdeutschland kriegswichtige Informationen besorgen. Ihre Aufgabe ist es, diese Nachrichten von ihrem Standort in der kriegsneutralen Schweiz an die Alliierten zu senden. Ihrem Sohn kauft sie ein Morsespielzeug, das, wenn er gerade nicht damit spielt, seiner Mutter zur Ausbildung der beiden Engländer dient. Einer davon, Len Beurton, wird 1940 ihr zweiter Mann, nachdem Rudolf Hamburger 1939 nach China zurückgekehrt war. Leon »Len« Charles Beurton ist ein englischer Kommunist, der bereits im spanischen Bürgerkrieg in den Internationalen Brigaden gekämpft hatte und nun wie »Sonja« als Agent im Dienst des sowjetischen Nachrichtendienstes GRU steht – sein Deckname: John Miller. Aus der anfänglichen Scheinehe lassen die beiden später eine richtige Ehe werden, die bis zu seinen Tod bestehen bleibt.

Die beiden englischen Kommunisten, mit denen »Sonja« arbeitet, planen abenteuerliche und riskante Aktionen. So wollen sie einen deutschen Zeppelin sprengen – und als die beiden Männer ein Restaurant entdecken, in dem Adolf Hitler öfter verkehrt, sogar den Reichsführer selbst töten. Doch die Zentrale antwortet zu spät, die politische Lage ändert sich und es kommt nicht zum Anschlag. Als das langjährige Kindermädchen der Familie Beurton die Agentenzelle denunzieren will, wird die Aussage der Gouvernante von den Behörden wegen ihrer unverständlichen Schreibweise zwar nicht ernst genommen, doch die Arbeit fortzuführen und zugleich die Kinder zu schützen, wird unmöglich.

Also geht es für »Sonja« und Micha weiter nach England. Beurton kann erst zwanzig Monate später seiner Familie folgen. Im englischen Schulheim begreift Micha zum ersten Mal, dass die Art, auf die er bisher aufwuchs, ungewöhnlich ist: »Ich war ziemlich überrascht, als ich in England dann von meinen Schulkameraden hörte, dass die ihr ganzes Leben in einem Ort oder sogar in einem Haus verbracht hatten.«

Ende 1942 stellt Ursula Kuczynskis Bruder Jürgen den Kontakt zum deutsch-britischen Kernphysiker Klaus Fuchs her, der maßgeblich im amerikanisch-britischen Atombombenprojekt beschäftigt ist. Als sowjetischer Spion will er Moskau bei der Entwicklung einer eigenen Atombombe helfen. 1943 übergibt er »Sonja« ein etwa 100 Seiten umfassendes Buch mit zahlreichen detaillierten Blaupausen – dass es sich dabei um Dokumente der Amerikaner zum Bau der Atombombe handelt, erfährt »Sonja« erst später. Doch wohl ahnend, dass es sich um wichtige Informationen handelt, folgt sie dem konspirativen Protokoll, lässt zur richtigen Zeit am richtigen Ort in London ein Kreidestück fallen, zertritt es und zeigt so an, sich treffen zu wollen. Der Mittelsmann »Sergej« übergibt das Buch besonders schnell an die Zentrale. Moskau betont in der Antwort den Wert der Informationen gleich doppelt. Für Kuczynski geht das Leben normal weiter und noch im selben Jahr bekommt sie ihr drittes Kind Peter.

Später arbeitet ihr Bruder in den USA im »Büro für amerikanische Bombenstrategie« und übermittelt ihr von dort Unterlagen zu einem Analysesystem, das eine genaue Einschätzung der Rüstungsproduktion des militärischen Gegners erlaubt: Informationen, zu denen sonst nur Roosevelt, Eisenhower, Churchill und die drei Chefs großer militärisch-strategischer Büros in den USA Zugang haben.

1946, nach 16 Jahren geheimer Arbeit im Namen des Kommunismus, bricht für »Sonja« der Kontakt zur Zentrale ab und Kuczynski beendet ihre Spionagetätigkeit. Als einige Jahre später wieder der Kontakt hergestellt ist, entscheidet sie sich gegen eine Weiterarbeit und für ein Leben in der DDR. Dort beginnt sie eine lang ersehnte Karriere als Schriftstellerin und nimmt den Namen Ruth Werner an, bleibt jedoch bis zu ihrem Tod im Jahre 2000 überzeugte Kommunistin. Kuczynski hinterlässt drei Kinder von drei Männern, denen sie einen tiefen Eindruck davon mitgegeben hat, was es heißt, für seine Überzeugungen zu kämpfen. Uns allen offenbart sich in 15 Büchern ein umfangreicher Lebensbericht einer Frau, der geprägt ist von Mut und Lebensfreude. Auf der letzten Seite von »Sonjas Rapport«, ihrem bekanntesten Werk, schreibt sie: »Für die zukünftigen Generationen will ich immer noch soziale Gerechtigkeit, Zugang für jeden zu einer guten Bildung, und vor allem will ich, dass nirgendwo irgendjemand hungert und daß Frieden ist auf der Welt.(...)«. Auch ohne überzeugte Kommunistin zu sein, kann ich drei Generationen später der Utopie meiner Urgroßmutter beipflichten. •

ZUM WEITERLESEN

Ruth Werner: Sonjas Rapport (zuerst 1977)

Rudolf Hamburger: Zehn Jahre Lager: Als deutscher Kommunist im sowjetischen Gulag – Ein Bericht (2013)


Nominiert für den Edgar Allen Poe Award
Detektiv sein
FÜR
DUMMIES
Dr. Motte
VORSÄTZE FÜRS NEUE JAHR
Sei pünktlicher!
trainiere dein Köpfchen!
lerne die Menschen kennen!
mach mal wieder Sport!!
Navigation
Menu
mobile

»INFORMATION IST TRUMPF«

Strafverfolgung geht vom Staat aus. Das ist ein Grundsatz, der im Guten wie im Schlechten von einer Berufsgruppe gebrochen wird, die am liebsten im Verborgenen arbeitet: Detektive.

TEXT PHILIPP STEFFENS
ILLUSTRATION TERESA MÖNNICH

Es geht um meinen Ex, er zahlt keinen Unterhalt.« Mit diesen Worten beginnt ein Fall für Gerhard Bastin. Er war früher Kriminaloberkommissar, heute arbeitet er als Detektiv in Bremen. Ausbleibende Unterhaltszahlungen sind typische Aufgaben für private Ermittler. Zum Alltag gehören auch: Arbeitnehmer überwachen, die an einem anderen Ort arbeiten, obwohl sie krankgeschrieben sind, oder untergetauchte Schuldner und vermisste Personen finden. Außerdem können Detektive für die Abwehr von Industriespionage, IT-Forensik* und Abhörschutz zuständig sein. Umso erstaunlicher ist es, dass Ausbildung und Berufsfeld des privaten Ermittlers gesetzlich kaum geregelt sind.

DAS ARBEITSLEBEN DER ANDEREN

Ein Detektiv ist kein Polizist – er ist privater Ermittler. Er hat nicht mehr oder weniger Rechte als ein normaler Bürger, denn er handelt als Privatperson. Dennoch gelten für ihn andere Bestimmungen, was das Beschatten von sogenannten Zielpersonen angeht: Während die Polizei sich über richterliche Beschlüsse die Genehmigung einholen muss, andere zu überwachen, agiert ein Detektiv frei nach eigenem Ermessen. Trotzdem muss er sich natürlich an das Gesetz halten. Ob er allerdings jemanden mit dem Auto verfolgt oder auf seiner Facebook-Seite nach Hinweisen sucht, ist ihm überlassen. ▸

*IT-FORENSIK

Als IT-Forensik bezeichnet man die Untersuchung von verdächtigen Vorfällen im Zusammenhang mit IT-Systemen sowie die Feststellung des Tatbestandes und der Täter durch Erfassung, Analyse und Auswertung digitaler Spuren.

Gängige Methoden wie das Verwenden von GPS-Peilsendern sind laut Bundesgerichtshof nur in Ausnahmefällen zulässig. Das wichtigste Gerät im Detektivalltag ist der Fotoapparat. Er kann unter Umständen voll mit Bildern sein, die Personen in privaten Situationen zeigen, ohne dass sie Relevanz für den Auftrag haben. Doch auch hier gilt: Die Privatsphäre, wie die Wohnung eines Überwachten sind streng tabu. Auch die Beobachtung einer Zielperson in der Öffentlichkeit oder in allgemein zugänglichen Gebäuden wie Restaurants oder Hotels bedarf eines berechtigten Interesses von Seiten des Auftrages. Nur dann sind die dabei angefertigten Foto- oder Videoaufnahmen als Beweismittel in einem Prozess voll verwertbar. Was ein »berechtigtes Interesse« ist, entscheidet notfalls ein Gericht.

Die anlasslose Überwachung durch einen Detektiv ist in Deutschland ebenso verboten, nur bei Verdacht auf ein Vergehen darf beschattet werden. Das urteilte das Bundesarbeitsgericht vor zwei Jahren, als eine Arbeitnehmerin zu Unrecht beschuldigt wurde, ohne Anlass krank zu feiern und von einem Detektiv überwacht wurde.

Aber es ist natürlich möglich, dass ein Detektiv über einen kurzen Zeitraum jemanden beschattet, nur um dann festzustellen, dass die Person unschuldig ist. Zu diesem Zeitpunkt wurde dann allerdings schon anlasslos überwacht. Da die meisten privaten Ermittler alleine arbeiten, kann es außerdem eher dazu kommen, dass sie sich für Ermittlungswege entscheiden, die nicht legal sind.

DETEKTIV WERDEN KANN JEDER?

Die Probleme fangen bereits mit der Ausbildung an. Ein polizeiliches Führungszeugnis zum Erlangen des Gewerbescheins genügt, um eine Detektei zu gründen. Der Beruf des Detektivs ist in Deutschland komplett offen; eine Ausbildungspflicht gibt es nicht. Das statistische Bundesamt zählte 2008 ungefähr 950 Detekteien mit mehr als 3.000 Beschäftigten. Ein Missstand, findet Patrick Kurtz, der seit vier Jahren als privater Ermittler arbeitet: »Das ist fahrlässig. Es gab nie eine Regelung oder ernstzunehmende Berufsvoraussetzung für den Detektivberuf. Das ist ein großes Manko, weil wir qualifizierte Detektive brauchen.«

Kurtz selbst kam über ein Praktikum in die Branche. Danach entschied er sich zu einer Detektiv-Ausbildung an der Sicherheitsakademie in Berlin. Er gründete 2013 seine eigene Detektei, die es mittlerweile an 27 Standorten in Deutschland sowie als separate Firma in der Schweiz gibt. Mit Hilfe von Subunternehmern von 40 bis 50 Ermittlern hat er ein flächendeckendes Netzwerk geschaffen.

Laut Kurtz waren viele Detektive früher Polizisten; dieser Job ist ein typischer Einstieg in den Beruf. »Wir lösen auch Fälle, in denen es um kriminelle Taten geht. Oft ist es einfach so, dass die Polizei nicht tätig wird oder nicht die Kapazitäten hat, um zu ermitteln. Da reicht das Budget nicht aus, das der deutsche Staat in die Sicherheit investiert. Somit erfüllen Detektive meiner Meinung nach auch eine wichtige gesellschaftliche Rolle«, beschreibt Kurtz die Relevanz des Gewerbes. Die Zukunft sieht er positiv: »Information ist immer Trumpf.«

Die Berliner Sicherheitsakademie bietet Weiterbildungskurse an, die von der Industrie- und Handelskammer (IHK) geprüft wurden. Diese zertifizierten Ausbildungen sind jedoch eine Seltenheit. Alternativ ist es beispielsweise möglich, sich über die Zentralstelle für die Ausbildung im Detektivgewerbe (ZAD) weiterbilden zu lassen oder dies direkt in einer Detektei zu tun. Aber selbst die Agentur für Arbeit gibt auf ihrer Webseite zu den Ausbildungsinhalten nur an, dass diese durch »interne Vorschriften der Lehrgangsträger geregelt ist«. Auch die Ausbildungsdauer kann variieren, von zwei Monaten bis zu zwei Jahren ist alles möglich.

AUSBILDUNGSMÄNGEL FÜHREN ZU ERMITTLUNGSFEHLERN

Zu welchen Schwierigkeiten die ungeregelten Wege in den Detektivberuf führen können, zeigt der Fall von Detektiv Bastin, einem ehemaligen Polizisten. Während seiner Ermittlungen in besagtem Unterhaltsstreit platzierte Bastin einen GPS-Sender am Auto der Zielperson und erstellte ein Bewegungsprofil. Das ist nicht nur illegal, diese unerlaubte Maßnahme war zudem in einer NDR-Reportage von 2015 zu sehen.

Wegen unerlaubt erstellter Bewegungsprofilen kann ein Detektiv vor Gericht verurteilt wurden. Der Bundesgerichtshof bestätigte 2013 ein Urteil des Landgerichts Mannheim, bei dem klargestellt wurde, dass GPS-Überwachung nur in notwehrähnlichen Situationen erlaubt ist. Ohne »starkes berechtigtes Interesse« mache man sich strafbar. Während der Verhandlungen sagte einer der zu Bewährungsstrafen verurteilten Detektive, dass er nicht gewusst habe, dass das Verwenden von GPS-Peilsendern verboten sei. Hier zeigen sich die Probleme, die entstehen, wenn Ermittlungen privatisiert werden, ohne die Ausbildung dazu deutlich zu reglementieren.

Detektive decken ein Feld ab, das die Polizei meist nicht bedienen kann. Ein krankgeschriebener Arbeitnehmer wird nicht von der Kriminalpolizei überwacht, nur weil der Chef glaubt, dass sein Mitarbeiter doch nur auf das Konzert der Lieblingsband wollte. Ebenso ist es verständlich, dass es keine polizeiliche Telekommunikationsüberwachung von säumigen Unterhaltszahlern gibt. Die Anlässe sind einfach nicht schwerwiegend genug, um die Staatsgewalt zum Einmischen zu bringen.

ARBEIT IN DER GRAUZONE

Es ist fraglich, ob die Überwachung und Beschattung von Privatpersonen durch andere Privatpersonen erfolgen sollte. Die Polizei darf nur unter ganz bestimmten Umständen verdeckt ermitteln – solch ein Vorgang ist streng geregelt. Das Prinzip dahinter ist ein moralisches: In einem Rechtsstaat wirkt die Polizei möglichst offen.

