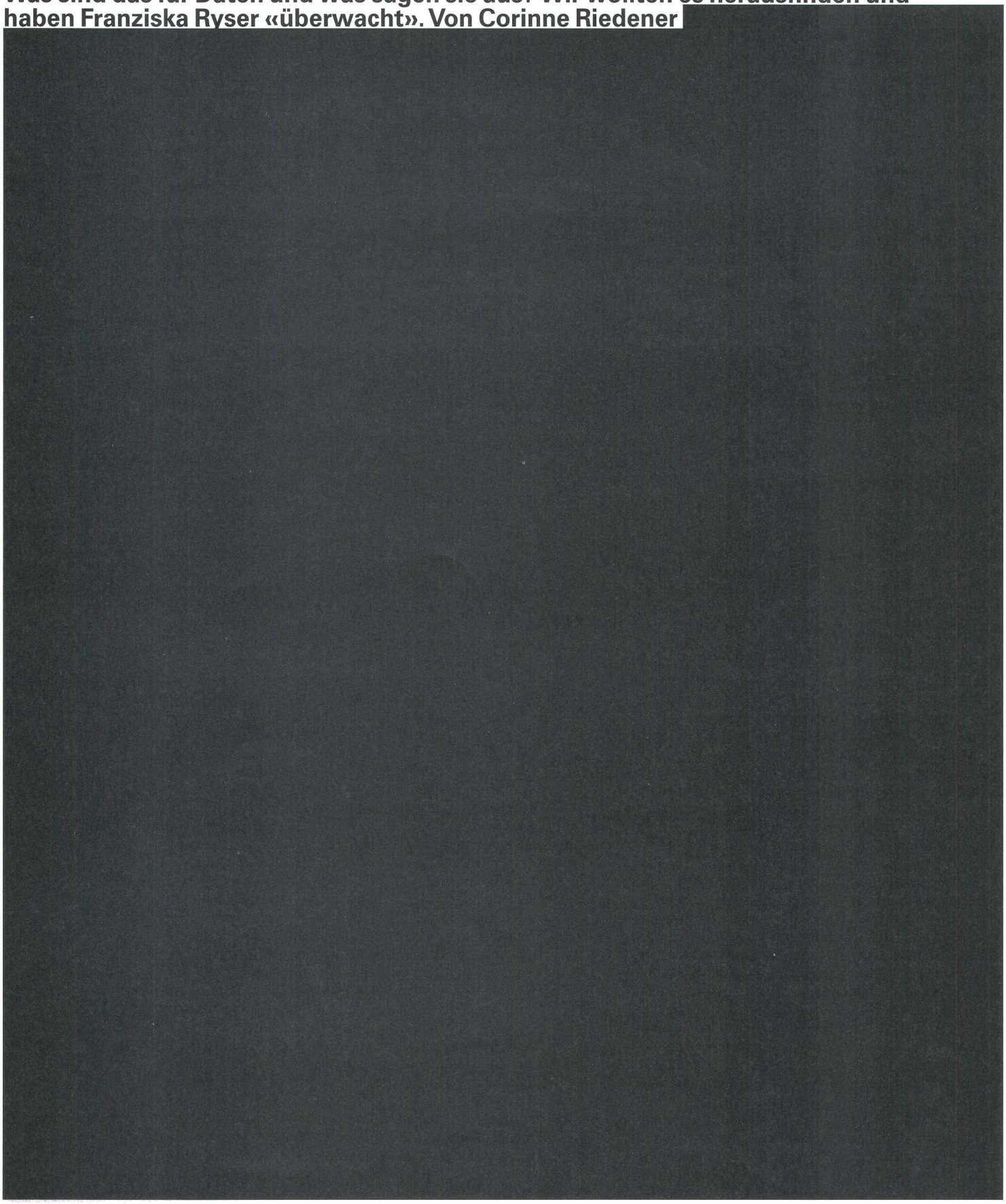
Willkommen im digitalen Totalitarismus

WILLKOMMEN IM DIGITALEN TOTALITARISMUS

Die Schweizer Anbieterinnen von Post-, Telefon- und Internetdiensten sind verpflichtet, das Kommunikationsverhalten ihrer Kundinnen und Kunden für sechs Monate zu speichern und diese Daten wenn nötig den Strafverfolgungsbehörden zu übergeben. Was sind das für Daten und was sagen sie aus? Wir wollten es herausfinden und haben Franziska Ryser «überwacht». Von Corinne Riedener



