Über den höchst unterschiedlichen Umgang mit persönlichen Daten und Datenschutz, Privatsphäre und staatlicher Überwachung – exemplarisch die Situation in den USA, in Ägypten, in der Schweiz und in Südkorea

Wenn Mr. Hähnchen und Mrs. Baileys shoppen gehen

Über den Umgang der US-Amerikaner mit Daten

Frank Herrmann aus Washington

Neulich in San Francisco, im Commonwealth Club of California. Bruce Schneier, amerikaweit einer der führenden Experten auf dem Gebiet der Computersicherheit, philosophiert über das zwiespältige Verhältnis, das seine Landsleute zu Big Data haben. „Verlangte die Regierung von uns, jederzeit Überwachungsgeräte bei uns zu tragen, gingen wir natürlich auf die Barrikaden. Forderte uns das FBI dazu auf, ständig im Bilde darüber zu sein, was unsere Freunde gerade tun, würden wir alle sofort zu Rebellen."

Aber tue man Letzteres nicht, indem man immerzu bei Facebook nachlese, von Facebook alarmiert werde, wenn Freunde auch nur ein neues Foto ins Netz gestellt hätten? Wer in allen Lebenslagen sein Handy in Reichweite habe, nehme der nicht billigend in Kauf, jederzeit anzuzeigen, wo er sich gerade aufhält? Nur: Wolle er deswegen auf ein so praktisches Hilfsmittel wie ein Handy verzichten?

„Wir leben im goldenen Zeitalter der Überwachung", sagt Schneier. Computer, Überwachungskameras, Smartphones, elektronische Ladenkassen: alles Instrumente, um Daten zu speichern. Und weil das Datenspeichern so preiswert geworden sei, betreibe man es bis zum Exzess.

Die NSA, fügt Schneier hinzu, handle per se nach dem Grundsatz: „Kannst du es sammeln, dann sammelst du es" – eine Mentalität des Vollständigkeitswahns. Sie zu bremsen könne nicht mit technischen Mitteln, es könne nur durch politisches Handeln geschehen.

> „Das größte Risiko für die Firmen ist, dass sich Hacker der Daten bemächtigen und die Düpierten mit Sammelklagen reagieren."

Wobei immer wieder festzustellen ist, dass die Abhöroffensive der NSA ausgesprochen differenzierte Reaktionen hervorruft, je nachdem, ob sie Amerikaner betrifft oder „nur" das Ausland. Lautstarke Proteste (und nachfolgende Reformen, wenn auch bescheidene), wenn es um das lückenlose Sammeln der Verbindungsdaten einheimischer Telefonkunden geht. Eher ein Achselzucken, einmal abgesehen von Anwälten und Aktivisten an den liberalen Küsten, wenn das weltweite Ausspähen des Internets, wenn die Privatsphäre Bürger anderer Staaten zur Debatte steht. „America first", kann man sagen.

Der gläserne Kunde

Mitteleuropäer behaupten gern, der Datenschutz in den USA sei unterentwickelt. Das stimmt. Als Nachrichten die Runde machten, denen zufolge die Lufthansa nicht lückenlos informiert gewesen sei über die Krankengeschichte des Piloten Andreas Lubitz, reagierten Nachbarn in Washington mit verständnislosem Kopfschütteln. Was Amerikaner indes immer heftiger umtreibt, ist die Aussicht auf eine Konsumwelt, in der sie zu gläsernen, ausrechenbaren, anhand jeder Kaufentscheidung vermessenen Kunden werden.

Eine Studie der University of Pennsylvania, veröffentlicht Anfang Juni, zeichnete ein Bild, wie es nicht unbedingt zu erwarten war. Ein Bild profunder Skepsis. Denn eigentlich erfreuen sie sich großer Beliebtheit, die personalisierten Empfehlungen, wie sie etwa Online-Handelsriese Amazon bei jeder Gelegenheit gibt.

Selbst Schneier, ein scharfzüngiger, witziger Kämpfer in Sachen Privatsphäre, räumt ein, dass er es mag, wenn ihm hin und wieder ein Tipp ins digitale Postfach flattert. Warnt Google Maps vor aktuellen Verkehrsstörungen auf einer von ihm angegebenen Route, findet er das nützlich, auch wenn es voraussetzt, dass er Google Maps quasi einweiht in seine hochprivaten Streckenpläne.

In jedem größeren Supermarkt schieben einem die Kassierer seit Jahren ganz selbstverständlich einen oder auch mehrere Kupons übers Laufband. Beim nächsten Mal bedeuten sie einen Preisnachlass, wenn man, sagen wir, Haselnusseis oder Erdbeerjoghurt oder Snacks der Sorte Tex-Mex erwirbt. Einen Rabatt auf Haselnusseis, Erdbeerjoghurt und Tex-Mex, jedenfalls auf Waren, bei denen der Supermarktrechner ermittelt hat, dass man sie öfter kauft.