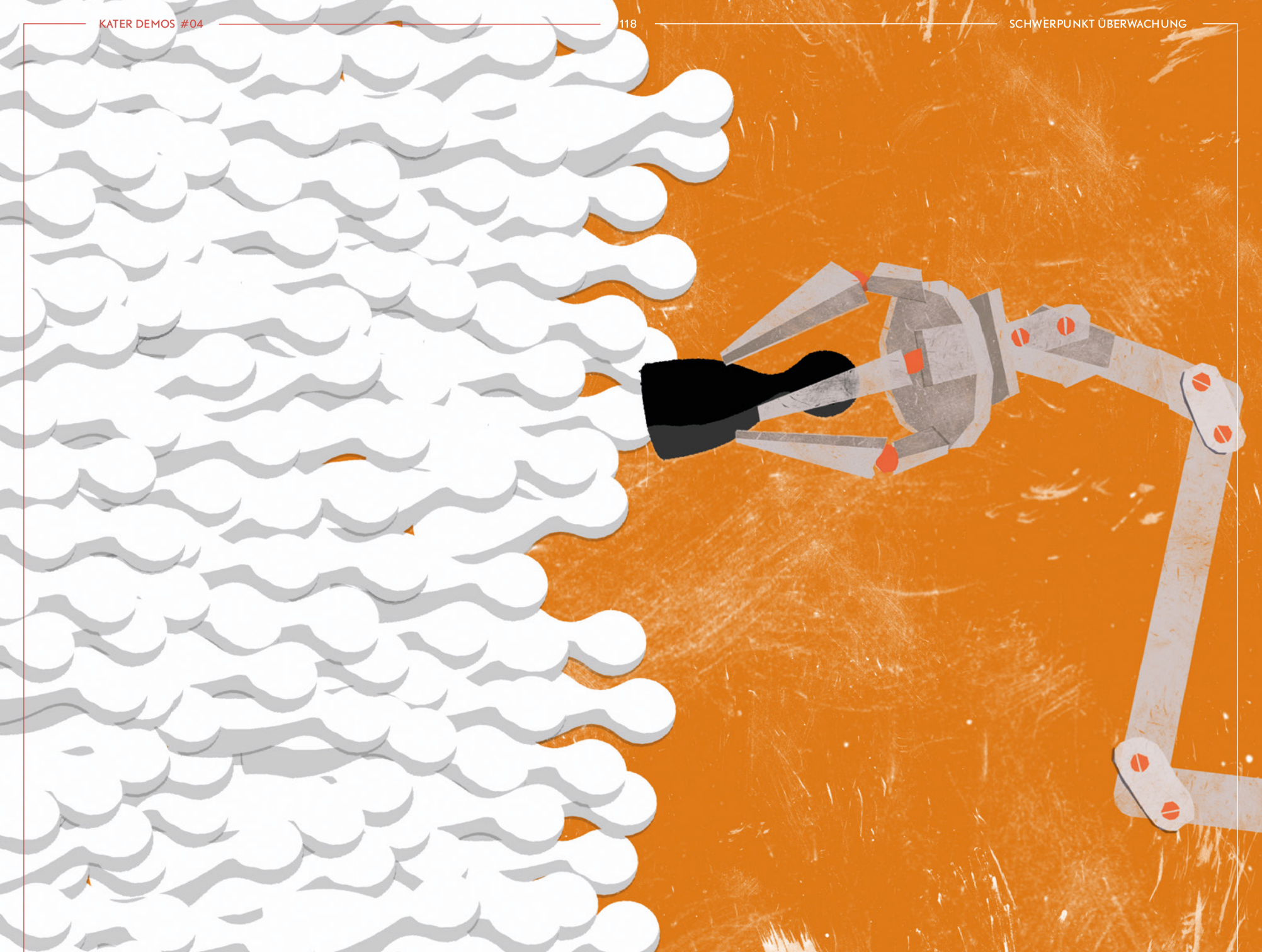
Detektive hingegen müssen anonym arbeiten. Zielpersonen dürfen sie bei der Beschattung nicht erkennen, sonst sind sie »verbrannt«, wie es im Fachjargon heißt. Wird die Privatsphäre eines Menschen gebrochen, wenn ein Detektiv stundenlang im Auto eine Person nur aufgrund eines Verdachts observiert? Auch wenn man nur wenig Sympathie für den unverlässlichen Vater hat, der seinen Unterhalt nicht zahlt, gibt es viele weitere Beispiele, die sich dagegen in Grauzonen abspielen.

Patrick Kurtz hat solche Fälle persönlich erlebt: »Man muss sich da distanzieren. Natürlich gibt es Situationen, in denen man denkt: ›Das ist aber ein ganz dreistes Schwein‹. Das sagt man dann nur intern. Im Gegensatz dazu hatte ich es aber auch schon, dass ich Zielpersonen observiert habe, bei denen ich mir dachte, dass die schon arm dran sind. Also zumindest im Vergleich mit den Leuten, die uns beauftragt haben, sie zu observieren, weil sie in Wahrheit lammfromm sind.« Als Beispiel nennt er Untreue, ein typischer Fall für Detektive: Er observierte eine Frau, die ihren Mann angeblich betrog, dabei fuhr sie nach der Arbeit immer direkt nach Hause. Zwei Wochen lang folgte er ihr, bis der Mann den Auftrag für beendet erklärte. Bezahlt wurde Kurtz natürlich trotzdem, obwohl sich der Verdacht als falsch herausstellte.

Das Recht auf Privatsphäre ist ein unerlässliches Gut, das nicht einfach durch einen Verdacht ohne Indizien gebrochen werden sollte. Für einen Detektiv ist es aber nicht immer klar erkennbar, ob der Verdacht begründet ist oder vielleicht andere Faktoren eine Rolle spielen. Kurtz lässt seine Mandanten daher einen Vertrag unterschreiben, in dem sie zusichern, dass sie ihm alle Informationen, die für den Fall relevant sind, mitgeteilt haben. Das ist allerdings mehr eine Absicherung für ihn, weniger zum Schutz des zu Überwachenden.

Man sollte nicht einer komplette Berufsgruppe Willkür oder Sorglosigkeit unterstellen. Doch ist es bemerkenswert, dass rechtlich gesehen jeder als Detektiv arbeiten kann und es quasi keine Barrieren in den Beruf gibt, obwohl für den Arbeitsalltag sehr spezielle Fähigkeiten und Kenntnisse erforderlich sind. Ohne ein fundiertes Wissen der deutschen Gesetzeslage kann niemand seriös als Detektiv arbeiten. Da in der Praxis die meisten Detektive alleine arbeiten, fehlt zudem eine Kontrolle durch erfahrene, objektive Kollegen. Der Fall von Gerhard Bastin offenbart, dass selbst ehemalige Polizisten Probleme haben können, sich als Detektiv korrekt zu verhalten. •

Philipp Steffens kam im zarten Alter von 19 zum ersten Mal dazu, Texte für die breite Öffentlichkeit zu schreiben. Angestachelt von diesem frühen Erfolg, stieg er wenige Jahre später in das lukrative Geschäft des Musikjournalismus ein. Nebenbei tut er so, als ob das Abspielen von geistigem Eigentum Anderer eine besondere Form der Kunst sei und verliert abwechselnd viel Geld im Plattenladen oder im asiatischen Lebensmittelgeschäft.



FARBENBLIND

Dunklere Hautfarbe als die weiße Mehrheitsgesellschaft? Für die Polizei reicht das, um Menschen willkürlich anzuhalten und zu kontrollieren. Offiziell gibt es jenes Problem namens »Racial Profiling« gar nicht, doch die Berichte Betroffener nehmen zu. Die Kölner Silvesternacht 2017 und die Fahndung nach so genannten »Nafris« zeigen, wie heikel das Thema ist.

TEXT LARA BOGAN
ILLUSTRATION SOPHIA SCHRADE

Abeeku (Name geändert) wurde in Ghana geboren und lebt seit vielen Jahren in Deutschland. Der zierliche Mann sitzt am Tisch und berichtet leise von seinen Erfahrungen auf Hamburgs Straßen. Falschen Zuschreibungen ist er fast täglich ausgesetzt – sein Aufenthaltsrecht nimmt ihm die Polizei in der Regel nicht ab. Er könne kaum seine Wohnung verlassen, ohne kontrolliert zu werden, empört er sich: »Sobald ich auf der Straße unterwegs bin, habe ich Probleme mit der Polizei.« Das hat Folgen für sein Wohlbefinden – durch die willkürlichen Kontrollen fühlt er sich permanent unsicher, blickt um sich, glaubt, verfolgt zu werden.

INNERE LANDKARTEN

Diese polizeiliche Praxis, bei der die Beamten nach Aussehen oder nach einer vermuteten »ethnischen« Zugehörigkeit kontrollieren, nennt sich Racial Profiling. Beispielsweise wird jemand aufgrund seiner Hautfarbe oder Kleidung verdächtigt, Drogen zu verkaufen, illegal eingewandert oder anders straffällig geworden zu sein und daraufhin angehalten, befragt und durchsucht. Offiziell gibt es keine Statistiken über derartige Vorfälle, doch weist die Erhebung der EU zu Minderheiten und Diskriminierung (EU-MIDIS) darauf hin, dass die Zahl der willkürlichen Kontrollen hoch ist.

Im Januar 2017 erlebt die deutsche Öffentlichkeit, wie die Kölner Polizei in der Neujahrsnacht die Bezeichnung »Nafri« (internes Kürzel für »nordafrikanischer Intensivtäter«) auf Twitter verwendete. Trotz der darauffolgenden Entschuldigung wird in der Aufklärung der Geschehnisse deutlich, wie fehleranfällig derlei Kategorisierung ist. Man habe nur »Nafris« kontrolliert, doch kam nur ein Bruchteil der festgehaltenen Personen tatsächlich aus Nordafrika, geschweige denn waren alle Festgehaltenen Intensivtäter. Herkunft lässt sich nicht am Aussehen festmachen. Und erst recht lässt daraus kein Verhalten gegenüber Frauen oder Kriminalität ableiten. ▸

Mit solchen Erfahrungen setzt sich auch Marina (Name geändert) von der Kampagne für Opfer von Polizeigewalt Bremen (KOP) auseinander. Die KOP ist eine unabhängige Beratungsstelle für Betroffene von Racial Profiling, die mit verschiedenen Anwälten kooperiert. Ihre Fälle zeigen, dass unbegründete Kontrollen auch zu »inneren Landkarten« führen, »sodass Menschen etwa den Hauptbahnhof oder bestimmte Wege aus Angst meiden.«

ZWISCHEN VERDACHT UND VORURTEIL

Grundsätzlich hat die Polizei die Möglichkeit zu verdachtsunabhängigen Kontrollen. Das ermöglichen das Bundespolizeigesetz und die Landespolizeigesetze. Dabei sollen sich die Polizisten auf ihre Erfahrungen und Einschätzung der Gefahrenlage verlassen. Der Polizeisoziologe Rafael Behr arbeitete selbst 15 Jahre bei der Hessischen Polizei, bevor er begann, an der Akademie der Polizei Hamburg zu forschen und zu lehren. Er erklärt, dass schließlich nicht jeder kontrolliert werden könne, mache »es notwendig, dass Polizisten über Instrumente der Verdachtsschöpfung verfügen, die ihre Selektion legitimieren.«

Diese Instrumente seien durch das persönliche Menschenbild geprägt und bildeten auch gesellschaftliche Vorurteile ab. Polizisten mit eigener Migrationsgeschichte einzustellen habe daran nichts geändert, merkt Behr an. Denn um in der Institution bestehen zu können, müsse man sich früh den Haltungen des Kollegiums anpassen, und blende eigene, möglicherweise negative Erfahrungen aus.

In der konkreten Situation bleibt es eine Gratwanderung: Handelt es sich um eine tatsächliche Gefahr oder mischen sich in den Verdacht stereotype Bilder? Abeeku deutet das Verhalten der Polizei für sich so: »Sie scheinen zu glauben, dass alle Schwarzen keine Papiere haben und Drogen verkaufen. Für sie sind wir alle gleich.« Von diesem Verdacht sind nicht nur straffällige Menschen betroffen, sondern alle, die ins Raster passen, wie das Kölner Beispiel zeigt. Dabei trifft es auch häufig People of Colour, die seit Generationen in Deutschland leben. Eine äußerst unangenehme Erfahrung: Wer möchte schon regelmäßig grundlos auf offener Straße angehalten werden?

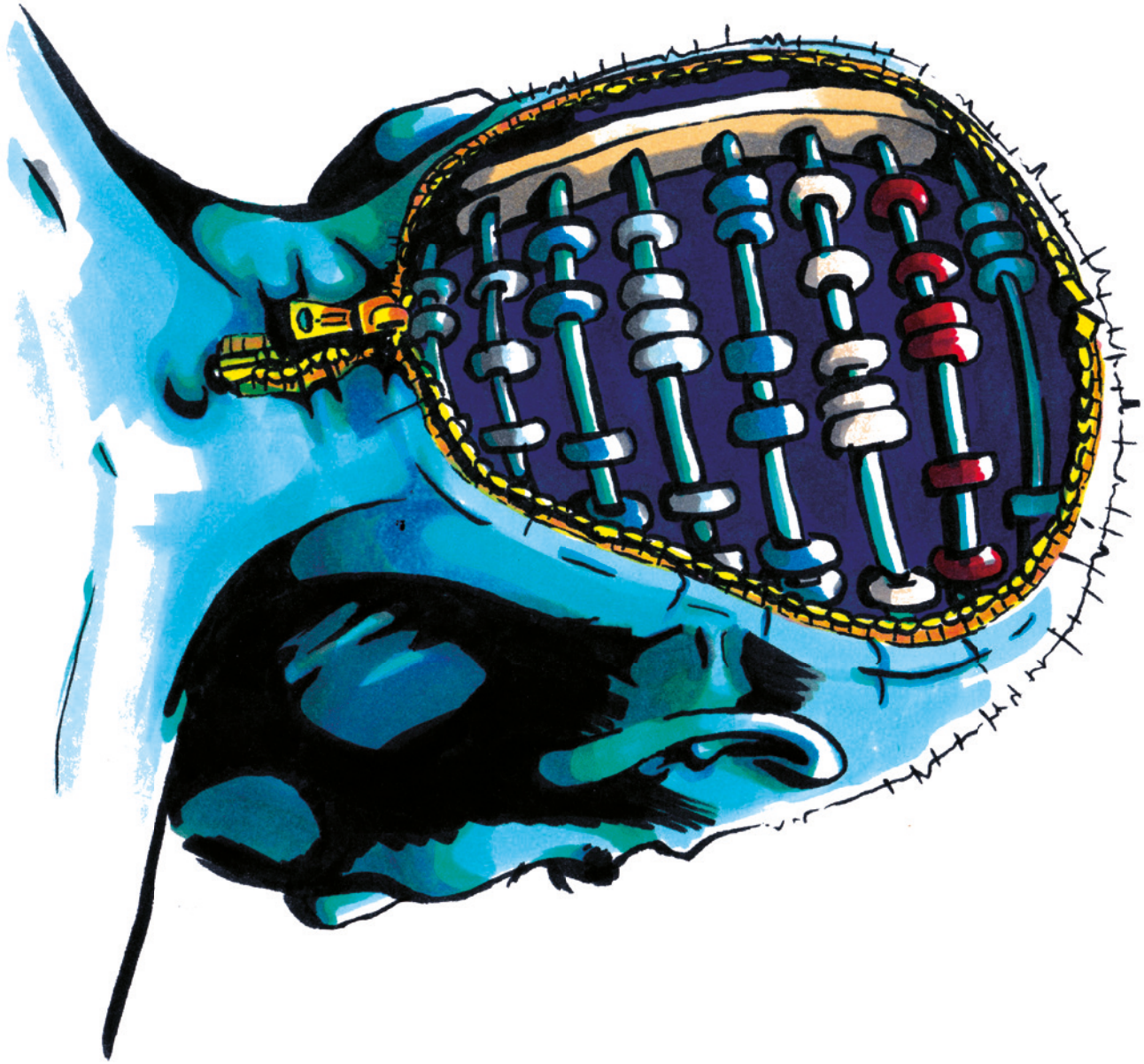
WAS NICHT SEIN DARF, GIBT ES ANGEBLICH NICHT