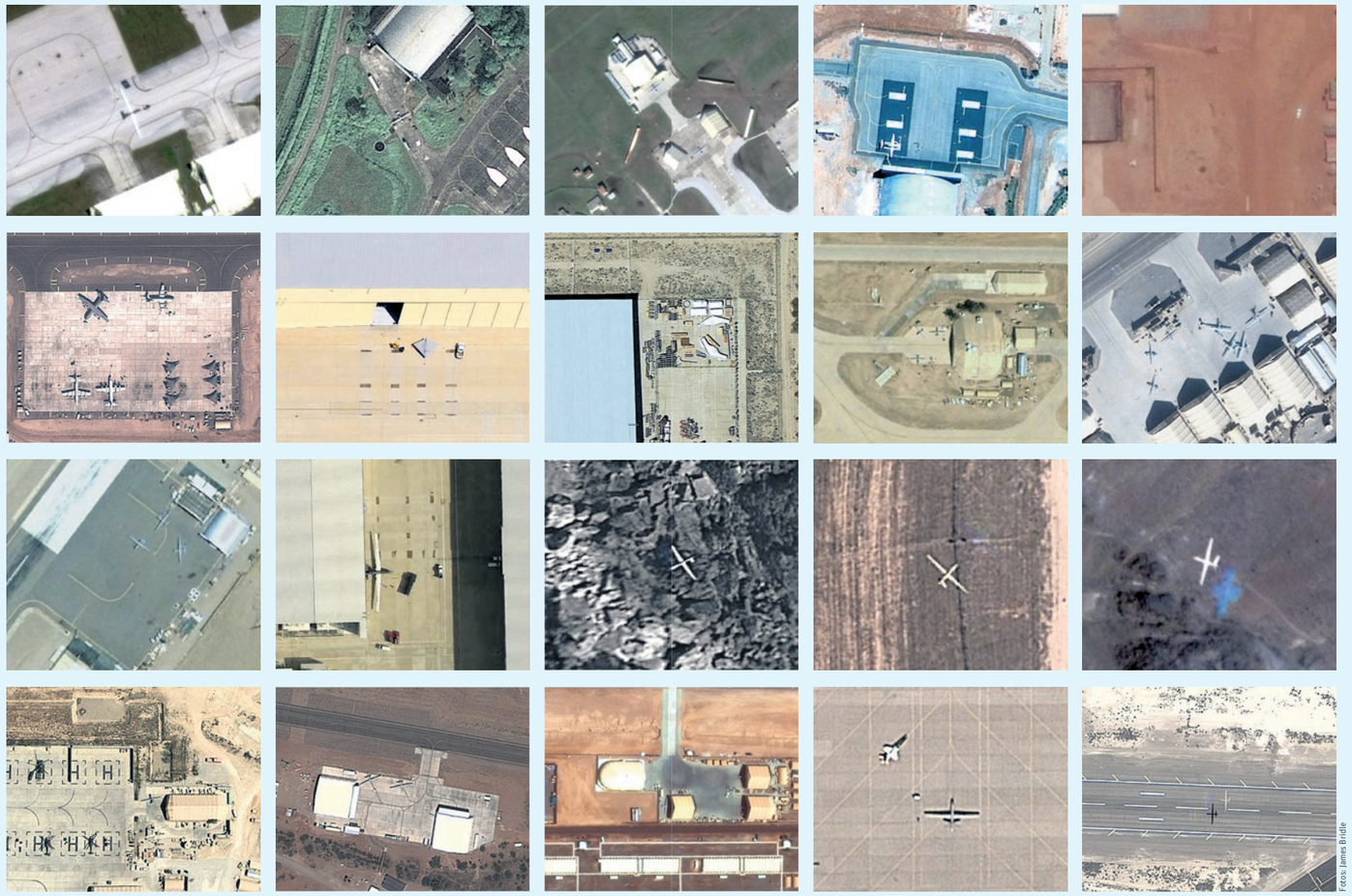
„Just for you"-Liste

Auch nicht mehr ganz neu ist die Rubrik „Just for you": Wer will, kann auf der Supermarkt-Website Posten für Posten eine Liste durchgehen, die ganz individuell auf einen selbst zugeschnitten ist. Sie haben vor drei Wochen bei den Hähnchenschenkeln zugeschlagen? Bitte sehr, wenn Sie wieder welche nehmen, wird es besonders billig für Sie! Kreuzen Sie an! Und beehren Sie uns bald mit Ihrem Besuch! Ein Drittel Discount, ganz individuell, versteht sich, ist durchaus üblich.

So verlockend das klingen mag – Schneier verbindet mit dem Trend ein Szenario, bei dem die Handelsketten die Menschen in Schubladen sortieren. Der Joghurtfreund. Mr. Hähnchen. Mrs. Bailey's. Oder aber, diskriminierender: das Dorf, in dem keiner Geld hat. Die Altenenklave mit Niedrigeinkommen usw.

Aber zurück zur University of Pennsylvania. „Viele Amerikaner halten das Tauschgeschäft – persönliche Daten gegen personalisierte Dienstleistungen oder Schnäppchen – nicht für einen fairen Deal", fassen die Autoren der Studie ihre Erkenntnisse zusammen. Ob es okay sei, dass der Laden, in dem ich shoppe, meine Informationen sammelt, um ein genaueres Konsumentenprofil meiner Person entwickeln zu können, hieß eine Frage. 55 Prozent beantworteten sie mit Nein.

Das größte Risiko für die Unternehmen, der potenziell wichtigste Faktor, um sie zu bremsen, besteht aus Schneiers Sicht in der Gefahr, dass sich Hacker sensibler Kundendaten bemächtigen und die Düpierten mit einer Sammelklage reagieren. Was in Amerika mit exorbitanten Schadensersatzzahlungen enden kann. Dem werde sich die Geschäftswelt irgendwann anpassen, prophezeit er, und nicht mehr wie mit dem Staubsauger aufsaugen, was immer an Daten verfügbar sei. Sein wirksamster Beitrag zum Schutz des Privaten bestehe im Übrigen darin, nicht auf Facebook zu sein. „Das stempelt mich zwar zum komischen Kauz, aber es macht mich auch höchst produktiv."



Was wäre, wenn die unsichtbaren Überwacher selbst plötzlich überwacht würden? In der „Watching the Watchers" betitelten Werkreihe sammelt der Londoner Künstler James Bridle Luftaufnahmen von militärischen Drohnen, die er alle via Online-Karten aufgespürt hat – in Nevada, Pakistan oder im Jemen; im fliegenden Einsatz, geparkt vor dem Hangar, auf Start- und Landebahnen. Alle Fotos samt genauer Ortsangaben sind auf Flickr öffentlich dokumentiert.

Fotos: James Bridle

Wenn sich der Staat in den privaten Computer schleicht

Die Schweiz erlaubt weitreichende Überwachung

Klaus Bonanomi aus Bern

Es klingt rührend harmlos, riecht ein bisschen spießbürgerlich, als könnte es niemandem ein Haar krümmen: Büpf, das neue Schweizer Polit-Schlagwort, die Abkürzung für das neue „Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs". Es gibt den Strafverfolgern neue Mittel im Kampf gegen Kriminelle in die Hand. Gleichzeitig mit dem Büpf genehmigte das Parlament ein neues Nachrichtendienstgesetz, um auch die Staatsschützer besser zu munitionieren gegen Terror und andere Gefahren. Doch weil mit diesen Gesetzesverschärfungen allzu stark in die Grundrechte der Bürgerinnen und Bürger eingegriffen werde, wollen Jungsozialisten und Grüne Unterschriften sammeln, um eine Volksabstimmung zu erzwingen.

Wanzen waren gestern

Wurde früher einfach ein Telefon eines Verdächtigen angezapft oder eine Wanze platziert, um Gespräche aufzuzeichnen, darf der Staat nun auch „Trojaner" in die Computer von Verdächtigen einschleusen, um die Kommunikation übers Internet, etwa via Skype oder Whatsapp, zu überwachen. Kritiker fürchten, dass damit auch die Computer selber manipuliert werden könnten, um Beweismittel zu fälschen oder zu fabrizieren. Ferner darf der Staat künftig auch IMSI-Catcher einsetzen, um Handys zu orten und abzuhören.

Künftig darf der Nachrichtendienst des Bundes auch im Ausland Kabelaufklärung betreiben, also Signale aus leitungsgebundenen Netzen erfassen, da auch Terrororganisationen zunehmend über Internet kommunizieren.

Es gehe nicht an, dass die Kriminellen die neuen technologischen Möglichkeiten nutzen könnten, während die Ermittler bloß veraltete Methoden zur Verfügung hätten, argumentierten die Befürworter der neuen Gesetzgebung. Es gehe nicht um präventives Schnüffeln, sondern um schwere Straftaten, betonte der Abgeordnete Karl Vogler von der christdemokratischen CVP: „Wir müssen den Strafverfolgungsbehörden die notwendigen Instrumente für eine wirksame Strafverfolgung in die Hand geben."

Auch eine verlängerte Vorratsdatenspeicherung wurde genehmigt. Während eines Jahres müssen die Telekom-Anbieter künftig die Randdaten aller Gespräche speichern: wer wann mit wem von wo aus wie lange gesprochen hat.

Dies kritisierte der grüne Abgeordnete Daniel Vischer: „Nicht von ungefähr hat der Europäische Gerichtshof diese Vorratsdatenspeicherung mit dem Recht der persönlichen Freiheit – einem der höchsten Güter im Verfassungsstaat – als unvereinbar erklärt."

Auch ein Teil der rechtskonservativen und staatskritischen SVP lehnte die neuen Gesetze ab: „Der Staat soll die Bürger schützen und nicht unter Generalverdacht stellen", mahnte Lukas Reimann. „Mit dem Büpf entscheiden wir, ob die Schweiz weiter ein Land der Freiheit und Bürgerrechte sein will oder ob sie zu einem Polizei- und Überwachungsstaat verkommt!"

Dem hielt die sozialdemokratische Justizministerin Simonetta Sommaruga entgegen, man solle nicht nur die Grundrechte der Täter thematisieren, sondern auch jene der Opfer. Es gehe darum, bei schweren Straftaten wie Kindsentführung einschreiten oder Pädophilen-Ringe aufdecken zu können. Damit erhielt die Ministerin die Unterstützung der bürgerlichen Parlamentsmehrheit und der Mehrheit ihrer Parteigenossen.

Der Spion, der vor der Haustür steht

Er ist eine ägyptische Institution, der Bawab – der Mann an der Tür in ägyptischen Häusern. Er wacht über das Haus, kehrt die Stiege und macht kleine Besorgungen, vor allem aber hat er ein wachsames Auge auf alle Bewohner.

Ein Bawab aus Oberägypten im Schatten seines Hauses in Kairo.