Polizeigesetze müssen die Grundrechte Einzelner auch bei Eingriffen wahren. Das Deutsche Institut für Menschenrechte zeigt in einer Studie über Racial Profiling, dass verdachtsunabhängige Kontrollen verfassungswidrig sind, denn im Grundgesetz wird die Diskriminierung aufgrund der »Rasse« untersagt. Auch verstoße es gegen das Recht auf informationelle Selbstbestimmung. Der Europäische Gerichtshof urteilte im Jahr 2010, dass verdachtslose Kontrollen nicht mit dem europäischen Unionsrecht zum »Schengen-Raum« vereinbar sind. Der Gesetzgeber sollte die Polizeigesetze dort ändern, wo sie diskriminierende Handlungen begünstigen – konkret den §22 Abs. 1a des Bundespolizeigesetzes. Auf Landesebene handelt es sich um alle Bestimmungen, die Personenkontrollen ohne konkreten Anlass beinhalten. Nur so kann einem institutionell verankerten Rassismus entgegnet werden. Auch Polizeisoziologe Behr befürwortet ein diskriminierungssensibles Recht, denn sonst liege es nahe, »dass die Polizei diskriminierende Handlungen betreibt, ohne es zu wollen.«

Im vergangenen Jahr kehrt Abeeku von seinem Sprachunterricht zurück nach Hause. Er schildert seine drastische Erfahrung so: An der Ampel wartend wird er plötzlich von fünf zivilen Polizisten umstellt, die sein Fahrrad überprüfen und seine Tasche durchsuchen. Darin befindet sich kein Cannabis und das Fahrrad ist auch nicht gestohlen. Dennoch muss er sich ausweisen. Später dokumentiert Abeeku alles genau und beschwert sich auf der Wache. Ohne Erfolg – bis heute habe die Polizei nicht reagiert.

Die Ohnmacht Betroffener wie Abeeku zeigt, dass Veränderungen auch auf übergeordneten politischen Ebenen in die Wege geleitet werden müssen. Die aktuelle Bundesregierung ist derweil in der Angelegenheit gespalten. Auf eine Anfrage der Linken schrieb sie im Februar 2014, dass Racial Profiling zwar rechtswidrig sei, argumentiert jedoch, dass es genau deshalb in der deutschen Polizei nicht vorkomme. Was nicht sein darf, gibt es also nicht? An anderer Stelle wird darauf verwiesen, dass das Aussehen nicht das stärkste Kontrollkriterium sein dürfe, dass es aber durchaus zulässig ist. Doch wer kann das im Nachhinein noch feststellen? Für Behr ist dies kniffelig, denn letztlich habe der Polizeibeamte die Definitionsmacht. Eine Kontrolle kann im Nachhinein plausibel gemacht werden, auch wenn sie es in der Situation nicht war.

Neben Gesetzesänderungen gibt es weitere Lösungsansätze: So hat sich in Bulgarien, Spanien, Ungarn und Großbritannien ein Formular bewährt, in dem nach jeder Kontrolle Grund, Ort und Zeitpunkt festgehalten werden. Zuletzt kann der Kontrollierte, wenn er zustimmt, seine ethnische Zugehörigkeit angeben. Dadurch kommt es zum Reflektieren ihrer Handhabung und erfolgreicheren Kontrollen. Für Abeeku bleibt in der Zwischenzeit nur die Hoffnung, dass sich das Verhalten der Polizei auch in Deutschland ändert. •



MICHEL UND DAS SUPERGEFÄNGNIS

Auf welchem Mist ist eigentlich diese Ich-hab'-doch-nix-zu-verbergen-Haltung gewachsen? Kann es sein, dass wir uns in unserer Lebenspraxis viel mehr von äußeren Einflüssen leiten lassen als uns bewusst ist? Der Soziologe Michel Foucault hat auf diese Fragen eine unangenehme Antwort, eröffnet aber auch eine wichtige Perspektive auf Überwachung, die gänzlich ohne NSA und Co. funktioniert.

TEXT JUDITH PAPE
FOTO MATTI MICHELS

In postmodernen sozial- und geisteswissenschaftlichen Theorien macht sich ein Trend bemerkbar: Ich nenne ihn Subjekt-Bashing. Dabei geht es darum, dem Subjekt aus den verschiedensten theoretischen Perspektiven eine Abhängigkeit und Formbarkeit zu attestieren. Seine Wünsche und Idealvorstellungen: alle sozial erzeugt. Seine Identität und Persönlichkeit: ein Spiel aus gesellschaftlicher Belohnung und Bestrafung. Beliebt ist auch die Ansicht, dass das Subjekt in westlichen Gesellschaften schlichtweg nur noch als Zwischenlager zwischen Kauf und Entsorgung einer immer größer werdenden Fülle von Waren fungiert. Vorbei sind die glücklichen Zeiten, in denen Immanuel Kant noch Loblieder auf die menschliche Vernunft als Mittel der Selbstermächtigung sang. Das Konzept des selbstbestimmten Individuums hat es leider nicht in unsere goldene Ära des Cat-Content geschafft.

Ein Theoretiker, der sich damit intensiv beschäftigt hat, war Michel Foucault (1926–1984). Auch er lässt nicht viel Gutes am Konzept des selbstbestimmten Menschen und zeichnet ein düsteres Bild unserer Zeit. In seiner historisch angelegten Studie – die passenderweise »Überwachen und Strafen« (1975) heißt – kommt er zu der Erkenntnis, dass sich eine Veränderung hinsichtlich der »ordnungsgewährleistenden Machtausübung« in Gesellschaften vollzogen hat. Während Macht als Form von Züchtigung im Mittelalter unmittelbar am Körper einzelner Menschen vollzogen wurde (etwa Marter als Form der schmerzvollen, langwierigen Hinrichtung), wirkt sie seit zwei- bis dreihundert Jahren zunehmend nur noch mittelbar – als permanent drohende Eventualität.

Foucault sieht darin auch die Entwicklung zu einer Gesellschaft aus Individuen, die sich einerseits selbst überwachen und gleichzeitig hochsensibel für Erwartungen sind, die von allen Seiten an sie gerichtet werden. Um nachzuvollziehen, wie wirkmächtig diese neue Form der Macht tatsächlich ist, muss man sich zunächst von der gängigen Vorstellung der Selbstverwirklichung verabschieden, also der Vorstellung, der Mensch könne unter freiheitlich-demokratischen Rahmenbedingungen sein ureigenes, inneres Wesen ausleben. Aber eins nach dem anderen. ▸

VON DER DIREKTEN ZUR INDIREKTEN ÜBERWACHUNG

Foucault zufolge wirkten die früheren Formen der Machtausübung vorrangig direkt. Durch die öffentliche Zurschaustellung der Qualen wusste jeder Mensch, was ihm beim jeweiligen Vergehen drohen würde. Die ausgedehnten Prozeduren der Hinrichtung dienten dabei als Abschreckung und bändigten so potenziell Aufständische.

Die Machtausübung im kapitalistischen Zeitalter wirkt hingegen nicht mehr nur am Rande der Gesellschaft wie in Zeiten der Marter an den Schwellen zum Verwerflichen und Verbotenen, sondern greift nun in alle Aspekte des sozialen Lebens ein. Foucault beschreibt sie anhand eines bestimmten Gefängnistyps: des Panopticons. Dieses zeichnet sich durch seine spezielle Architektur und die damit einhergehende Effizienz aus, bei der lediglich eine Wachperson nötig ist, um eine maximale Zahl an Insassen zu überwachen. So befindet sich in der Mitte eines ringförmigen, mehrstöckigen Gebäudes ein einziger Wachturm, von dem aus die Zellen mit einem 360-Grad-Blick einsehbar sind. Durch einen Blickschutz, der die Beobachtung nur einseitig vom Wachturm aus zulässt, besitzt die Aufsicht zusätzliche Kontrollmacht.

Hier liegt der Knackpunkt des perfiden Supergefängnisses: Während die Wachperson einen Insassen jederzeit beobachten könnte, weiß dieser selbst nicht, wann er tatsächlich im Fokus steht. Darüber hinaus kann die Wache alle Gefangenen gleichermaßen betrachten, während die einzelnen Insassen jeweils völlig isoliert sind. Damit wäre theoretisch selbst diese eine Wachperson letztlich überflüssig, da die architektonische Formation allein genügen würde, um allen Sträflingen den Zustand permanenter Überwachung zu suggerieren. Oder, um es im Manager-Sprech zu sagen: Die Überwachung wurde »outgesourct« – der zu Überwachende überwacht sich selbst.

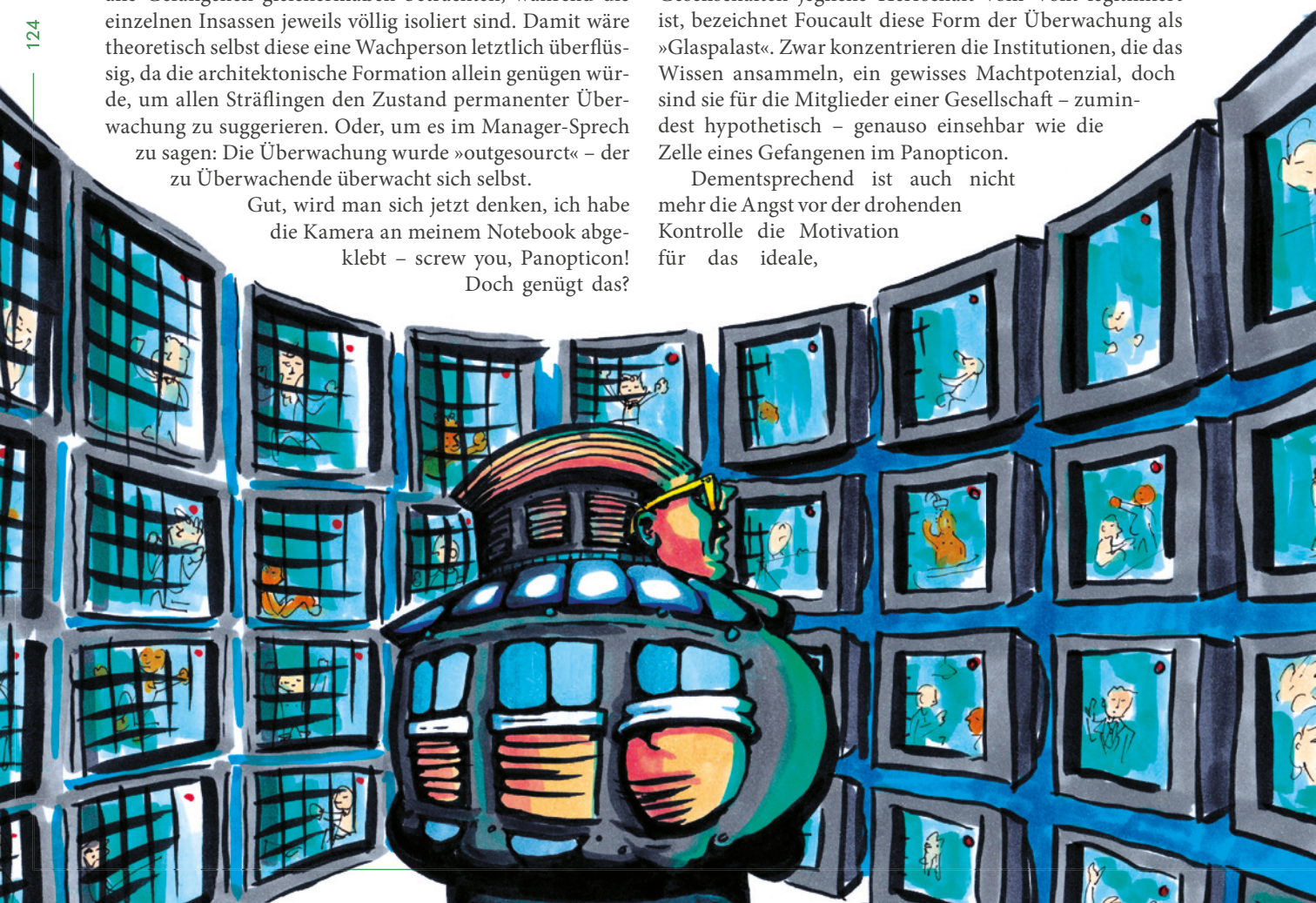
Gut, wird man sich jetzt denken, ich habe die Kamera an meinem Notebook abgeklebt – screw you, Panopticon! Doch genügt das?

Für Foucault ist diese Form der Überwachung nämlich eine Metapher für das alltägliche Leben. Seiner These nach sind wir Individuen in modernen, aufgeklärten und scheinbar freien Gesellschaften völlig von dieser neuen Form der Macht durchdrungen. Ballungspunkte jener fluiden Macht sind Institutionen wie Schulen, Krankenhäuser, Verwaltungseinrichtungen und auch Arbeitgeber. Sie alle sammeln und speichern Informationen über uns, klassifizieren uns permanent und besitzen damit die stetige Möglichkeit, Abweichungen festzustellen und im Zweifelsfalle zu intervenieren. Wer in einer solchen Gesellschaft aufwächst, hat sich mit dieser subtilen und omnipräsenten Dynamik meist längst arrangiert, sodass der tatsächliche Vollzug der Macht, ein Hausbesuch beispielsweise, kaum noch nötig ist. Allein die Möglichkeit reicht aus, Individuen zu gängeln und sie dazu zu bringen, nicht-konformes Verhalten zu unterlassen oder gar nicht erst darüber nachzudenken.