Foto: afr

Astrid Frefel aus Kairo

Mitten in der Nacht auf einer lokalen Polizeiwache nahe des Zentrums von Kairo. Es gilt, eine Anzeige wegen eines Taschendiebstahls aufzugeben. Pass, Kreditkarten, Telefon, Geld, Schlüssel sind weg, und das muss amtlich dokumentiert werden. Der junge Offizier in blütenweißer Uniform weiß zwar auch, dass die Diebe auf ihrem Motorrad nie gefasst werden, aber die Schreibarbeit muss dennoch sein. Höflich fragt er nach den persönlichen Daten, Name, Beruf, Staatsbürgerschaft, Geburtsdatum. Noch bevor ich etwas sagen kann, kommen die Antworten wie aus der Pistole geschossen von Khaled, dem Bawab, der sich als Begleitung anerboten hatte.

Ich bin perplex und sprachlos. Kann mir nicht erklären, woher er alle diese persönlichen Details weiß. Zudem erklärt er mir, er kenne Namen und Telefonnummern von jenen Leuten, die ebenfalls einen Schlüssel von meiner Wohnung besitzen würden. Während der ganzen Amtshandlung, die weit über eine Stunde dauert, unterhält sich Khaled immer wieder verschwörerisch flüsternd mit dem diensthabenden Offizier. Es ist ganz offensichtlich, dass es da eine ganz besondere Nähe gibt.

Der Pförtner als Institution

Der Bawab – wörtlich übersetzt der Pförtner – ist eine fest verankerte ägyptische Institution. Es gibt ihn in fast allen Wohnhäusern, mindestens in den etwas besseren Quartieren. Früher stammten fast alle Bawabs aus Oberägypten, trugen eine Galabiyya, das traditionelle bodenlange Kleid, und einen weißen Turban. Diese Bilderbuch-Typisierung trifft heute nur noch zum Teil zu. Auch viele Männer aus anderen ländlichen Gegenden, etwa dem Delta, arbeiten inzwischen als Bawabs in der Millionenmetropole Kairo. Sie leben fern von zu Hause, meist ohne Familie, in einem winzigen fensterlosen Verschlag und fahren nur hin und wieder zu Feiertagen in ihre Dörfer aufs Land.

Die Bawabs haben einen umfangreichen Aufgabenkatalog. Sie fegen die Treppen, waschen Autos, kaufen Zeitungen, erledigen kleine Reparaturen und machen Botengänge für die verschiedenen Hausbewohner. Für diese Gefälligkeiten gibt es jedes Mal, zusätzlich zum monatlichen Obolus, noch ein Trinkgeld. Im besten Fall ist der Bawab der gute Geist des Hauses. Aber vor allem wacht er rund um die Uhr darüber, wer wann über die Schwelle und wieder hinaustritt. Seine Augen und Ohren sind überall, auch wenn er selbst nicht sichtbar ist. Vor allem neue Mieter und ihre Gewohnheiten werden genaustens unter die Lupe genommen. Er fragt Fremde, die ins Haus wollen, nicht nur, zu wem sie wollen und was sie hier zu suchen haben, er ist auch so etwas wie ein Moralpolizist. Mit seiner bloßen Präsenz sorgt er dafür, dass die ungeschriebenen Regeln, die in dieser konservativen Gesellschaft gelten, eingehalten werden. Ausländer können dabei meist auf etwas mehr Toleranz hoffen. Aber es ist immer von Vorteil, sich mit dem Bawab gut zu stellen.

Die Bawabs stehen in der strikten, extrem undurchlässigen gesellschaftlichen Kastenordnung auf einer der unteren Stufen, mit wenig Chancen, die Leiter emporzuklettern.

Ihr soziales Stigma war auch das Thema des in Dutzende Sprachen übersetzten Erfolgsromans *Der Jakubiján-Bau* von Alaa al-Aswany, wo der Sohn eines Bawabs trotz guter Prüfungsergebnisse von der Polizeiakademie ausgeschlossen wird und nach und nach in den Extremismus abdriftet. Aber ihr Wissen verleiht den Bawabs Macht. Ihre gesammelten Erkenntnisse behalten sie nicht nur für sich, sie sind eine unbezahlbare Quelle für den weit verzweigten Inlandgemeindienst, der über alle Bürger und Bürgerinnen Dossiers führt und überall seine Zuträger hat.

Die Arbeit als Informant ist ganz selbstverständlich. Ägypten ist ein Polizeistaat, das war in Mubaraks Zeiten vor der Revolution vom Frühjahr 2011 so und hat sich seither nicht geändert. Ein spezielles Gesetz, das den Schutz der persönlichen Daten regelt, gibt es nicht. Für Sicherheit zu sorgen ist wie eine Berufung für die Bawabs, die oft in einer Straße ein ganzes verschworenes Netzwerk bilden.

Revolution in „ihrer" Straße

Bewährt hat sich die eingespielte Gemeinschaft in den ersten Tagen der Revolution, als sich die Polizei von den Straßen und Polizeiwachen zurückgezogen hatte. Es dauerte nur Stunden, bis die Bawabs ihre Straßen mit Baumstämmen abgeriegelt, eine Art Bürgerwehr und ein ausgeklügeltes Warnsystem aufgestellt hatten.

Westkonzept Privatsphäre

In Südkorea wird das Internet exzessiv überwacht

Fabian Kretschmer aus Seoul

In Südkorea besitzen über 80 Prozent der Bevölkerung ein Smartphone, flächendeckendes WLAN ist in urbanen Räumen Standard, die Internetleitungen gelten als schnellste der Welt. Dennoch schreibt das Land am Han-Fluss derzeit ein dunkles Kapitel in seiner Erfolgsgeschichte: Noch nie wurde das Netz derart exzessiv überwacht wie unter der amtierenden Präsidentin.

Erst im September 2014 beschwerte sich Park Geun-hye, dass die Gerüchte in Online-Foren über sie „zu weit" gehen würden. Die Staatsanwaltschaft nahm dies zum Anlass, eine Sondereinheit zur Internetüberwachung zu gründen. Das erste prominente Opfer war bald gefunden: eine Lehrerin, die online den Rücktritt der Präsidentin forderte. Dass die Beschuldigte einen ausländischen – und daher für die koreanische Strafverfolgung nicht einsehbaren – E-Mail-Server benutzte, wollten die Staatsanwälte damals als Schuldgeständnis anlasten.

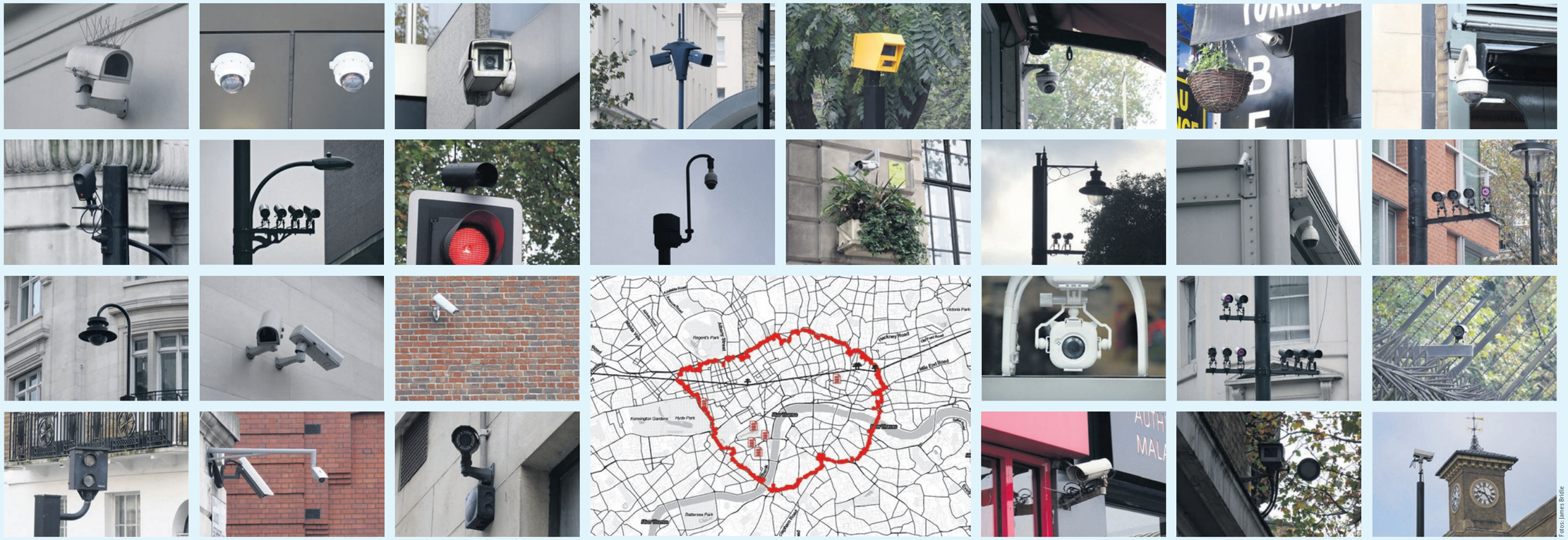
Unter dem Vorwand der nationalen Sicherheit werden regelmäßig Gewerkschafter, Journalisten und Oppositionelle ausspioniert. Jahrelang haben die drei großen Telekommunikationsfirmen des Landes im großen Stil die Kontaktdaten ihrer Kunden an Behörden weitergegeben – ohne je einen richterlichen Bescheid zu verlangen, geschweige denn die Überwachungsopfer zu informieren. Allein in der ersten Jahreshälfte 2014 waren mehr als sechs Millionen Telefonnummern betroffen.