WER SITZT IM WACHTURM ODER WER PROFITIERT VON ALLDEM?

Heutzutage hat nicht mehr irgendein Fürst ein persönliches, materielles Interesse daran, dass die Bauern schuften und nicht stehlen, sodass er jeden einzelnen Querschläger aufknüpft, um ein Exempel zu statuieren. Die neue, dezentrale Form der Macht unterscheidet nicht mehr zwischen Beherrschendem und Beherrschtem. Da in demokratischen Gesellschaften jegliche Herrschaft vom Volk legitimiert ist, bezeichnet Foucault diese Form der Überwachung als »Glaspalast«. Zwar konzentrieren die Institutionen, die das Wissen ansammeln, ein gewisses Machtpotenzial, doch sind sie für die Mitglieder einer Gesellschaft – zumindest hypothetisch – genauso einsehbar wie die Zelle eines Gefangenen im Panopticon.

Dementsprechend ist auch nicht mehr die Angst vor der drohenden Kontrolle die Motivation für das ideale,



produktive Verhalten. Schließlich wäre die Voraussetzung für Angst das Wissen darum, dass es jene subtile Kraft, die einen kontrolliert, formt und sanktioniert, tatsächlich gibt. Stattdessen besteht eine breite Zustimmung zu dieser ausdifferenziert strukturierten Gesellschaft. Gemeinhin gilt diese Organisationsform als vernünftig; schließlich steigert die damit verbundene Macht die gesellschaftlichen Kräfte, erhöht die Produktivität und das Niveau der öffentlichen Moral – sie treibt an, ohne den Fortschritt zu stören. Somit entzieht die demokratische Legitimation und vernünftige, institutionelle Organisation der fluiden Macht jeder widerstrebenden Bewegung von Beginn an jegliches Aggressionspotenzial, da sie mit einem scheinbar hohen Grad an Freiheit einhergeht und eben nicht von außen oder oben, sondern eher von innen wirkt.

Der Soziologe Ulrich Bröckling betrachtet die Wirkungsweise dieses Strukturgeflechts im 21. Jahrhundert genauer und sieht darin ein »Kraftfeld«, welches das einzelne Subjekt als unternehmerisches Selbst hervorbringt; er beobachtet eine Ökonomisierung des Sozialen, einen Imperativ der ständigen individuellen Entwicklung hin zum besseren, effizienteren und erfolgreicheren Selbst. Demnach bedeutet konform zu sein heutzutage, den Pfad der Selbstoptimierung ein Leben lang brav zu beschreiten und das eigene Leben als Portfolio von Projekten zu begreifen, wie Arbeits-, Beziehungs-, Freizeit- und Gesundheitsprojekte. Jedes dieser Projekte verlangt nach Management, Optimierung und schließlich nach Erfolg. Gleichzeitig fallen bei einem effizienten Portfolio-Management auch Lebensbereiche unter den Tisch: Für ehrenamtliches Engagement in Deiner Freizeit bekommst Du in der Regel nicht so viel Anerkennung wie für das Travel-Jahr in Südostasien. Während also das panoptische System als sich selbst kontrollierender Mechanismus zu begreifen ist, liefert das Kraftfeld des unternehmerischen Selbst momentan dessen Inhalt oder Zielvorgabe.

»PRISON BREAK ANTHEM (ICH GLAUB' AN DICH)«

Bröckling denkt auch darüber nach, wie man sich diesem Zugriff entziehen kann – ein Unterfangen, das gar nicht so einfach zu bewerkstelligen ist: »Wovon sich befreien, wenn ein grundlegendes Verlangen nach Freiheit die Triebkraft des unternehmerischen Handelns darstellt?« Am Anfang Deines persönlichen Prison Break steht also die Erkenntnis, dass es eine wirkmächtige, stimulierende und sanktionierende gesellschaftliche Kraft gibt, die uns antreibt, formt und sich paradoxerweise unter dem Deckmantel der Freiheit verbirgt.

Die gute Nachricht ist aber, dass dieser Tage nicht mehr gemartert wird, wer sich dieser Selbstoptimierungshegemonie entzieht. Dennoch liefert auch Bröckling keinen Masterplan für den endgültigen Ausbruch aus diesem Subjektivierungsregime: »Gelingen kann das Außerkraftsetzen des unternehmerischen Kraftfelds stets nur für den Moment, aber es sind diese Momente, die schlagartig erkennen lassen, dass der Sog nicht unausweichlich ist.« Dabei hilft es natürlich, sich bewusst zu machen, welche vorherrschenden Bedeutungszusammenhänge jeden Tag subtil auf jeden Einzelnen von uns wirken – und diese kritisch zu hinterfragen. Selbstentfaltung, die sich diesem Konformitätsdruck entzieht, kann daher auch nicht allein die ständige Arbeit an sich selbst bedeuten, sondern entspringt aus dem Bewusstsein dafür, wo man steht und wo man hinwill (oder ob man sich überhaupt bewegen will). Das Gefühl, »anders« zu handeln, sollte in einer freien Gesellschaft jedenfalls nicht als Anlass zur permanenten Rechtfertigung gedeutet werden.

Ob Du Dich mit diesem Wissen jetzt nach Kuba absetzt, um dort ein autarkes Leben als Segelboot-Hippie zu leben, oder ob Du politischen Aktivismus in Europa zu Deinem neuen Hobby machst, ist dabei erst einmal egal. Wichtig ist, dass wir uns des Ausmaßes unserer tatsächlichen Freiheit bewusst werden und uns auch langfristig dementsprechend verhalten. Für die politische Situation in Deutschland wäre es aber vermutlich besser, Du würdest anfangen, Dich mehr einzumischen und Dich für das einzusetzen, was Du für richtig und relevant hältst. Das würde sicher auch Kant gefallen. •

Als alter Hase der Überwachungsabwehr hat **Judith Pape** Facebook schon vor Jahren mit einem falschen Nachnamen hinters Licht geführt. Ihr eigenes Bedürfnis, in die Privatsphäre anderer einzudringen, befriedigt sie durch exzessives Reality-TV-Gucken an Katertagen. Judith kennt zudem alle (189!) Folgen von »Keeping up with the Kardashians«.

ZUM WEITERLESEN

Michel Foucault: Überwachen und Strafen (1975)

Harald Welzer: Selbst denken. Eine Anleitung zum Widerstand (2013)

Ulrich Bröckling: Das unternehmerische Selbst. Soziologie einer Subjektivierungsform (2007)

EINE ALLZWECKWAFFE DER AUFKLÄRUNG

Millionen Menschen werden überwacht, ohne es zu wissen. Die Filmemacherin Theresia Reinhold hat es sich zur Aufgabe gemacht, das zu ändern. Ihr neues Projekt ist ein einzigartiges Experiment im Bereich des Dokumentarfilms.

TEXT KRIS CATZ
FOTO STREIFENBLICKE.DE

KATER DEMOS *Theresia, Dein aktuelles Filmprojekt »Information. What are they looking at?« soll Menschen das Thema Überwachung näher bringen. Was ist für Dich Überwachung?*
THERESIA REINHOLD Überwachung bedeutet für mich, dass gewisse Menschen meine Situation ausnutzen. Eine Situation, an der ich nichts ändern kann. Die meisten Menschen haben heute keine andere Wahl mehr, als internetbasierte Dienste zu nutzen. Ich kann damit nicht einfach aufhören, weil ich mich dadurch beruflich und privat ins Abseits stellen würde. Es gibt schlicht keine Ausstiegschance. Und genau diese Tatsache wird ausgenutzt. Gleichzeitig kann ich in den meisten Fällen nicht beweisen oder konkret wahrnehmen, dass ich überwacht werde. Deshalb sagen auch viele: »Ist mir doch egal, ich kann ja sowieso nichts ändern.«

KD *Wenn ich doch aber – wie Du sagst – an meiner Situation nichts ändern kann, ist diese Einstellung dann so falsch? Oder kann ich doch etwas ändern?*
TR Das ist eben die große Frage. Es gibt ja Methoden, um seine Mails und Telefonate sicherer zu machen. Ich kann auch meine Zugtickets mit Bargeld bezahlen und Bücher nicht bei Amazon, sondern beim Buchhändler kaufen. Das sind alles gute Ideen. Am Ende brauchen wir aber einen langfristigen Ansatz und dabei müssen wir auch mit

Politikern und Unternehmen zusammenarbeiten. Bei einem Verschlüsselungsworkshop erreiche ich vielleicht zehn bis zwanzig Menschen. Wenn ich aber eine politische Veränderung durchsetzen kann, betrifft das zum Beispiel in Deutschland im Idealfall mehr als 82 Millionen Menschen. Der Staat ist deshalb nicht per se unser Feind. Es gibt auch Politikerinnen und Politiker, die gegen diese Form der Überwachung sind. Diese Leute müssen wir konkret stärken.

KD ***Mit Deinem Film willst Du aber zunächst das Bewusstsein für das Thema Überwachung stärken. Mit welchen Mitteln willst Du das erreichen?***
TR »Information. What are they looking at?« ist zunächst einmal ein analytischer Dokumentarfilm, der das Thema Überwachung so einfach wie möglich erklärt. Die Personen, die ich dazu interviewt habe, entsprechen aber nicht unbedingt dem Schema, das man aus Talkshows und Zeitungen kennt. Ich konzentriere mich nicht auf weiße, männliche Mittelklasse-Akademiker. Mir geht es darum, Leute außerhalb der westeuropäischen und amerikanischen Diskussion um Massenüberwachung zu erreichen.

KD ***Projekte, die auf Diversity achten, gibt es mittlerweile viele. Dennoch wird aber oft das übliche Publikum erreicht.***
TR Deshalb liegt mein Fokus auch darauf, ein viel breiteres Publikum zu erreichen. Eines, das aus unterschiedlichen Gründen auch keinerlei Vorwissen zu diesem Thema hat. Deshalb soll es als zweiten Teil des Projekts etwas geben, das diesen Film von anderen Dokumentarfilmen unterscheidet – eine App für Smartphones und andere mobile Endgeräte. Diese App hat das Ziel, sämtliche Inhalte barrierearm zu verbreiten. Auf dem Handy kann man dann die einzelnen Kapitel in einer Hörversion für Menschen mit Sehbeeinträchtigungen, in Gebärdensprache und in leichter Sprache konsumieren – und das in mindestens 20 Sprachen.

KD ***Aber ist es nicht eine Ohnmachtserklärung, dass Du den Film als App anbietest? Gerade diese Technologie ist doch Ziel von Überwachung.***
TR Tatsächlich ist das eine Perversion in sich, weil wir diese Dinge einfach benutzen müssen.

Auch ich muss sie benutzen, um Leute zu erreichen. Der Film muss ein Stück weit ein virales Projekt werden, um erfüllbar zu sein. Nur mit der Hilfe von vielen können wir ein Höchstmaß an Zugangsmöglichkeiten schaffen. Einige Teile des Films sind auch bereits online. Die Kapitel sind zwar noch lange nicht fertig, aber ich möchte schon früh Feedback einholen. Wenn mir jemand sagt: »Das verstehe ich nicht«, dann werde ich versuchen, etwas zu ändern. Etwas, das für Dokumentarfilme relativ unüblich ist.

KD ***Und wie ist das Feedback bisher?***
TR Bisher ist das Feedback positiv. Generell fehlt es einfach an der Öffentlichkeit für das Projekt. Es ist schwer, Menschen im Internet für derartige Themen zu begeistern, wenn ein Buzzfeed-Post nur einen Klick entfernt ist. Außerdem ist es nicht gerade das attraktivste Thema.

KD ***Trotzdem beschäftigst Du Dich schon lange mit Überwachung. Hat die Tatsache, dass Du in der DDR geboren wurdest, etwas damit zu tun, dass Dir dieses Thema vielleicht näher ist als anderen?***
TR Mit Sicherheit. In meiner Familie wurde über die Massenüberwachung in der DDR geredet. Es gab auf vielen Ebenen unterschiedlichste Formen der Repression. Meine Familie mütterlicherseits wurde stark überwacht. Meine Oma ist christlich, mein Opa wollte nicht in die LPG und hat sich wohl unter anderem aufgrund dessen das Leben genommen. Dieses Gefühl nicht frei zu sein, von dem sie mir berichteten, hat mir Eines ganz deutlich gezeigt: Dass das Recht, seine Meinung ohne Angst äußern zu können – ja überhaupt eine Meinung zu haben – ein Grundpfeiler einer aufgeklärten Gesellschaft ist.

KD ***Und was sagen Deine Verwandten heute dazu, dass Du mit Deinem Projekt gegen Überwachung kämpfst?***
TR Meine Familie findet es klasse. Und meine Oma vergisst zwar leider das meiste, das wir ihr erzählen, recht schnell wieder, aber wenn ich ihr sage, was ich mache, sagt sie: Das ist gut.

KD ***Theresia, vielen Dank für das Gespräch.***

LINKS ZUM THEMA

Teaser: www.vimeo.com/zitterart/teaser
Webseite: www.information-doc.org

V. MIT SIRI IN DEN SONNENUNTERGANG

VON SYLVIA LUNDSCHIEN

Im letzten Teil des Roten Fadens fragen wir: Wie wird sich unsere Vorstellung von Privatsphäre in den kommenden Jahrzehnten verändern? Werden wir völlig unbemerkt überwacht? Inwieweit helfen wir bei dieser Überwachung selbst mit? Egal, wie die Welt aussehen wird – auch in Zukunft ist darauf Verlass, dass Prognosen über das Kommende selten rosig sind.

Klimawandel, Bevölkerungswachstum und Migration: Irgendwas ist doch immer. Dass dies auch im Jahr 2030 so bleibt, sagt unter anderem eine Prognose des Bundesministeriums für Bildung und Forschung (BMBF) voraus. Unter dem sperrigen Titel »Gesellschaftliche Veränderungen 2030 – Ergebnisband 1 zur Suchphase von BMBF-Foresight Zyklus II« präsentierten Forscher vor zwei Jahren Trends für das erste Drittel des 21. Jahrhunderts. Dabei kommt auch das Verhältnis zwischen Überwachung und Privatsphäre nicht zu kurz, und so warnen die Autoren für 2030 vor zunehmendem »Hyperpuritanismus« und »Hypertransparenz«. Hyperpuritanismus bedeutet für die Bürger, dass immer mehr Alltagsangelegenheiten zum Anlass für Datensammelei würden, die auch noch mit moralischem Anspruch daherkämen. So warnt der Band schon gegenwärtig vor der Neugier der Krankenkassen und Gesundheitsträger, die Beiträge und Leistungen vom persönlichen Verhalten ihrer Kunden abhängig machen könnten. Wer raucht, Extremsport betreibt oder übergewichtig ist, müsse eventuell Sanktionen oder den Ausschluss aus der Versicherung befürchten.

HOME, SWEET SMART HOME

Das Zuhause der Zukunft wird standardmäßig smart sein, denn unser Leben und Wohnen produzieren Tag und Nacht Daten. Auf Schritt und Tritt folgen uns Kameras, digitale Assistenten und Sensoren: Sie ermitteln, wann wir zuhause sind und steuern Wärme, Licht und Lüftung, kalkulieren unseren Wocheneinkauf und bestellen ihn online. Doch auch unser Lebensumfeld wird mit der »Smart City« intelligenter, denn 2030 leben bereits 60 Prozent der Weltbevölkerung in Städten. In aktuellen Entwürfen wird daher eine vernetzte Infrastruktur diskutiert, mit der Städte Geld sparen, den Verkehr besser steuern und die urbane Lebensqualität erhöhen. Dafür würden aber auch zusätzliche Kameras, Sensoren und Schnittstellen im öffentlichen Raum benötigt, die Bevölkerung und Umraum gleichzeitig vernetzen und überwachen würden. Vor diesem Hintergrund befürchten Kritiker, dass die Anreize der Smart City auch zu mehr Kontrolle im öffentlichen Raum führen, die dann gar als Service etikettiert würden.

Denkbar sind auch tragbare persönliche Computer, wie sie mit der Apple Watch oder Google Glass heute schon existieren. Zukünftig könnten derartige Geräte die gesamte Biografie und alle dazugehörigen Dokumente eines Menschen verwalten. Praktisch für Behördengänge, doch gruselig für den Schutz unserer Intimsphäre. Neue Algorithmen würden in Zukunft vor allem Prognosen über wahrscheinliche Ereignisse treffen und entsprechende Werbung und Produkte anpreisen: Welche Note hat mein Schulabschluss gemessen an meinem Geburtsort? Wann bekommt man das erste Kind – in Abhängigkeit vom Einkommen? Bereits heute nutzen Firmen wie Big Data Scoring ein Verfahren zur Ermittlung der Kreditwürdigkeit anhand von sozialen Profilen. Fraglich bleibt, was mit jenen geschieht, die offline bleiben möchten.

PICKNICK MIT DEN CYBORGS

2030 sinkt die Zahl der Teenager von heute rund 20 Millionen auf knapp 13 Millionen. Dies bedeutet vor allem, dass wir in einer alternden Gesellschaft leben werden, in der viele Arbeiten ohne Roboter oder Cyborgs nicht mehr denkbar sind. Aktuell wird daher diskutiert, dass zukünftig Roboter und intelligente Systeme monotone Tätigkeiten des Niedriglohnsektors übernehmen könnten. Ganz oben auf der Wunschliste stehen Roboter in der Altenpflege, die Oma und Opa rund um die Uhr betreuen. Viele derart personalisierte Maschinen wären damit so etwas wie ein weiteres Familienmitglied – sie wüssten so gut wie alles über Vitalfunktionen, Diagnosen, Medikation und den neuesten Familienknatsch.

Doch wer stellt diese Maschinen her, wer schreibt ihre Software, wer repariert sie und wie viel Souveränität haben die User derartiger Technik? Dies ist heute schon ein Problem, denn wer sich beispielsweise auf Produkte von Apple oder Google verlässt, zahlt in der Regel mit seinen Daten. Die US-amerikanische Professorin Shoshana Zuboff sieht in den wachsenden Monopolen der IT-Giganten die Gefahr, dass User und ihre persönlichen Daten selbst zur Ware würden. Es wäre nur eine Frage der Zeit, wann das Recht, in Ruhe gelassen zu werden, auch zum wortwörtlich unbezahlbaren Luxus würde.

ALTE KONFLIKTE MIT DIGITALER SIGNATUR

In der smarten Stadt würde nicht nur mehr Komfort entstehen, sondern auch neue Konflikte. Bereits heute ist deshalb das sogenannte »Predictive Policing« in den USA weit verbreitet. Eines dieser Systeme zur Prognose von Verbrechen soll beispielsweise in Chicago dafür sorgen, dass »Risikopersonen« identifiziert werden, die als Opfer oder Täter in eine Schießerei verwickelt werden könnten. Dafür führt die Chicagoer Polizei seit 2013 eine sogenannte »Strategic Subject List«, die aktuell laut Bundeszentrale für politische Bildung (BPB) an die 1000 Personen umfasse. Problematisch sei dabei, dass viele der Polizisten keine ausreichende Schulung für das Programm erhielten und nicht genau wüssten, wie sie die Liste anzuwenden haben. Die Software stamme in der Regel von kommerziellen Anbietern, deren geheime Algorithmen keine öffentliche Diskussion über Kriterien zur Erfassung zuließen. Laut BPB betone das Programm bestehende Vorurteile: »Wenn die Polizei etwa verstärkt in bestimmten Vierteln wie sozialen Brennpunkten patrouilliert, erfasst sie dort mehr Kriminalitätsmeldungen, die dann wieder stärker gewichtet in Zukunftsprognosen einfließen.« Dadurch entstehe eine verzerrte Statistik, vor der auch die amerikanische Menschenrechtsorganisation American Civil Liberties Union (ACLU) warnt.

Die Zukunft unserer Privatsphäre braucht daher neue Spielregeln, die wir schon heute entwickeln müssen. Denn bei allem Optimismus über digitalen Fortschritt gehen viele Prognosen davon aus, dass Technologien stets praktisch und zivil seien und ihre Einbettung überwiegend in demokratischen Systemen stattfinde. Doch gegenwärtig wackelt die Weltordnung von den USA bis in die Ukraine. Dies macht es notwendig, dass Technologien und Digitalisierung nicht nur rein wirtschaftliche, sondern auch politische Felder bleiben. So müssen die Monopole der IT-Giganten aufgebrochen werden, denn bereits heute ist die Wirtschaftskraft des Google-Mutterkonzerns Alphabet größer als das Bruttoinlandsprodukt mancher Staaten. Bei einem Bevölkerungswachstum auf 8,3 Milliarden Menschen bis 2030 gäbe es nicht nur mehr Nutzer digitaler Systeme – sondern auch mehr Menschen, die gemeinsam handeln würden. Denn irgendwas ist ja immer. •

DER ROTE FADEN

DIE GEDANKEN SIND FREI

»Die Gedanken sind frei, wer kann sie erraten,
sie fliegen vorbei wie nächtliche Schatten.
Kein Mensch kann sie wissen, kein Jäger erschießen
mit Pulver und Blei: Die Gedanken sind frei!«

Die berühmteste Veröffentlichung des Volksliedes publizierte 1842 **Hoffmann von Fallersleben**. Die Zeilen waren bereits um 1780 auf Flugblättern bekannt, die Melodie seit etwa 1810.

Du hast etwas zu verbergen. Dich und Dein ganzes Leben. Deine Leidenschaften, Deine Gedanken, Deine Wünsche und Träume – Du bist der einzige der entscheiden sollte, wen diese etwas angehen. Denn verbergen ist menschlich. Ein Mensch, der nicht privat sein kann, kann nicht frei sein. Er kann gar nicht sein.

Deine Daten sind Teil Deines Leben – und das ist nicht mehr oder weniger als ein Menschenrecht. Damit in Zukunft nicht wirklich nur noch die gedachten Gedanken frei sind, schließen wir die Überwachungsausgabe mit ein paar geschriebenen Gedanken und Forderungen, die wir als Redaktion für die Erhaltung unser aller Freiheit als essentiell verstehen. ▸

YANNICK

Meine bescheidene Utopie ist, dass die, die meinen, heute nichts zu verbergen zu haben, es aus Solidarität und weiser Voraussicht trotzdem tun. Und dass Edward Snowden verdammt nochmal endlich Asyl in Deutschland angeboten wird.

ALEX

Das Recht auf Privatsphäre gilt als Menschenrecht und ist in allen modernen Demokratien verankert. Eine Erweiterung auf das Grundrecht auf Datenschutz wäre eine notwendige und zeitgemäße Erweiterung des Grundgesetzes ins 21. Jahrhundert. Doch bis es soweit ist, kann man nur selbst versuchen, mehr Bewusstsein für den Umgang mit den eigenen Daten zu schaffen. Julian Assange hat hier in seinem Buch „Cypherpunks« von 2013 ein schönes Gleichnis gefunden: „Ich glaube, die einzig wirksame Verteidigung gegen das kommende Überwachungsregime besteht darin, eigene Schritte zum Schutz der Privatsphäre zu unternehmen, denn den Datenkraken, die heute alles abgreifen können, fehlt jeder Anreiz zur Selbstbeschränkung. Man könnte eine historische Analogie zur Verbreitung des Händewaschens ziehen.

Bevor immer mehr Menschen von den Vorteilen der Handhygiene überzeugt waren, musste erst die Keimtheorie allgemein anerkannt und popularisiert werden. Dann musste man den Menschen auch die Angst vor der Ausbreitung von Krankheiten auf diesem Weg einimpfen, vor der Infektion durch unappetitliches Zeug an den Händen, das unsichtbar war, genauso wie die Massenüberwachung unsichtbar ist. Sobald die Leute ein ausreichendes Verständnis davon hatten, haben ihnen die Seifenfabrikanten dann Produkte zur Besänftigung ihrer Ansteckungsangst geliefert. Es ist notwendig, den Leuten Angst einzujagen, damit sich ein Verständnis für das Problem entwickeln kann und schließlich genügend Nachfrage entsteht, um das Problem zu lösen. Es gibt allerdings auch noch eine Schattenseite der Gleichung, nämlich Programme, die zwar ihrem Anspruch nach durch Verwendung von Kryptografie sicher sind, die aber in Wirklichkeit häufig Mogelpackungen sind, weil Verschlüsselung komplex ist und man den Betrug hinter Komplexität verstecken kann.«

JULIA

Kein Staat im Staat! Auch Nachrichtendienste sollten einer demokratischen Kontrollinstanz unterworfen werden und zwar einer, die auch funktioniert!

KRISTINA

Wir müssen uns intensiv mit unserer Vergangenheit auseinandersetzen, um die Gegenwart zu verstehen.

JOHANNES HAHN

Software ist wichtig – zum Beispiel in der Verwaltung. Dort regiert Microsoft mit Windows und hat so vielfach die öffentliche Verwaltung von seinen Programmen abhängig gemacht. So wollte München seine öffentliche Verwaltung auf das freie Betriebssystem Linux umstellen; der Versuch soll aber quasi auf halber Strecke abgebrochen werden. Man wolle wieder zu „marktüblichen Standards" zurück, so Oberbürgermeister Dieter Reiter. Die städtische Verwaltung von Schwäbisch Hall aber zeigt, dass es auch anders geht: Dort setzt man auf Linux als Betriebssystem und OpenOffice zur Textbearbeitung und Tabellenkalkulation. Die Gemeinde spart dabei sogar Geld. Das zeigt also, dass man sich nicht von privaten Unternehmen abhängig machen muss, um eine öffentliche Verwaltung zu organisieren. Ich würde mir wünschen, mehr Gemeinden würden diesem Beispiel folgen.

SYLVIA

Erinnert Ihr Euch noch an die Verkehrserziehung in der Grundschule? Man lernte rechts vor links, was Straßenschilder bedeuten oder warum man besser einen Zebrastreifen benutzt. Diese Regeln haben den meisten geholfen, sich sicher und selbstständig im Straßenverkehr zu bewegen und Gefahren richtig einzuschätzen. So sollte das doch auch auf das Internet und die Art, wie wir uns in digitalen Infrastrukturen bewegen, angewendet werden. Politik könnte dazu beitragen, genau diese Regeln für alle weiterzuentwickeln – und sich nicht nur für die eigenen Belange oder die großer IT-Konzerne zu interessieren. Dazu gehört auch eine für die Allgemeinheit sicht- und spürbare Debatte über Datenschutz und Datensammelei in Zeiten der Terrorgefahr.

RAIMON

Ich fordere die Politik – also Bundesregierung und Opposition – dazu auf, gemeinsam das neue BND-Gesetz noch einmal zu überdenken und zu reformieren. Es kann nicht sein, dass die Geheimdienste vier Jahre nach Snowdens Enthüllungen weiterhin schalten und walten können, wie es ihnen beliebt. Das Abhängigkeitsverhältnis zur NSA muss ebenso auf den Prüfstand wie eine adäquate Kontrolle der Geheimdienste durch den Bundestag.

ELISA

Wissen ist Macht. Daher ist Bildung im Umgang mit neuen Medien, dem Internet und allem Technologischen da draußen unabdingbar! Und hier geht es nicht nur um Kinder in der Schule. Wir brauchen kostenlose, leicht zugängliche, vielleicht sogar verpflichtende Schulungen für alle von uns. Denn: Kompliziert ist nur das, was man nicht versteht, und schützen können wir uns erst, wenn wir wissen wie.

ARNE

Überwachung schützt nicht vor Kriminalität. Eher leidet die Privatsphäre aller darunter. Ich finde, man hat das Recht, auf die Straße zu gehen und dabei nicht dokumentiert zu werden. Wenn dann noch Bewegungsprofile erstellt werden, gleicht das der Verfolgung jedes Bürgers. Die Regierungen sollten ihr Geld in Sinnvolleres als zum Beispiel Überwachungskameras stecken.

JUDITH

Wir brauchen eine neue Schwerpunktsetzung innerhalb des Bildungssystems. Das fördert momentan nämlich noch zu sehr die Konkurrenz unter Schülern, indem es von einer präzisen Mess- und Vergleichbarkeit schulischer Leistungen ausgeht. Menschen, die dieses Bildungssystem durchlaufen, können sich zwar gut an gegebene Regeln anpassen, aber sie lernen nicht, diese Regeln infrage zu stellen. Der Notendruck sollte deshalb gemildert werden, und den Schülern sollten ihre (politischen) Gestaltungsmöglichkeiten konkret aufgezeigt werden. Außerdem gehört dazu auch die Aufklärung über Missstände in der Bundesrepublik – wie die mangelhafte Aufklärung der NSA-Affäre – verbunden mit dem Verständnis, dass hier immer auch die Zivilgesellschaft gefragt ist, die Behebung von Missständen und den Schutz von Grundrechten einzufordern.