Über 98 Prozent aller Überwachungsanfragen kommen vom südkoreanischen Geheimdienst. Dieser hatte bereits im Vorfeld zur Wahl der amtierenden Präsidentin für einen Cyberskandal gesorgt: Mit gefälschten Accounts schrieben Geheimagenten über 1,2 Millionen Twitter-Nachrichten, in denen sie die Oppositionskandidaten etwa als „Kommunistenschweine" diffamierten.

Der Aufschrei der Zivilgesellschaft blieb bislang vergleichsweise verhalten. „Wir haben eine lange Periode an Diktatoren überdauern müssen. Koreaner sind daran gewöhnt, überwacht zu werden", sagt Internetaktivist Oh Byoung-il. Zudem verortet der 45-Jährige eine kulturelle Eigenheit: „Viele Koreaner sind mit dem Konzept von Privatsphäre nicht vertraut. Das ist eine westliche Idee, die es in unserer kollektivistischen Historie nicht gab."

SA./SO., 27./28. JUNI 2015 SCHWERPUNKT DER STANDARD 19

Wie und wo wir im Alltag überall überwacht werden oder selbst bewusst und unbewusst Datenspuren hinterlassen und wie wir der allgegenwärtigen Überwachung zumindest teilweise entkommen können



Sie sind überall: Eigentlich wollte Künstler James Bridle am 30. Oktober 2014 den mautpflichtigen Innenstadtbereich Londons, die „Congestion Charge Zone", umwandern und jede Überwachungskamera fotografieren. Nach der Hälfte der Strecke, rund zehn Kilometern, hatte er 427 Kameras in seiner Kamera – wissend, dass er nur einen Bruchteil auch wirklich entdeckt hatte.

Fotos: James Bridle

Von früh bis spät ausgespäht

Was unsere Datenspuren alles über unser Leben verraten können

Nina Weißensteiner

Die ersten Datenspuren hinterlassen die meisten schon vor dem Frühstück, wenn sie am Smartphone die Nachrichten „checken" – und ihre Befindlichkeiten beim Kaffeehäferl womöglich auch noch auf Facebook „sharen". Von morgens bis abends gibt der moderne Bürger an einem stinknormalen Tag „tausende digitale Einblicke" in seine Privatsphäre, erklärt Andreas Krisch (45), Wirtschaftsinformatiker und Facebook-Verweigerer.

Der Mann muss es wissen. Er ist von den Grünen entsandter, aber unabhängiger Experte im Datenschutzrat, seine Initiative „AK Vorrat" hat mit erfolgreichen Klagen das heimische Gesetz sowie die EU-Richtlinie zur Vorratsdatenspeicherung gekippt. Nur mehr im Waldviertel und in einsamen Bergregionen, also da, wo es keinen Handyempfang gibt, entkommt man hierzulande den riesigen Speichern, die Behörden, aber womöglich auch der eigene Arbeitgeber, diverse Geheimdienste und wissbegierige Datenhändler über uns angelegt haben.

Wildwuchs an Kameras

Wer in der Bundeshauptstadt seinen Weg mit den Öffis antritt, über den wachen allein hier rund 6000 Kameraaugen. Bis zu 72 Stunden darf das Mitgefilmte nach dem Datenschutzgesetz gespeichert werden, bei einem Verbrechen in Bim, Bus oder U-Bahn das Material aber nur von wenigen, genau definierten Personen eingesehen werden.

Doch längst halten auch viele Einzelhandelsgeschäfte, die Sie betreten, draußen wie drinnen das Geschehen fest. Krisch spricht deshalb von einem „Wildwuchs an Kameras" in den letzten Jahren.

Viele große Firmen setzen bei ihrem Schutz zudem auf elektronische Zutrittskontrollsysteme, sodass für sie theoretisch auch jedes Kommen und Gehen der Mitarbeiter auf die Minute genau nachvollziehbar wäre. Allerdings müssten sich diese Arbeitgeber bei derartigen Protokollen ins Datenverarbeitungsregister eintragen lassen, denn: Wer gegen diese Meldepflicht verstößt, für den werden bis zu 10.000 Euro fällig. Nur rund 15 bis 20 Prozent der Unternehmer, schätzt Krisch, machen aber zu derartigen Aufzeichnungen korrekte Angaben.

Zu den Betriebsvereinbarungspflichten gehört es wiederum, alle Beschäftigten über gestattete und unerwünschte Benutzung von Telefon, Internet, E-Mail am Arbeitsplatz aufzuklären. Vor allem in kleineren Betrieben, meint der Experte, ist bei Auffälligkeiten eines Mitarbeiters rasch dessen Account geknackt – „eine E-Mail ist damit so transparent wie jede Postkarte". Dasselbe gilt freilich für das tagtägliche Surfverhalten.

Wer uns aber ständig ausspäht, wenn wir uns im World Wide Web herumtreiben, sind jene, die rege mit Daten handeln. Sie registrieren alles, was wir jemals an Persönlichem auf Amazon, Ebay & Co preisgegeben haben. Das führt auch dazu, dass wir beim Ansurfen diverser Webseiten gleich die für uns passende Werbung für Bücher, Kleidung, Flüge mitserviert bekommen. Eine Studie des US-Senats aus dem Jahr 2013 kam zu dem Schluss, dass die „Data Broker" mittlerweile von rund 700 Millionen Konsumenten „75.000 Attribute pro Nase" angesammelt haben, wie es Krisch ausdrückt.

Nicht jedem gefällt das

Allein was Facebook-Fans alles „liken", lässt untrügliche Rückschlüsse über ihre persönlichen Vorlieben, ihre politische Einstellung und ihre sexuelle Orientierung zu. „Das Problem ist, dass man dabei rasch in eine Schublade gesteckt werden kann, wenn diese Daten an Falsche geraten", sagt der Fachmann.

Eine Befragung unter 60.000 Freiwilligen auf der sozialen Plattform ergab, dass man mit hoher Wahrscheinlichkeit feststellen könne, ob die Eltern eines Users bis zu dessen 21. Geburtstag noch ein Paar waren. Die dahintersteckende These, die untermauert worden sein soll: dass Scheidungskinder wegen ihres höheren Harmoniebedürfnisses häufiger den „Gefällt mir"-Button drücken als andere.