PHILIPP

Wenn man wie bei der Telekommunikationsüberwachung nach der Nadel im Heuhaufen sucht, nützt es nichts, den Haufen größer zu machen. Darum sollte jeder Politiker, der es Polizei und Geheimdiensten einfacher machen will, durch Massenüberwachung Datensätze zu horten, seine Browserhistorie veröffentlichen müssen.

VIKTOR

Meine Utopie ist, dass sich möglichst viele Menschen mit Überwachung als gesellschaftlichem Problem auseinandersetzen. Denn diese Auseinandersetzung – oder eben das Fehlen derselben – wird unsere Zukunft prägen. Somit habt Ihr, liebe Leser, den ersten Schritt mit dem Blick in dieses Magazin schon getan. Der zweite lautet: Diskutiert mit Euren Freunden, engagiert Euch politisch, macht auf Eure Weise deutlich, dass massenhafte Überwachung keine Selbstverständlichkeit ist. Und schon gar nicht ein hinnehmbares Zukunftsszenario.

LEBEN. STUDIEREN. ARBEITEN.

ZEIT CAMPUS – das Studentenmagazin der ZEIT – ist ganz nah dran: am Studium, am Leben, am Berufseinstieg.

Sicher Dir jetzt den idealen Studienbegleiter im Jahresabo für nur 15,– € – gedruckt als Magazin oder digital als E-Paper erhältlich!

ZEIT CAMPUS IM JAHRESABO

6 AUSGABEN FÜR NUR 15,– €

WWW.ZEIT.DE/CAMPUS-JAHRESABO

ZEIT Campus

D E N K A R I U M

Jedes Thema, das wir in der Redaktion und mit dem Team bearbeiten, stimmt auch uns selbst nachdenklich. Welchem Gedanken zur vierten Ausgabe haben wir besonders lange nachgehangen oder welcher hat uns selbst besonders bewegt? Die Beschäftigung mit einem Thema verändert manchmal auch einen selbst und man findet zu neuen Standpunkten und Ideen. Einen Blick in unsere Gedanken möchten wir daher mit Euch im Denkarium teilen.

Die Angst vor Überwachung bleibt ein diffuses Gefühl: Man weiß, dass es sie gibt, kann sich aber immer noch keine konkreten Folgen für das eigene Leben vorstellen. Wenn ich einen unsicheren Browser benutze, wer schaut sich dann an, was ich mache? Und warum sollte das jemanden interessieren? Das tut vielleicht im Moment niemand. Das Verschlüsseln der eigenen Daten dient aber nicht nur dem Schutz derselben – es ist für mich vor allem auch eine politische Aussage. Nämlich, dass es niemals in Ordnung sein kann, wenn ein Staat alles über seine Bürgerinnen und Bürger weiß, weil das potenziell Autoritarismus ermöglicht. Und nur wenn eine Nachfrage besteht, hat der Datenschutz überhaupt eine Chance.
—**YANNICK**, Redakteur

Überwachung ist omnipräsent. Ich fühle mich selbst oft machtlos dagegen. Obwohl ich alle Vorzüge von Technologie genieße und auch nicht auf sie verzichten möchte, fällt es mir schwer, mich damit soweit auseinander zu setzen, dass ich mich und meine Daten wirklich beschützt fühle. Dabei würde ich mich schon in die Kategorie Mensch einordnen, die durchaus ein Grundinteresse für Technologie und ihre Tücken mitbringt. Und trotzdem: Es fällt mir nicht leicht, alles in Anspruch zu nehmen, was es so an Möglichkeiten des eigenen Datenschutzes gibt. Ich finde Facebook praktisch, surfe gern in offenen Netzwerken und habe mein Telefon selten ausgeschaltet. Die vorliegende Ausgabe und hier vor allem unser »Und jetzt kommst Du« finde ich daher super. Ich habe mich nicht nur mehr denn je mit diesem brennenden Thema beschäftigt, sondern finde nun auch in unserer Rubrik wirklich gute Tipps für den Alltag!
—**ELISA**, Redakteurin

Die allumfassende Überwachung ist längst da und wird als zähnefletschende Monstrosität gerade noch durch die dünnen Stäbe des Käfigs, in dem sie sitzt und der sich Demokratie nennt, im Zaum gehalten. Doch die Gitterstäbe lösen sich auf. Die Monstrosität zernagt sie mit immer neuen Möglichkeiten, neuen Räumen, die sie sich erobert, und den schwachen Gesetzen, die ihr das erlauben. Gefüttert wird sie von Staat und Wirtschaft gleichermaßen, die Daten zur Zweitwährung des digitalen Zeitalters erkoren haben und die eigene Hoheit über diese gleich mit. Und von denen, die von Sicherheit und Kontrolle reden – und Unfreiheit meinen. Leise, still und heimlich wird die Monstrosität ihren Käfig eines Tages verlassen und uns verschlingen, wenn wir nicht alle zusammen die Stäbe ihres Käfigs regelmäßig prüfen und erneuern. Denn: Für den Triumph des Bösen reicht es, wenn die Guten nichts tun!
—**ALEXANDER**, Chefredakteur

Eigentlich sollte ich Programmieren lernen. Denn Software wird immer wichtiger in unserem Leben. Eine der Sprachen zu beherrschen, die unser tägliches Leben bestimmen, vom Handywecker bis zum Navigationsgerät, ist eine Form von Selbstbestimmung. Nur fällt das neben Arbeit, Freizeit und Familie ziemlich schwer. Zumindest in der Schule sollte es daher Informatik-Unterricht geben. Außerdem sollten wir alle versuchen, wenigstens im Ansatz zu verstehen, wie die wichtigsten Programme funktionieren. Ansonsten liefern wir uns in die Hände von anonymen Unternehmen.
—**HAJO**, Redakteur

Ich war überrascht, für wie weltfremd man mich hielt, wenn ich Leuten aus meinem Umfeld leidenschaftlich zum Umstieg auf sichere E-Mail-Anbieter wie Posteo oder Messenger-Dienste wie Signal riet. Digitale Überwachung ist so abstrakt, dass keine Notwendigkeit für Veränderung gesehen wird, geschweige denn für Proteste gegen einen Staat, dessen Gesetze einen stetig wachsenden Überwachungsstaat legitimieren. Es braucht wohl einen größeren Knall als Snowden, um die Gesellschaft wachzurütteln. Ich habe Angst, darauf hoffen zu müssen.
—**MARTHA**, Redakteurin

Ich glaube, dass massenhafte Überwachung niemandem egal ist. Ob es um die digitale Assistentin Alexa, unsere Smartphones, Laptops oder gar Kundenkarten im Supermarkt geht – das kann so vielen Menschen nicht egal sein. Trotzdem fühlt sich das oft so an. Kein Wunder: Auch während der Artikelrecherche für diese Ausgabe kam mir Überwachung in ihrer Übermacht wie ein Fass ohne Boden vor. Es wird nicht einfach, sich dagegen zu wehren. Wenn wir uns aber nicht mal trauen zu sagen, dass uns Überwachung nicht egal ist, wird sich eher wenig ändern.
—**VIKTOR**, Gastautor

Öffentliche Daten nützen, private Daten schützen.
—**SASKIA**, Gastautorin

Ich habe Derek Howard vor zwei Jahren auf der Transmediale in Berlin kennengelernt. Dort hat er seinen Film »Doctor Korbes« gezeigt. Nach dem Screening fragte ich Derek nach seiner Email-Adresse, weil ich damals mit dem Gedanken gespielt hatte, meine Masterarbeit über »Voyeurismus« zu schreiben. Derek holte einen Stempel mit seinen Kontaktdaten hervor und drückte ihn in mein Notizbuch. Ein prägendes Erlebnis! Die Masterarbeit habe ich dann doch nicht über »Voyeurismus« geschrieben.
—**ARNE**, Redakteur

Mir ist bewusst geworden, wie grenzenlos die Macht der Geheimdienste ist – sei es der deutsche BND, die amerikanische NSA oder der britische GCHQ. Diese Behörden sammeln im Auftrag des Staates jeden Tag Millionen an Daten über jeden ihrer Bürger. Muss das sein? Als Grund wird stets auf den Kampf gegen den internationalen Terrorismus verwiesen, und nach jedem neuen Anschlag bekommen die Geheimdienste mehr Befugnisse, und unser Recht auf Privatsphäre wird damit weiter eingeschränkt. Wie sollen wir jedoch ohne Privatsphäre noch frei und offen diskutieren können? Es ist an der Zeit, dass unsere Gesellschaft dies erkennt und sich mit allen zur Verfügung stehenden Mitteln dagegen wehrt!
—**RAIMON**, stellv. Chefredakteur

Überwachen ist ein negativ besetzter Begriff. Das ist aber nicht automatisch richtig so. Umso wichtiger ist daher, dass man sich klarmacht, wie sehr einen jeden dieses Thema angeht: Im Internetzeitalter mehr denn je. Was man dabei okay und nicht okay findet, muss jeder für sich herausfinden und sich nicht einfach auftischen lassen.
—**JOHANNES**, Redakteur

Neulich kaufte ich zusammen mit meiner Mutter ihr erstes Smartphone. »Das ist irgendwie ein bisschen DDR«, scherzt sie als wir die Sicherheitsupdates durchgehen, den GPS-Tracker ausstellen und ein Google-Konto mit Fake-Daten anlegen. Es ist einfach ärgerlich, wie schnell Menschen ohne große IT-Kenntnisse auf komplizierte Einstellungen, Updates und AGBs reinfallen können. Große IT-Konzerne reden sich damit heraus, dass sich die User selbst über Datenschutz informieren müssen. Warum aber drehen wir den Spieß nicht einmal um? So müssten digitale Produkte beweisen, dass sie Usern nicht schaden, sie tracken, verfolgen oder heimlich Informationen über sie sammeln. Eine Art Sicherheits-TÜV, der zwingend notwendig wäre, bevor ein Produkt auf den Markt gelangt. Dasselbe gilt für verschachtelte AGBs: Apple, Facebook & Co. müssten ihre Texte in eine kurze und einfache Sprache übersetzen lassen. Denn man staunt oft nicht schlecht, welcher Datenschnüffelei man da ganz arglos zustimmt.
—**SYLVIA**, Redakteurin

Im Laufe der Arbeiten an meinem Beitrag zu Überwachungsparanoia kam mir irgendwann die Frage auf: Wer ist hier eigentlich paranoid? Wir, die wir mit einfachem Klebestreifen unsere Laptopkamera abkleben oder die Geheimdienste, die beispiellose Anstrengungen des Abhörens betreiben? Das ist natürlich nur eine überhebliche Spitzfindigkeit, aber manchmal kommt es beim Denken auch auf eigenwillige Perspektiven und Relationen an, um bei gesundem Verstand zu bleiben.
—**ROMAN**, Redakteur

Die Überwachung in der DDR ist ein spannendes und enorm wichtiges Thema, über das wir sprechen müssen. Für jüngere Generationen ist es fast unvorstellbar, warum, wie und in welchem Ausmaß das Ministerium für Staatssicherheit Menschen damals überwacht und verfolgt hat. Karsten Dümmels Schicksal hat mich fassungslos gemacht und mir vor Augen geführt, welche Rechte wir genießen dürfen. Die Lehren unserer Geschichte zeigen, dass wir Demokratie, Meinungs-, Presse- oder Reisefreiheit nicht als selbstverständlich annehmen dürfen.
—**KRISTINA**, Gastautorin

Ich habe was zu verbergen. Jede Menge sogar. Trotzdem gibt es bei jeder dieser zu verbergenden Tatsachen Menschen, die diese wissen – jeder etwas anderes, niemand alles. Erst die Summe der Einzelaussagen bildet die Gefahr, ein intimes Bild. Deswegen denke ich, hat jeder von uns etwas zu verbergen. Denn, wenn eines Tages rote Gummibärchen verboten werden und in Deiner Akte steht, dass Du welche gegessen hast, als Du fünf warst, kann Dir das zum Verhängnis werden.
—**EVA**, Illustratorin & Redakteurin

UND JETZT KOMMST DU!

Kann der Kampf gegen die Überwachung schon im Privaten beginnen? Wir haben euch eine kleine Liste an Ratschlägen zusammengetragen, wie ihr eure Daten ein wenig besser schützen könnt. Ohne, dass Ihr Eure technischen Geräte gleich in einem Metallsarg verbuddeln und nie wieder auf die Straße gehen müsst.

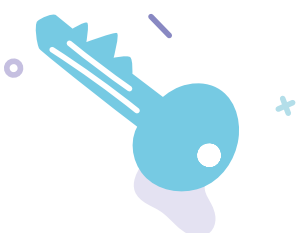
TEXT MARTHA GRASMEIER & YANNICK VON EISENHART ROTHE
ILLUSTRATION PAUL STURM

WELCHES SMARTPHONE IST SICHER?

Hier würden wir Euch gerne *das* massentaugliche Betriebssystem für's Smartphone präsentieren, das Eure Daten schützt. Das gibt es leider bisher nicht.

Bisherige Modelle, die auf höhere Sicherheit gesetzt haben, konnten sich nicht durchsetzen. Vielversprechendster Kandidat war das *Blackphone* von *Silent Circle*, das mit der modifizierten Android-Version *Silent OS* und Verschlüsselung von Nachrichten, Gesprächen und Speicher ausgeliefert wurde. Beide Versionen des Telefons floppten, weil die Geräte sehr teuer waren und die Verschlüsselung nur funktioniert, wenn von Blackphone zu Blackphone kommuniziert wird. Die aktuellste Version ist fast zwei Jahre alt, die dritte Auflage lässt auf sich warten.

Auch Telefone mit dem auf *Linux* basierenden Betriebssystem *Ubuntu-Phone* konnten sich nicht durchsetzen, die Entwicklung von weiteren Versionen ist pausiert.



Man muss also mit dem arbeiten, was man hat. Und dafür gilt, was derzeit so oft gilt: Don't be like the Donald. Mr. Trump nutzt nämlich laut der New York Times immer noch ein »*old, insecure Android Phone*«. Dabei sind regelmäßige Updates wichtig, um Sicherheitslücken zu schließen. Hier sind Nutzer von iPhones klar im Vorteil, weil Apple für seine Telefone deutlich länger Updates zur Verfügung stellt und diese auch immer gleich verfügbar sind. Wenn eine neue Android-Version veröffentlicht wird, müssen die einzelnen Hersteller diese erst implementieren und machen das zudem oft nur für ihre Topmodelle regelmäßig.

Die einzige Möglichkeit, sein Android-Handy regelmäßig updaten zu können, auch wenn der Hersteller dies nicht mehr unterstützt, ist das sogenannte *Rooten*, das Erlangen der vollständigen Zugriffs- und Schreibrechte. Online gibt es viele Anleitungen zu jedem Modell, zu empfehlen ist dies jedoch nur fortgeschrittenen Nerds. Wer nicht genau weiß, was er tut, kann das Gerät damit zerstören. Zudem verfällt mit dem Vorgang jeglicher Garantie-Anspruch.

WIE SICHERE ICH MICH VOR UNBEMERKTEM ABHÖREN?

Die Kamera des Handys oder Laptops abzukleben, erscheint logisch und schützt vor unliebsamen Beobachtern. Anders ist es jedoch mit dem Mikrofon. Es reicht nicht aus, Klebeband über das Mikrofon zu kleben oder es stumm zu schalten. Auch eine extra App herunterzuladen, kann ein Ausspionieren nicht komplett verhindern, da Technik immer umgangen werden kann. In diesem Fall scheint die einzig halbwegs sichere Möglichkeit zu sein, selbst Hand an zu legen.

Hier zwei Vorschläge: Man stecke alte Kopfhörer mit eingebautem Mikro in das Gerät und schneide die Kabel ab. Dadurch schaltet das Handy auf externes Mikro um. Da nun dieses nicht mehr da ist, können keine Geräusche aufgenommen werden. Wichtig ist also dieser Plugin, damit das Handy das externe Mikrofon erkennt. Allerdings muss dabei geschaut werden, dass das Gerät tatsächlich auf dieses umschaltet.

Solltet Ihr zufällig als Agent für den KGB oder einen anderen kuscheligen Verein im Einsatz sein, ist dies jedoch nicht wirksam, da das interne Mikrofon bei einem Hack einfach manuell wieder angestellt werden kann.

Eine andere etwas drastischere Maßnahme wäre das Entfernen der internen Mikrofone, wie es Edward Snowden in einem Video für *Vice News* vormacht. Anschließend ist es nur noch möglich über ein externes Mikrofon zu telefonieren, vor sämtlichen Lauschangriffen ist man jedoch geschützt, so lange das externe Mikrofon nicht gehackt wurde. Dieses Ausbauen ist allerdings etwas komplizierter und Ihr solltet Euch am besten Hilfe von dem Nerd Eures Vertrauens holen.

EINFACHHEIT

SICHERHEIT

ALLTAGSTAUGLICHKEIT

WELCHE ADD-ONS ERHÖHEN MEINE SICHERHEIT IM NETZ?

Wenn Ihr Euch (noch) nicht den Tor Browser heruntergeladen habt, empfiehlt es sich, Browserverlängerungen zu installieren, auch Add-ons genannt. Es gibt Add-ons zur Terminkoordination, Passwortspeicherung und seit kurzem eine, die das Wort »Trump« mit Schimpfwörtern ersetzt, genannt *Detrumpify*. Wir beschränken uns dennoch auf Add-ons, die sich mit Sicherheitsaspekten beschäftigen.

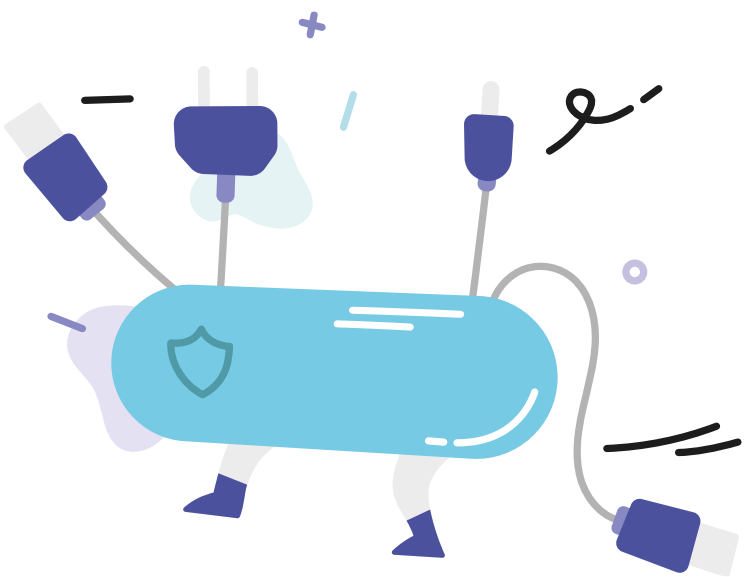
Diese drei vorgestellten, kostenlosen Add-ons, können in verschiedenen Browsern genutzt werden und sind relativ unauffällig, obwohl das Laden von manchen Websites etwas länger dauern kann.

HTTPS Everywhere, nutzt eine sichere SSL/TLS Verbindung, wenn die Website diese unterstützt. Das erkennt man in der URL an dem "S" hinter HTTP.

Allerdings kann trotzdem nicht verhindert werden, dass die aufgerufenen Websites gespeichert werden. Dafür muss Tor genutzt werden oder eine VPN.

Vorhanden bei Firefox, Opera und Chrome.

Ublock Origin, blockt Werbung und Malware und bietet somit werbefreies und sichereres Surfen. Vorhanden bei Firefox, Opera und Safari.



Cookie Controller bietet die Möglichkeit einzustellen, auf welchen Websites Cookies erlaubt sind und wie lange sie gespeichert werden. Cookies bergen an sich keine Gefahr, aber die Informationen aus dem Suchverlauf vereinfachen das gezielte Schalten von Werbung. Dritte Anbieter können dadurch ein umfassendes Bild deiner Persönlichkeit erhalten und nutzen.

Das Add-on erfordert etwas mehr Arbeit, sorgt aber für eine anonymere Präsenz im Netz.

Vorhanden nur bei Firefox, eine Alternative für den Browser Chrome ist das Add-on *Disconnect*.

Habt Ihr diese bereits installiert und dabei Blut geleckt, stellen wir Euch noch zusätzlich ein etwas weiter fortgeschrittenes Add-on für Mozilla Firefox vor. Als kleines Bonbon sozusagen.

Noscript blockiert JavaScript, Java, Flash und andere Plugins, welche sich ansonsten automatisch auf der Website öffnen. Dadurch ist man vor dem Tracking durch dritte Anbieter und vor Skripten mit gefährlichen Inhalten besser geschützt. Das Add-on lässt nur Skripte zu, die zuvor akzeptiert wurden. Die Anwendung erfordert etwas Geduld und technisches Wissen, da man entscheiden muss, welche Skripte notwendig sind und sie dann auf jeder besuchten Website zulassen muss. Zu Beginn braucht man also etwas Zeit, um die Skripte auf den häufiger besuchten Websites zu akzeptieren.

Eine Alternative bei Chrome ist das Add-on *umatrix*.

WELCHER E-MAIL-ANBIETER IST AM SICHERSTEN?

Hallo kuschelmausoo@gmail.com, mjacksonfan234@yahoo.de und katzenjammer@gmx.de. Keine Sorge, Ihr könnt Eure süßen Nutzernamen behalten, habt Ihr allerdings schonmal darüber nachgedacht, wie es mit der Sicherheit von Gmail, Yahoo, GMX und anderen Anbietern aussieht? *Google* und *Yahoo* beispielsweise durchsuchen automatisch die E-Mails zu Werbezwecken. Dienste wie *web.de* und *gmx.de* (die von demselben Unternehmen betrieben werden) sammeln bei der Kontoeinrichtung persönliche Daten. Außerdem stimmt man der Datensammlung zu Marketingzwecken zu, welche dann an andere, mit dem Anbieter verbundene Unternehmen, übermittelt werden.

Viele Anbieter bieten zwar Verschlüsselung wie TLS an, also eine Transportverschlüsselung vom Sender zum Empfänger, allerdings liegen die Nachrichten dabei trotzdem unverschlüsselt auf den Servern des Dienstes.

Man kann seine E-Mails extra sichern, in dem man das PGP Verschlüsselungsverfahren nutzt. Eine andere Möglichkeit wäre ein Anbieterwechsel zu einem Unternehmen, dass sich auf Sicherheit spezialisiert hat.

Alternativen sind *mailbox.org* und *posteo.de*. Diesen wollen wir Euch im Folgenden vorstellen. Die Server von *Posteo* stehen auf deutschem Boden, wodurch sie von den EU- Datenschutzgesetzen geschützt sind. Das Unternehmen erlaubt eine anonyme Anmeldung, ist werbefrei und bietet mehrere Alias-Adressen. Zusätzlich dazu ist eine 2-Faktor- Authentifizierung (TOTP) möglich, TLS verschlüsselter Zugriff und TLS verschlüsselter Transportweg (wenn der Server des Empfängers dies auch unterstützt) und eine Ende-zu- Ende-Verschlüsselung ist einrichtbar. Ein Krypto-Mailspeicher verschlüsselt Mails auf dem Server, sodass weder der Dienst noch Behörden darauf Zugriff haben (Achtung: Das Vergessen des Passwortes führt zum Verlust aller Daten).

Oder, um es für den Laien zu sagen: Alles ziemlich sicher!

Das Ganze kostet zwar etwas zusätzliche Arbeit, aber der Anbieter bietet Hilfe bei der Einrichtung der einzelnen Verschlüsselungsmöglichkeiten an. Solange Eure Freunde und Familie nicht bei einem solchen Anbieter angemeldet sind, bleibt immer das Risiko Eurer Authentifizierung durch den Kontakt mit ihnen. Versucht also Überzeugungsarbeit zu leisten und möglichst viele zu einem Wechsel zu überreden.

Anders als andere Anbieter gibt es diesen Dienst allerdings nicht für umme: 1€ kostet er pro Monat. Die Bezahlung kann jedoch anonym getätigt werden und ist neben normaler Überweisung per Bitcoin oder Barzahlung möglich. Wir finden, dafür kann man sich einen Kaffee-to-go im Monat sparen.

EINFACHHEIT

SICHERHEIT

ALLTAGSTAUGLICHKEIT

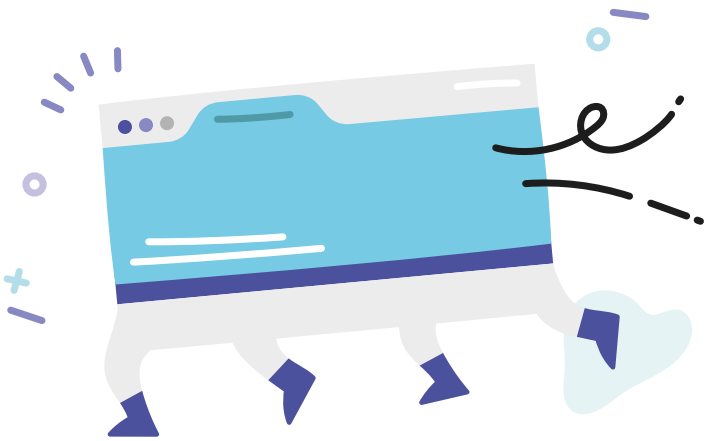
WELCHER BROWSER SCHÜTZT MEINE PRIVAT-SPHÄRE?

Wer auf der Suche nach einem überwachungssicheren Browser ist, der kommt um Tor nicht herum. In der öffentlichen Wahrnehmung hat der Tor-Browser einen zwielichtigen Beiklang, weil er meist mit der Verbindung zum sogenannten Darknet in der Berichterstattung auftaucht. Achtung, die erste Tor-Erfahrung könnte enttäuschen: Man betritt keine mystische Unterwelt der Gesetzlosen und Dissidenten, stattdessen sieht das Ding erstmal fast so aus wie dein normaler Browser. Der Unterschied: Alle Anfragen werden anonymisiert über verschiedene Server des weltweiten Tor-Netzwerkes geschickt. So hinterlässt der User keine Spuren, die ihm direkt zuzuordnen sind. Das verlangsamt die Internetverbindung zwar merklich, hält sich aber in unserem Test in erträglichem Rahmen, selbst HD-Videos laufen meist flüssig.

Einiges ist dann doch anders als gewohnt: Der Browser zeigt immer an, in welchen Ländern die Server stehen, über die deine Verbindung gerade läuft. Die Server sind zufällig ausgewählt und wechseln bei neuen Anfragen. Das führt zu ungewohnten Vorschlägen bei YouTube und Problemen bei geogeblockten Diensten. Soziale Netzwerke begegnen Tor mit Argwohn: Twitter zum Beispiel lässt den Log-In erst nach Verifizierung durch einen zugemailten Code zu und informiert danach über einen »verdächtigen Zugriff aus Roubaix, Frankreich«. Nach mehrmaliger Nutzung hört das aber auf, außerdem widerspricht die Nutzung von personalisierten Accounts bei Datenkraken sowieso der Nutzungslogik von Tor.

Zusammengefasst: Tor ist vielleicht nicht der neue, sichere Browser für die Massen und eignet sich nicht für den gemütlichen Netflix-Abend. Er ist aber auch keine dubiose Anlaufstelle für Kriminelle, sondern ein unterstützenswertes Projekt für mehr Privatsphäre und eine Alternative, die Du in Erwägung ziehen solltest, wenn Du nicht willst, dass Dein Provider weiß über welche Geschlechtskrankheit Du Dich informierst oder welchen Porno Du gerade schaust.

Mehr dazu in unserem Artikel übers Darknet auf Seite 48.



EINFACHHEIT

SICHERHEIT

ALLTAGSTAUGLICHKEIT

WELCHER MESSENGER IST AM SICHERSTEN?

Du nutzt WhatsApp, deine Mutti nutzt WhatsApp, die Kater Demos-Redaktion nutzt WhatsApp – oder nutzte es bis zur Arbeit an dieser Ausgabe, dazu später mehr.

Der Messenger gehört zwar zu Facebook, ist aber tippitoppisicher seit er die Ende-zuEnde-Verschlüsselung eingeführt hat, oder? So einfach ist es leider nicht. Anfang des Jahres berichtete der Guardian über eine Sicherheitslücke, die Experten in der WhatsApp-Verschlüsselung entdeckt haben. Diese ermöglicht zwar keine Massenüberwachung, bietet aber Facebook oder auch Behörden und Nachrichtendiensten die Möglichkeit, einzelne Nachrichten gezielt abzufangen und zu entschlüsseln. Auch wenn das Risiko für Otto und Anna Normalverbraucher wohl eher gering einzuschätzen ist, fühlt sich damit nicht jeder wohl. Deshalb werfen wir einen Blick auf ein paar Alternativen.

Der Musterschüler der sicheren Messenger hört auf den Namen Signal, genutzt und empfohlen von Edward Snowden. Signal ist kostenlos und für Android und iOS verfügbar.