Auch die angeblich so vielen Vorteile verschaffende Kundenkarten bei Lebensmittel-, Bau- und Drogeriemärkten, die nach Dienstschluss gern angesteuert werden, eignen sich hervorragend als Speicherkarte für das Kundenverhalten. Wohl am längsten haben bisher aber die Banken all unsere Daten und Transaktionen parat – bis zu dreißig Jahre beträgt die für sie erlaubte Speicherfrist. Krisch: „Und wer in Wien auf der falschen Seite des Gürtels wohnt, hat wegen seiner Adresse mitunter keine Chance auf einen Kredit."

Die Beschützer des Postgeheimnisses

Phil Zimmermann und Werner Koch haben mit PGP und GnuPG die zwei wichtigsten Verschlüsselungsstandards entwickelt – und früher heftig miteinander gestritten.

Fabian Schmid

Jene Männer, die in den vergangenen Jahrzehnten wohl am meisten zum Schutz der Privatsphäre beigetragen haben, könnten ungleicher nicht sein.

Da wäre einerseits Phil Zimmermann: ein 61-jähriger Friedensaktivist, Informatiker und Geschäftsmann, der nie um einen Scherz verlegen ist. „Seid vorsichtig, was ihr jetzt sagt", witzelte der US-Amerikaner unlängst in Wien, als bei einer Podiumsdiskussion die Teilnehmer verkabelt wurden. Die Universität Wien hatte aus Anlass von 25 Jahren Internet in Österreich zu einer Debatte über Privatsphäre geladen, die Zimmermann mit seiner Präsenz dominierte – und dabei gegen Geheimdienste und datenhungrige Konzerne austeilte.

Der andere Teil des ungleichen Duos lebt zurückgezogen in Düsseldorf und sieht laut *taz* aus „wie ein deutscher Familienvater: kleiner Bauchansatz, Jeans, Hemd, kein bisschen modisch". Doch Werner Koch gilt als jener Entwickler, der mit dem Verschlüsselungsstandard GnuPG sogar die mächtige NSA vor große Probleme stellt. Das hatten Filmemacherin Laura Poitras und Aktivist Jacob Appelbaum Anfang 2015 anhand von Snowden-Dokumenten enthüllt. Bei einer Rede beim Hackerkongress 31C3 in Hamburg bedankten sie sich öffentlich bei Koch, der im Publikum anwesend war. Die restlichen Zuhörer – über tausend an der Zahl – erhoben sich, um Koch mit Standing Ovations ihren Respekt zu zeigen.

Vom Kalten zum Krypto-Krieg

Den Anfang machte jedoch Zimmermann. 1991 schuf er die Verschlüsselungssoftware „Pretty Good Privacy", die unter der Abkürzung PGP berühmt wurde. Zimmermann war somit der erste Informatiker, der ein kryptografisches Verfahren für Normalverbraucher zugänglich machte. Zuvor hatte sich Zimmermann als Friedensaktivist einen Namen gemacht. In den 1980-ern war er in der Anti-Atom-Bewegung aktiv, demonstrierte gegen die nuklearen Drohgebärden der Supermächte USA und Sowjetunion. Nach dem Ende des Kalten Krieges überlegte Zimmermann, welche Entwicklungen nun die Bürgerrechte bedrohen könnten.

Fündig wurde er beim Thema Überwachung. Die Infrastruktur des Internets wurde gerade ausgebaut, erstmals hatten auch Privatpersonen Zugang zum WWW. Zimmermann war klar, dass Behörden jederzeit E-Mails abfangen und lesen konnten. Deshalb mussten diese verschlüsselt werden. Das Wundermittel dafür war eben PGP, das relativ einfach funktioniert: Jeder Nutzer hat einen öffentlichen Schlüssel, der ihn eindeutig identifiziert. Der Absender verschlüsselt die Nachricht nun für den öffentlichen Schlüssel. Um die E-Mail dann zu lesen, muss der Empfänger den dazu passenden privaten Schlüssel einsetzen, der passwortgeschützt ist.

Fangen Behörden die Nachricht ab, sehen sie nur eine wirre Kette an Ziffern und Buchstaben. Sie müssen nun den Verschlüsselungsalgorithmus knacken oder sich den privaten Schlüssel des Empfängers besorgen. Im militärischen Bereich waren solche Vorsichtsmaßnahmen schon lange Usus – was übrigens zur Entwicklung des Computers geführt hatte: Denn Alan Turing hatte in den 1940ern vom britischen Geheimdienst die Aufgabe erhalten, den Verschlüsselungscodes der Nazis zu knacken. Das war nur mittels neuer Rechenmaschinen möglich.

Aufgrund dieser militärischen Logik nahmen dann auch US-Behörden die Fährte von Zimmermann auf: Er durfte den Programmcode von PGP nicht exportieren, da es sich um ein Rüstungsgut handle, beschied ihm das FBI. Zimmermann trickste die Behörden aus, indem er den Code als Buch herausbrachte.

1997 wurde PGP dann vom Antivirenhersteller McAfee gekauft. Ein Schritt, den unter anderem Werner Koch heftig kritisiert. Er warf Zimmermann wiederholt vor, Freie Software nicht verstanden zu haben und mit dem Verkauf von PGP dessen Sicherheit verraten zu haben. Deshalb machte sich Koch daran, eine offene Alternative zum jetzt in der Konzernwelt beheimateten PGP zu schaffen.

Verschlüsselungspioniere Phil Zimmermann (li.) und Werner Koch.

Fotos: picturedesk.com / Schönherr, GnuPG

Interview mit Werner Koch auf derStandard.at/Web

Spenden für Privatsphäre

Eine Aufgabe, die ihn nicht mehr losließ: Seit 1997 widmet Koch den Großteil seiner Zeit GnuPG. Mehr als 16 Jahre war er auf Spenden angewiesen: „Anfang 2013 hatte ich fest geplant, die Sache aufzugeben, nach den Snowden-Enthüllungen im Juni konnte ich das aber nicht mehr machen."

Durch das große Lob von Poitras, Snowden und Co konnte Koch nun genug Geld auf die Beine stellen, um GnuPG sorgenfrei weiterentwickeln zu können. Zimmermann hat indes eine neue Firma namens Silent Circle, mit der er abhörsichere Telefonate ermöglichen will. Die Pioniere der Verschlüsselung: Sie kämpfen weiter für unsere Privatsphäre.

Abtauchen ins Darknet

Anonymisieren und verschlüsseln: Wie man der Netzüberwachung entrinnt

Alois Pumhösel

Wie entkommt man den Überwachern? Wie kann man sich im Internet bewegen und dennoch sicher sein, dass die Privatsphäre geschützt ist; dass NSA & Co nicht mitlesen, Unternehmen die Verbindungsdaten nicht zu Marketingzwecken verwenden oder Hacker nicht private Dateien durchstöbern? Selbst für Markus Kammerstetter vom Secure Systems Lab am Institut für Rechnergestützte Automation der TU Wien ist das „in der Tat sehr schwierig". Der IT-Experte hat mit seinem Team bereits zweimal den internationalen iCTF-Hacker-Wettbewerb der Universität Santa Barbara in Kalifornien gewonnen, wo die Teilnehmerteams beispielsweise Server gegen Angreifer verteidigen müssen.

Vorweg: Das Smartphone sollte man besser wegwerfen. Benutzer haben hier kaum eine Möglichkeit, der potenziellen Überwachung entgegenzutreten. Apps versenden zum Teil ungefragt persönliche Informationen und GPS-Ortsdaten, Netzbetreiber können jederzeit eruieren, an welcher Mobilfunk-Basisstationen sich ein Gerät anmeldet. „Aus Datenschutzsicht ist das Smartphone die schlechteste Wahl", sagt Kammerstetter. Spezielle Krypto-Handys zur sicheren mobilen Kommunikation, wie sie von Politikern oder Wirtschaftsbossen verwendet werden, kosten ein Vielfaches üblicher Smartphones.