In Sachen Funktionalität steht der Dienst WhatsApp in nichts nach. Sprachnachrichten, Dateien, Fotos, Kontakte und Gifs, alles kann einfach verschickt werden. Besonders wichtig für uns: Auch in Sachen Katzenemojis müssen keine Abstriche gemacht werden. Ein Add-on für Google Chrome holt Signal auch auf den Desktop, das freut die Zehn-Finger-Schreiber.

Signal unterstützt auch verschlüsselte Internettelefonie. Im Selbstversuch funktionierte diese jedoch trotz stabiler W-Lan-Verbindung nur mit mäßiger Tonqualität und starker Verzögerung.

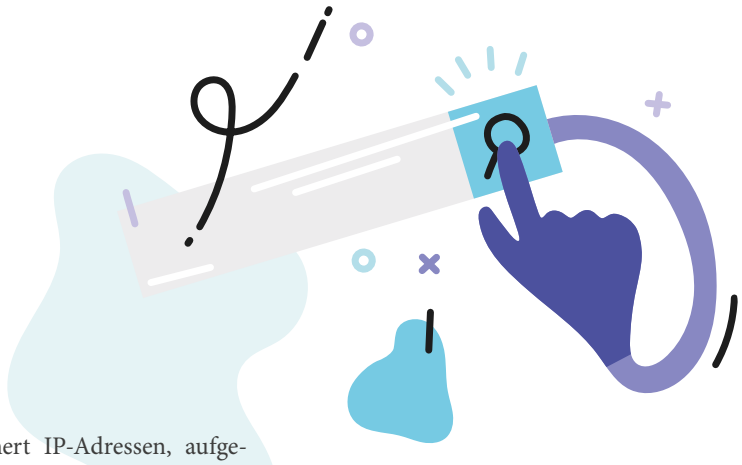
Weitere Alternativen sind Threema (iOS, Android, Windows Phone - 2,99 Euro) und Wire (iOS, Android - kostenlos), alle mit ähnlichen Funktionen und Sicherheitsstandards. Threema wird zwar dafür kritisiert, seinen Code nicht offen zu legen, bietet dafür aber als einziger der Dienste eine anonyme Nutzung ohne Verknüpfung mit Telefonnummer oder Mailadresse an.

Bleibt nur noch dieser eine, kleine Vorteil, den WhatsApp allen Alternativen voraus hat: Alle nutzen es, Wechsler haben zunächst mal das Gefühl, etwas zu verpassen. Wem höchste Sicherheitsstandards wichtig sind, der sollte sich davon jedoch nicht abschrecken lassen. Was die Kater Demos-Redaktion kann, dass schafft Ihr auch: Sprecht mit Euren Freunden, Familien und Kollegen darüber und wagt gemeinsam den Wechsel. Und vor allem: Vorsicht vor Facebook-Messenger und der guten, alten SMS, die haben nämlich gar keine Verschlüsselung.

EINFACHHEIT

SICHERHEIT

ALLTAGSTAUGLICHKEIT



WELCHE SUCHMASCHINE SCHÜTZT AM BESTEN MEINE PRIVATSPHÄRE?

Google speichert IP-Adressen, aufgerufene Links, den Zeitpunkt der Suche und Cookies erlauben es dem Unternehmen, Eure Interessen anhand der Suchverlauf ausfindig zu machen. Dadurch kann spezifisch Werbung geschaltet werden und es entsteht ein umfassendes Bild Eurer Persönlichkeit. Man kann sagen: Google kennt Dich besser als Deine Freunde. Na, nervös? Vielleicht nicht ganz unberechtigt.

Alternativen gibt es. Zum Beispiel das amerikanische Unternehmen *DuckDuckGo* oder die niederländische Suchmaschine *Startpage* (*Ixquick*), die zur Recherche dieses Artikels genutzt wurde.

Startpage läuft über eine sichere SSL/TLS Verschlüsselung. Hier wird Deine IP Adresse nicht gespeichert und es gibt keine Tracking-Cookies, die Deine Suche aufzeichnen und Dich somit auffindbar machen könnten. Anders als bei Google befindest Du Dich also nicht in der sogenannten »Filter Bubble«, die Suchergebnisse nach vorhergegangenen sortiert.

Neben jedem aufgelisteten Suchergebnis findet sich der Button »Proxy« (bei *DuckDuckGo* nicht vorhanden), welcher anonymes Öffnen von Websites ermöglicht, sofern diese vom Proxy unterstützt werden. Schließlich nützt eine anonyme Suchmaschine nicht viel, wenn beim Öffnen der Website die eigenen Daten doch wieder gespeichert werden können.

Ein weiterer Vorteil gegenüber *Google* ist, dass *StartPage* als niederländisches Unternehmen nicht unter den US Patriot Act fällt. Dieser verpflichtet Unternehmen mit Servern auf amerikanischem Boden zur Herausgabe persönlicher Daten an US-Behörden.

Obwohl *StartPage Googles* Suchergebnisse nutzt, geschieht dies unter oben genannten Sicherheitsbedingungen, weswegen die European Privacy Seal, dem Unternehmen als erster Suchmaschine überhaupt ein Zertifikat für Sicherheit unter dem europäischen Datenschutzrecht bestätigte.

EINFACHHEIT

SICHERHEIT

ALLTAGSTAUGLICHKEIT

WAS DU SONST NOCH TUN KANNST

Neben der technischen Optimierung Deiner Geräte gibt es natürlich auch noch andere Möglichkeiten, wie Du dich schützen kannst.

INFORMIER' DICH!

Datenschutz und Überwachung sind nicht die sexy Themen, die es zu den Anne Wills und Frank Plasbergs dieser Republik schaffen. Deshalb muss man sich seine Informationen selbst suchen. Besonders gut geht das auf netzpolitik.org. Die journalistische Plattform engagiert sich für digitale Freiheitsrechte und sollte den meisten seit ein Begriff sein, seit gegen sie wegen angeblichem Landesverrat ermittelt wurde.

ENGAGIER' DICH!

Der Kampf für Privatsphäre wird nicht durch Installation eines Browsers oder einer App gewonnen, politisches Engagement muss eine große Rolle spielen. Was man machen kann? Einfach mal eine NGO gründen! Das hat sich eine Gruppe von Juristen um den Berliner Landesrichter Ulf Buermeyer und die Hamburger Professorin Nora Markard gedacht und die Gesellschaft für Freiheitsrechte gestartet. Die GFF kämpft durch Klagen gegen Eingriffe in Informations- und Pressefreiheit und koordiniert zum Beispiel eine Verfassungsbeschwerde gegen das neue BND-Gesetz.

Wenn Du aber keine Zeit hast, eine NGO zu gründen, Dich in den Bundestag wählen zu lassen oder ein supersicheres Betriebssystem für Smartphones zu schreiben, unterstütze Leute, die das für Dich machen.

MACH NE PAUSE!

In seinem Buch »Wem gehört die Zukunft?« beschreibt der Computerwissenschaftler Jarod Lanier das Heranwachsen einer »Informationswirtschaft«, in der mit Userdaten Vermögen verdient werden. Das Nutzen von Facebook und Co sei also nicht gratis, jeder bezahle mit seinen Daten. Deshalb fordert er: Um eine humanistische Informationswirtschaft aufzubauen, müssten User für ihre Daten bezahlt werden. Da das aber nicht so bald passieren wird, hilft nur Boykott. Er schlägt seinen Lesern vor, in einem Selbstversuch ein halbes Jahr auf alle kostenlosen Internetdienste zu verzichten. Damit müsse man zwar einem erheblichen sozialen Druck widerstehen, Lanier verspricht aber: »Sie werden wahrscheinlich Dinge über sich selbst, Ihre Freunde, die Welt und das Internet erfahren, die Ihnen sonst entgangen wären.«

Das klingt radikal, ist aber momentan vielleicht der einzige Weg, um sich wirklich konsequent gegen Datenkraken zu wehren.

BUCH-TIPP

Jarod Lanier: Wem gehört die Zukunft? (2014)

DIE SCHNELLSTEN WEGE ZU UNS

Für alle, die Artikel kommentieren wollen:
redaktion@katerdemos.de

oder an die Verlags- und Redaktionsadresse:
Kater Demos, Frankfurter Allee 43, 10247 Berlin

Wir freuen uns über Eure Zuschriften. Je kürzer, desto höher die Chance, dass sie auch veröffentlicht werden. Bitte nenne Deinen kompletten Namen und Wohnort, den würden wir zu Deinem Leserbrief abdrucken. Die Redaktion behält sich vor Leserbriefe zu kürzen.

Für alle, die eine Frage zu einem Artikel haben:
Betrifft sie einen bestimmten Artikel, erreichst Du unsere Redakteure direkt. Unsere Mailstruktur ist einfach:
vorname@katerdemos.de

Betrifft Deine Anfrage einen unserer Gastautoren, schreib einfach an: redaktion@katerdemos.de

Für Autoren, die ein Thema für die nächste Ausgabe vorschlagen wollen (der Schwerpunkt ist »Das Fremde«):
redaktion@katerdemos.de

Für Leser, die ein Einzelheft bestellen möchten:
Schaut vertrauensvoll in unseren Online-Store vorbei:
https://holvi.com/shop/katerdemos/

Für Leser, die ein Abonnement bestellen möchten:
abo@katerdemos.de

Noch ist die Kater Crew ein wilder Haufen Magazinmacher, der das ehrenamtlich nebenher stemmt. Daher wissen wir selbst auch nicht so genau, wann unsere nächsten Ausgaben kommen. Nur so viel: Sie kommen. Die nächste Ausgabe hat den Schwerpunkt »Das Fremde«. Magst Du trotzdem ein Abo haben, kannst Du unser unkonventionelles Growing Cat Supporter Abo bestellen, das kostet je nach enthaltenen Ausgaben und ist über unseren Online-Store (https://shop.katerdemos.de) erhältlich.

Für alle, die uns online folgen möchten:
Ihr findet uns auf den gängigen Plattformen:
www.facebook.com/katerdemos
www.twitter.com/katerdemos
www.instagram.com/katerdemos
www.katerdemos.de

Für alle, die sich fragen, wo die Digitalausgabe bleibt:
Du bist Programmierer und hast Zeit? Melde Dich! <3
Bis dahin gilt: Abwarten und Tee trinken. Und für alles andere kannst Du uns einfach schreiben:
info@katerdemos.de

We are proud to be an Indiemag.

Für alle, die sich fragen, warum hier eine Anzeige drin ist:Wir haben für unsere Medienausgabe mit drei Medien einen Anzeigentausch gemacht: Sie werben bei uns, wir bei ihnen. Manchmal klappt das mit den Deadlines aber nicht so, wie man sich das wünscht. Daher ist die ZEIT Campus erst jetzt dabei.

Die nächste Ausgabe »Das Fremde« erscheint im Winter 2017.

IMPRESSUM

HERAUSGEBER
Kater Demos Verlag

CHEFREDAKTEUR
Alexander Sängerlaub (V.i.S.d.P.)

REDAKTION
Elisa Bilko, Kris Catz, Martha Grasmeier, Yannick von Eisenhart Rothe, Johannes Hahn, Johannes Heim, Choleda Jasdany, Sylvia Lundschien, Raimon Klein (stellv. Chefredakteur), Roman Obst, Eva Palm, Arne Siegmund, Julia Stürzl

GASTAUTOREN IN DIESER AUSGABE
Lara Bogan, Jonas Ibel, Viktor Marinov, Judith Pape, Kristina Regentrop, Larissa Robitzsch, Saskia Sell, Philipp Steffens

LEKTORAT
Benjamin Birkner, Andreas Eder, Christina Große, Heidi Marleen Kuhlmann, Cilly Kurkhaus, Thomas Mautrich, Christiane Mehlig, Bastian Peters, Regina Pirogoff, Berit Rohde, Anne Schulze, Christina Spitzmüller, Anna Maria Stock, Viviane Stroede, Enrico Wagner

KREATIVDIREKTOR
Steffen Gorski

FOTOGRAFIE / BILDREDAKTION
Johannes Berger, Me Chuthai, Sima Ebrahimi

ILLUSTRATION
Steve M. Clements, Sophie Dreher, Philipp Haacke, Marika Haustein, Marc Heinrich, Heidrun Kleingries, Richard Klippfeld, Natascha Kornilowa, Matti Michels, Teresa Mönnich, Eva Palm, Sophia Schrade, Anne Selling, Anni Stelke, Volker Sträter, Paul Sturm, Jana van Thiel, Florian Thiemann

GESTALTUNG UND SATZ
Steffen Gorski

EVENTs
Silva Moderzinski, Anne Schulze

SUPPORT UND DANK
Volker Lilienthal & der Studiengang »Journalistik und Kommunikationswissenschaft« an der Universität Hamburg, Hoc Littmann & der Studiengang »Illustrationsdesign« an der Akademie für Illustration und Design Berlin (AID), Mitja von Eisenhart Rothe, Alexa Kern, Eftimios Tsituridis, Die Brueder/Indiecon

GESCHÄFTSFÜHRUNG
Alexander Sängerlaub, Franziska Teubert

DRUCK
Königsdruck GmbH
Alt-Reinickendorf 28
13407 Berlin
Danke an Désirée Eiben & Ingrid Hartwig

Dieses Magazin wurde auf Recyclingpapier gedruckt.

VERTRIEB
DPV Deutscher Pressevertrieb GmbH
www.dpv.de
Danke an Guido Lange und Marc Göbel

REDAKTIONS- UND VERLAGSSITZ
Kater Demos Verlag UG (haftungsbeschränkt)
Frankfurter Allee 43
10247 Berlin

BANKVERBINDUNG
Holvi, IBAN: FI41 7997 7997 0545 93 , BIC: HOLVFIHH

MAGAZINPREISE
Einzelheft: 9,80 Euro in Deutschland (Österreich: 11,50 Euro, Luxemburg: 11,80 Euro, Schweiz: 15,50 SF), Abonnement (für alle bisher erschienenen Ausgaben): 59 Euro, Auslandspreise auf Anfrage (abo@katerdemos.de), das Abonnement ist jederzeit kündbar.

»Kluge Köpfe, frischer Wind, viel Herz!«
Juliette, unsere Leserin

»Utopien für alle«
Norddeutscher Rundfunk

»Kater Demos ist ein ernsthaftes Heft. Es eignet sich nicht für die Badewannen-Blätterlektüre, sondern will eher tagelang im Rucksack herumgetragen, zergrübelt und mit Eselsohren versehen werden.«
Süddeutsche Zeitung

»Katzen, Katzen, Katzen!«
Würde Helmut Markwort vielleicht sagen, wenn wir ihn dazu zwingen würden.

04
4 190749 909804
D 9,80€ | A 11,50€ | CH 15,50 SFR | LUX 11,80€