Aber auch bei PCs, die mit dem Web verbunden sind, ist es recht aufwendig, ungebetene Beobachter auszuschließen. Das wichtigste Werkzeug für die Anonymisierung der Datenströme ist das TOR-Netzwerk, das Teilnehmer über mehrere zufällig gewählte, oft wechselnde Server verbindet.

„Das ist zwar langsam, in Verbindung mit einem entsprechend angepassten Browser aber die beste Möglichkeit, um anonym zu bleiben", so der Experte. Zusätzlich sollte man HTTPS-Verschlüsselung nutzen, die nicht nur die Vertraulichkeit, sondern auch die Authentizität der Daten garantiert. Für Mail-Clients empfehlen sich entsprechende Add-ons, die auf Phil Zimmermanns PGP-Software *(siehe Artikel links)* aufbauen, wobei sie aber von Absender und Empfänger verwendet werden müssen, um Schutz zu gewähren.

Zufluchtsort für Kriminelle

„Unverschlüsselt können die Daten sofort an Dritte gelangen", so Kammerstetter. Allerdings bestehe auch bei TOR eine kleine Unsicherheit. Wenn der zufällig gewählte Austrittsserver, an dem die Daten das Anonymisierungsnetzwerk verlassen, beispielsweise von der NSA betrieben würde, könnten die Überwacher mitlesen. Der Versender könne aber dennoch nicht eruiert werden.

Benutzern des TOR-Netzwerks muss klar sein, dass man sich nicht in bester Gesellschaft befindet. Das „Darknet" ist auch ein Ort krimineller Machenschaften, etwa dem Handel mit Drogen, Waffen oder Schadsoftware. Kürzlich konnte der Betreiber der Drogenplattform „Silk Road" dingfest gemacht werden – allerdings nicht aufgrund einer Unsicherheit des TOR-Netzwerks, erläutert Kammerstetter.

Eine Alternative zu TOR sind VPN-Dienste. Für ein paar Euro pro Monat wird Zugang zu einem Server irgendwo in der Welt geboten, der die Herkunft der Datenströme verschleiert. Oft sind die Unternehmen an Standorten wie Malaysia oder British Virgin Islands beheimatet. „VPN-Netzwerke bieten Schutz, solange die Anbieter nicht dazu gezwungen werden, die Kundendaten herauszugeben", erklärt Kammerstetter. „Dieses Risiko macht sie weniger sicher als das TOR-Netzwerk."

Kammerstetter rät zur Wahl von Open-Source-Software bei der Wahl der Security-Tools. „Man kann erwarten, dass keine versteckten Funktionen vorhanden sind, wenn der Programmcode offen verfügbar ist." Allerdings ist es für Laien oft nicht einfach, die komplexen Tools aufzusetzen. „Vieles spricht für fertige Softwarepakete, die von der Community zusammengestellt wurden." Mittlerweile gibt es auch Hardware-Projekte wie die „Freedom Box", Mini-Server, die auf die Verwendung Privacy-orientierter Techniken optimiert werden.

Die Bemühungen um Sicherheit laufen aber ins Leere, wenn ein paar Grundregeln nicht eingehalten werden. Erhält ein Überwacher physischen Zugang zum Computer, etwa um mit einem Keylogger alle Eingaben inklusive Passwörtern aufzuzeichnen, helfen alle Anonymisierungstools nichts. Und die beste Verschlüsselung garantiert keine Privatsphäre, wenn man selbst im Netz sensible Daten unachtsam verbreitet.

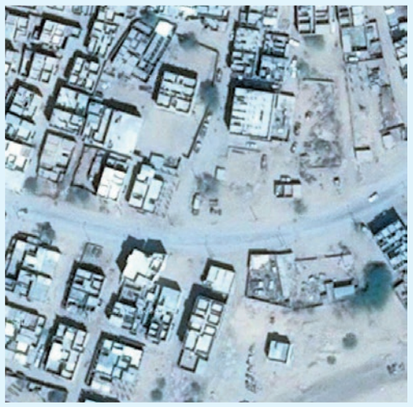
SA./SO., 27./28. JUNI 2015 SCHWERPUNKT DER STANDARD 31

Nicht nur die USA und Deutschland tun es, natürlich spionieren auch Briten, Russen, Chinesen und andere – so wie Österreich Experten in geheimer Mission hat – Muss das sein? Zwei Standpunkte und ein Ortsbesuch

The Drone's-Eye View

Sie seien die effizientesten Waffen, jene mit der größten Distanz zu ihren Opfern und unsichtbar obendrein: Drohnen. Der Künstler James Bridle macht ihr geheimes Tun sichtbar und real, indem er die Orte nach Angriffen dokumentiert.
https://instagram.com/dronestagram

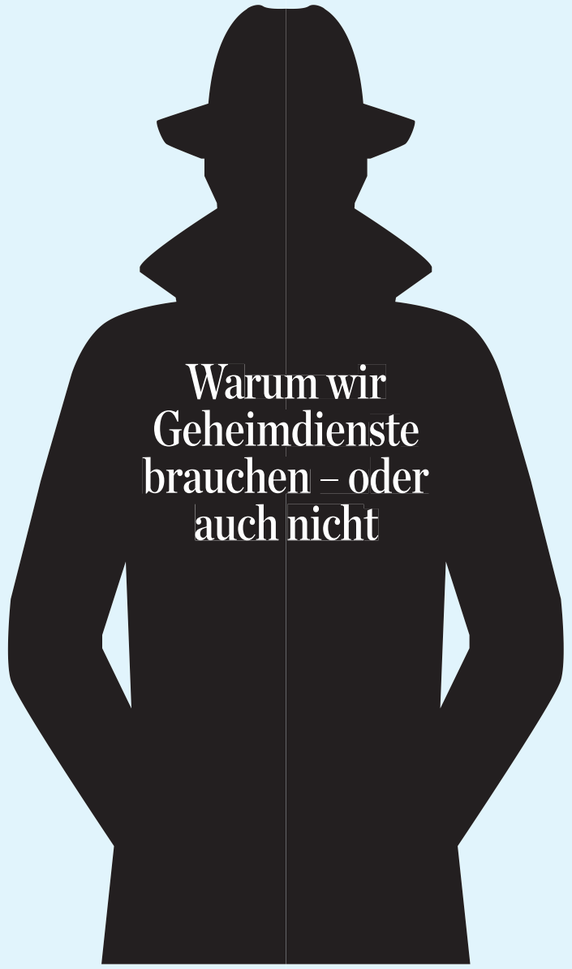
Shahi Khel, Shawal, Nordwasiristan (Pakistan), 19. Jänner 2015: Bei einem Angriff durch CIA-Drohnen auf ein Haus im pakistanischen Shawal-Tal wurden laut The Bureau of Investigative Journalism zwischen fünf und sieben Menschen getötet, darunter ein US-Bürger.



Jemen, 6. Dezember 2014: Bei einem US-Drohnenangriff in den frühen Morgenstunden wurden in der Region Nusab mindestens neun Menschen getötet. Laut jemenitischen Sicherheitskräften seien dabei neun mutmaßliche Al-Kaida-Kämpfer ums Leben gekommen.

Pakistan, 7. Dezember 2014: CIA-Drohnen töteten im Ort Datta Khel im an Afghanistan grenzenden Stammesgebiet Nordwasiristan mindestens vier Menschen. Darunter soll laut pakistanischen Behörden ein hochrangiges Al-Kaida-Führungsmitglied gewesen sein.

Warum wir Geheimdienste brauchen – oder auch nicht



Pro

Conrad Seidl

Man stelle sich vor, dass irgendwo in der westlichen Welt – Gott behüte, bei uns in Österreich – ein wirklich großer Anschlag passiert, einer mit 50 und mehr Toten. Sofort würde gefragt: Hätte man das nicht verhindern können? Hätte man nicht wissen müssen, dass der Attentäter seit Jahren in dubiosen Fundamentalistenkreisen verkehrt hat? Ist niemandem aufgefallen, auf welchen Websites er technische Anleitungen gesucht hat, welche Chemikalien er nach und nach gekauft hat, um seine Bombe zu bauen? Schaut solchen Leuten denn niemand auf die Finger?

Oh ja. Natürlich schaut man „solchen Leuten" auf die Finger – also allen, von denen man vermutet, dass von ihnen Gefahr ausgehen könnte. Und, zum Entsetzen von Bürgerrechtlern, man schaut noch einigen anderen Leuten auf die Finger; Leuten, die womöglich gar nichts mit Anschlagsplänen, radikalem Gedankengut oder sonst welchen gefährlichen Dingen zu tun haben – sondern einfach nur zufällig am falschen Platz waren oder zufällig Kontakt mit einer als gefährlich eingeschätzten Person hatten.

Geheimdienste müssen das tun. Und zwar oftmals ohne konkreten Verdacht. Sie beobachten und lauschen, sie sammeln offene Informationen und manche legal nicht beschaffbare Information – und konstruieren daraus ein Lagebild.

Wenn es gutgeht, verhindern sie damit Anschläge. Tatsächlich ist es in den vergangenen Jahren vielfach gutgegangen – weil etwa die (allen europäischen Diensten an Ausrüstung, Personal und Auswertungsmöglichkeiten überlegenen) Amerikaner die Deutschen vor einer Terrorzelle gewarnt haben, deren Gefährlichkeit den deutschen Verfassungsschützern noch nicht bewusst war. Lob bekommt man dafür kaum.

Wenn es nicht gutgeht, dann kracht es trotz aller geheimdienstlichen Bemühungen. Dann gibt es Spott und Hohn für die Terrorbekämpfer – und die Forderung, die Dienste besser gleich abzuschaffen. Weil sie zu wenig brächten – aber ständig unter der Gürtellinie der gesetzlichen Regeln und parlamentarischen Kontrollen agieren. Das, sagen Insider, müsse eben sein – sonst bekäme man die Informationen nämlich gar nicht.

Dass es immer wieder gelungen ist, entführte österreichische Touristen freizubekommen, hängt mit dieser geheimdienstlichen Praxis zusammen, Kontakte zu allerlei zwielichtigen Organisationen in Afrika und Nahost zu halten – Kontakte, über die man nicht spricht, Kontakte, derer man sich auch nicht rühmen würde. Aber die im Ernstfall Leben retten können.

Und natürlich muss man auch mit mehr oder weniger „befreundeten" ausländischen Diensten zusammenarbeiten und Informationen austauschen. Eine Hand wäscht die andere.

Aber warum spioniert dann ein Freund dem anderen hinterher? Nun: Das ist unter Geheimdiensten nicht anders als in zwischenmenschlichen Beziehungen, wo selbst in den harmonischsten Partnerschaften der Hauch eines Verdachts aufkommen kann, bei dem dann argwöhnisch nachgeprüft wird, mit wem der andere denn die langen Abende wirklich verbringt, mit wem er oder sie dauernd telefoniert und worüber. Das haben auch österreichische Soldaten im Auslandseinsatz erkennen müssen, als das Abwehramt des Bundesheeres aufgedeckt hat, dass ihre – private – Kommunikation mit der Heimat von einem ausländischen Dienst abgehört worden war.

Auch dazu sind Geheimdienste da: Sie müssen die eigenen staatlichen Einrichtungen, die eigenen Soldaten und Beamten, die eigene Wirtschaft vor fremden Diensten und deren Wissbegierde schützen. Und sie müssen imstande sein, der eigenen staatlichen Führung ein möglichst umfassendes Lagebild von den Absichten anderer – staatlicher und nichtstaatlicher – Akteure zu vermitteln.

In Krisen- und Kriegsfällen sind die Geheimdienstler oft die Letzten, die noch Fühlung halten, wenn diplomatische Beziehungen längst abgebrochen wurden.

Kontra

Fabian Schmid

Man stelle sich vor, französische Geheimdienste wüssten von einem gefährlichen Brüderpaar, das Absichten hegt, ein blutiges Attentat auf die freie Presse zu verüben – und den Plan unbehelligt in die Tat umsetzt. Man stelle sich vor, der russische Geheimdienst warnte US-Behörden vor einem jungen Tschetschenen, der in militante Kreise abrutscht – und der zündet mithilfe seines Bruders beim Boston-Marathon mehrere Bombensätze.

Man würde dann wohl erwarten, dass eine ernsthafte Debatte über die Kompetenzen von Geheimdiensten eingeleitet wird. Tatsächlich forderten Innenminister nach diesen Anschlägen aber nur noch mehr Befugnisse, noch mehr Daten für ihre Spione.

Die Digitalisierung erlaubt den Geheimdiensten in zuvor unvorstellbarem Ausmaß, Massen an (unbescholtenen) Bürgern auszuspähen. Doch der Algorithmus, der diese Daten durchforstet, macht Unschuldige zur Zielscheibe: So stürmte eine FBI-Spezialeinheit nach dem Attentat in Boston das Haus einer jungen Familie, weil Datenanalysen sie verdächtig gemacht hatten. Die junge Frau hatte online nach Kochtöpfen gesucht, ihr Ehemann nach großen Rucksäcken.

So wird eine Infrastruktur geschaffen, die in den Händen eines repressiven Regimes riesigen Schaden anrichten kann. Wollen wir hoffen, dass Österreich auch in hundert Jahren noch eine Demokratie ist – dafür die Hand ins Feuer legen kann niemand. Die Möglichkeiten zum Orwell'schen Überwachungsstaat sind jedenfalls schon gegeben.

Gleichzeitig blieb die NSA bisher Beweise schuldig, dass Massenüberwachung Anschläge verhindert hat. Als einziges Positivbeispiel wird ein US-Taxifahrer somalischer Abstammung genannt, der 8500 Dollar an die Al-Shabaab-Miliz überwiesen hatte.

Selbst in westlichen Demokratien sind die Geheimdienste außer Rand und Band geraten. Der deutsche Verfassungsschutz hatte äußerst dubiose Verbindungen zu den Neonaziterroristen der NSU, schredderte nach der Festnahme von Beate Zschäpe hektisch wichtige Ermittlungsakten. Der britische GCHQ gab Handbücher heraus, wie Agenten im Internet die Stimmung manipulieren und Aktivisten in Liebesfallen locken können. Das österreichische Abwehramt notierte sich Kennzeichen von Autos, die in der Nähe einer Demonstration gegen Eurofighter geparkt waren.

Dafür lieferte der BND den US-Diensten „Beweise" für Massenvernichtungswaffen im Irak – die zwar nie gefunden wurden, aber einen Krieg herbeiführten.

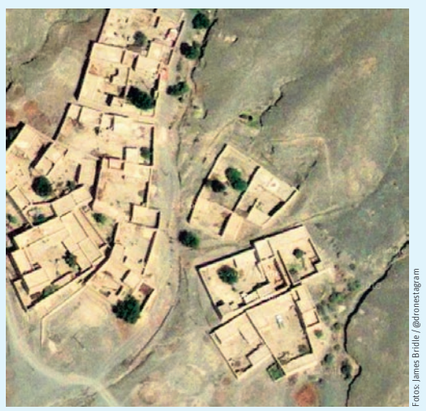
Solche Geheimdienste braucht kein Mensch. Im Gegenteil: In den vergangenen Jahrzehnten haben die ominösen Machenschaften in dieser Schattenwelt zahlreiche Menschenleben gekostet und unsere Freiheit fundamental eingeschränkt. Dass Russland sich die Krim schnappt und mit der Terrorbande „Islamischer Staat" ein monströses Gebilde entsteht, haben die ach so wichtigen Dienste aber verschlafen.

Aber sind wir dem Bösen nicht schutzlos ausgeliefert, wenn es keine Geheimdienste mehr gibt? Die Antwort darauf ist ein eindeutiges Nein. Im Bereich Jihadismus zeigt sich etwa, dass die Sensibilisierung der Bevölkerung zahlreiche Hinweise gebracht hat. Familienangehörige, Lehrer oder Freunde schlagen Alarm, wenn sich jemand plötzlich radikalisiert. Im rechtsextremen Milieu liefern unabhängige Journalisten seit Jahren wichtige Analysen und Hinweise, ohne sich mit den Neonazis zu verbrüdern. Die Polizei kann sich um diese Bereiche kümmern, nach transparenten Regeln und unter parlamentarischer Kontrolle.

Kommen Soldaten im Ausland zum Einsatz, kann das Militär vor Ort Aufklärung betreiben und auf die Hilfe der diplomatischen Vertretung hoffen. Satellitenbilder und Gefahrenanalysen müssen auch erstellt oder von Bündnispartnern erhalten werden können, ohne dass Bürgerrechte verletzt werden. Sonst sollte man sich neue Freunde suchen.

Pakistan, 26. Dezember 2014: Bei zwei US-Drohnenangriffen im Nordwesten Pakistans wurden im Shawal-Tal sieben Menschen getötet. Laut Angaben des dortigen Militärs soll es sich um Kämpfer der radikalislamischen Taliban gehandelt haben.

Jemen, 6. Dezember 2014: Bei einem gescheiterten Befreiungsversuch der US-Armee sind in der Provinz Shabwa zwei Geiseln – ein US-Fotograf und ein südafrikanischer Lehrer – ums Leben gekommen. Die USA fliegen dort regelmäßig Angriffe mit Kampfdrohnen.



Pakistan, 20. Dezember 2014: Bei einem US-Drohnenangriff im Dorf Datta Khel in Nordwasiristan wurden laut Angaben des pakistanischen Militärs sechs islamische Extremisten getötet. Es war die 22. Drohnenattacke in Pakistan in diesem Jahr, elf davon in Datta Khel.

Fotos: James Bridle / @dronestagram

Unter dem Wienerwald wird gelauscht

Nahe Neulengbach befindet sich eine der wichtigsten Abhörstationen des österreichischen Bundesheers. Anrainer berichten über zehn unterirdische Stockwerke und mysteriöse Antennen. Ein Lokalaugenschein.

Fabian Schmid

Eine unscheinbare Abfahrt führt auf den kleinen Hügel im Wienerwald. Wochenendhäuser säumen den Weg, dazwischen blühen Wiesen in bunten Farben. Ein idyllischer Ort, wären da nicht die riesigen weißen Masten, die durch eine Vielzahl von Schleifen miteinander verbunden sind. Ein bizarres Objekt in der naturbelassenen Landschaft, das an ein Spinnennetz erinnert.

Fotografieren streng verboten

Wer sich der Anlage über die Zufahrtsstraße nähert, um mehr über die ominösen Masten zu erfahren, stößt bald auf angsteinflößende Warnschilder: Das Betreten des eingezäunten Gebiets sei strengstens verboten, scharfe Munition würde bei Eindringlingen zum Einsatz kommen. Fotografieren oder das Anfertigen von Zeichnungen sei streng verboten. Eine Videokamera registriert jeden Neugierigen, hinter dem Zaun ist ein Hundezwinger samt zähnefletschendem Rottweiler.

Die Geheimniskrämerei überrascht nicht: Bei der Anlage am Kohlreithberg nahe Neulengbach handelt es sich um einen Lauschposten des Heeresnachrichtenamts (HNaA), das für das Bundesheer Auslandsaufklärung betreibt. Doch dass das Bundesheer hier spioniert, hat sich schon lange herumgesprochen. Prominenter als „Neulengbach" (die Anlage liegt geografisch eigentlich in Maria-Anzbach) ist nur die Königswarte nahe Hainburg. Während Wanderer die Satellitenschüsseln dort sogar über einen Aufsichtsturm, der unmittelbar neben dem Objekt liegt, unter die Lupe nehmen können, stehen die Zeichen in Neulengbach auf Abschottung. Dabei halten sich Gerüchte, dass besonders in Neulengbach elektronische Aufklärung betrieben wird.

DIE ÜBERWACHTEN BÜRGER

Schon 2003 schrieb der *Kurier*- und ORF-Journalist Kurt Tozzer über die Station Neulengbach: „Es gilt zwar als streng geheim, doch sickerte durch, dass die Fernmeldeaufklärer über Geräte verfügen sollen, mit denen man aus den überinternationalen Richtfunkstrecken der Telefonnetze Nachrichten auffangen kann. Und zwar nicht nur Telefongespräche, sondern auch Daten des E-Mail-Verkehrs."

Zehn Jahre später erhielten diese Spekulationen durch die Snowden-Enthüllungen neue Brisanz. Noch immer ist nicht geklärt, wie eng das österreichische Bundesheer mit der NSA kooperiert. Fakt ist, dass die US-Dienste Österreich Informationen bei Auslandseinsätzen österreichischer Soldaten liefern. Was im Gegenzug Richtung USA wandert, wissen nicht einmal Nationalratsabgeordnete.

Neulengbach dürfte einer der Schlüsselorte für diese Frage sein. Der Aufdecker Duncan Campbell, der für das EU-Parlament Ende der 1990er-Jahre über das globale US-Spionagenetz Echelon recherchierte, reagiert auf die Frage nach der Königswarte mit Verwunderung: „In Neulengbach passiert der Großteil. Dort muss man nachsehen."

„Zehn Stockwerke tief"

Seit 1976 gilt der Kohlreithberg per Verordnung als Sperrgebiet. Ein Anrainer, der in unmittelbarer Nähe zum Objekt wohnt, habe damals mehrfach nach Sinn und Zweck dieser Anlage gefragt. „Mir wurde gesagt, dass das Heer hier Taxilenker in Bratislava abhören kann", erzählt der Anwohner. Tatsächlich belegen Dokumente, dass Neulengbach gemeinsam mit der Königswarte und Stationen in Oberösterreich und Salzburg Teil einer Nato-Peilkette war, die von Norddeutschland bis Italien gen Osten lauschte.

Dieses Aufgabengebiet dürfte sich nach dem Lüften des Eisernen Vorhangs geändert haben. Die erkennbare Antenneninstallation liefert aber keine Anhaltspunkte: Vom STANDARD befragte Experten erkennen darin eine Vorrichtung für militärische Funksprüche. Zivile Kommunikation dürfte damit nicht abgehört werden.

Doch das wahre Mysterium dürfte sich unter der Erde befinden. „Vor rund 30 Jahren begannen rege Bau- und Grabungstätigkeiten", berichtet der erwähnte Anrainer weiter. Während auf der Oberfläche ein Haus in der Größe eines Bauernhofs steht, geht es nach unten „mindestens zehn Stockwerke in die Tiefe."

Im Ort hat man sich mittlerweile an die ominöse Nachbarschaft gewöhnt. Der grüne Gemeinderat Lothar Rehse berichtet, dass über das Objekt nicht gesprochen wird: Frage man nach dem Bundesheerposten, „steht in den Augen dieses typisch österreichische ‚falsche Frage – weiter bitte!'". Tatsächlich gibt der Amtsleiter der Bürgermeisterin (ÖVP) an, „im Alltag keine Nachteile zu sehen – im Gegenteil: Einige unserer Mitbürger haben dort einen Arbeitsplatz."

Anwohner arbeiten etwa in der Bewachungsmannschaft oder in der Hundestaffel, normalerweise schützen vier bis fünf Mann das Objekt. „Da stehen komplizierte elektronische Geräte herum", berichten diese. Gleichzeitig hört man, dass sich in den vergangenen 20 Jahren nicht viel verändert habe.

Beschwerden über den Lärm von der nahegelegenen Autobahn seien hingegen ein Gesprächsthema, so der Grünpolitiker Rehse. Von dubiosen weißen Masten lässt man sich im Wienerwald also nicht stören.