Wann haben Sie zum letzten Mal die Allgemeinen Geschäftsbedingungen von Facebook, Amazon oder Google studiert? Eben. Lieber rasch auf «agree» geklickt und fröhlich weitergesurft. «Wir haben ja ohnehin keine Kontrolle mehr über unsere Daten», denken sich viele achselzuckend, «abgesehen davon, sitzen diese Datenkraken eh alle im Ausland.» Das stimmt wohl, macht es aber nicht weniger besorgniserregend. (Immerhin gibt es Alternativen: Mails kann man verschlüsseln, statt Google kann man die Suchmaschinen DuckDuckGo oder Startpage verwenden, statt Safari, Windows Edge oder Chrome die Open-Source-Tools von Mozilla, einen Tor-Browser oder ein Virtual Private Network (VPN). Einkaufen kann man auch auf dem Markt, Musik hören auch mit dem Plattenspieler und so weiter.)

Aber was, wenn die Datenkrake in unserer Hosentasche sitzt? Laut dem Schweizer «Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs» (BÜPF) sind sämtliche Anbieterinnen von Post-, Telefon- und Internetdiensten seit 2002 verpflichtet, das Kommunikationsverhalten ihrer Kundinnen und Kunden für sechs Monate aufzuzeichnen – sprich wer, wann, wo und mit wem kommuniziert. Mit dieser verharmlosend gesagt «rückwirkenden Überwachung» lässt sich ein ziemlich detailliertes Bild einer Person anfertigen, ein Bewegungs- und Beziehungsprofil: Wer hat mit wem und wie oft Kontakt? Wer hat sich wann ins Internet eingeloggt oder aufs Email-Postfach zugegriffen? Wo hält sich diese Person auf und welche Interessen verfolgt sie im Internet?

Facebook ist freiwillig, die staatliche Überwachung nicht

Auf Verlangen müssen die Daten an die Strafverfolgungsbehörden oder den Geheimdienst herausgegeben werden. «Für einen Zugriff reicht der ‹dringende Verdacht auf ein Verbrechen oder Vergehen› – im Fall eines Missbrauchs einer Fernmeldeanlage sogar der Verdacht auf eine Übertretung», schreibt die Digitale Gesellschaft in ihrem Faktenblatt zur Vorratsdatenspeicherung. Die Verwendung der Vorratsdaten sei also nicht auf schwerste Straftaten beschränkt, sondern ist auch bei minder schweren Delikten wie einfachem Diebstahl, Urheberrechtsverletzung oder falschem Alarm möglich. «Bei sämtlichen Straftaten über das Internet – also selbst bei einer Beleidigung –, sind die Provider gezwungen, eine Identifikation des Urhebers oder der Urheberin zu ermöglichen. Es braucht dazu auch keinen richterlichen Beschluss.» Kommt hinzu, dass auch der Quellenschutz von Anwältinnen oder Journalisten mit der Vorratsdatenspeicherung empfindlich verletzt werden kann.

Anders als bei Facebook, Google & Co., auf deren Benutzung wir theoretisch auch verzichten können, erfolgt das amtlich verordnete, präventive Speichern von Kommunikations- und Bewegungsdaten in der Schweiz zwangsweise und massenhaft, ohne Autonomie der Einzelnen und ohne Kontrolle des Volkes. Kritische Stimmen sehen darin einen massiven und unverhältnismässigen Eingriff in die Grundrechte und die Privatsphäre – alle stehen unter Generalverdacht. Die möglichen Folgen? Wir meiden bestimmte Orte, bestimmte Kontakte, bestimmte Meinungen, reiten mit der Herde, zensieren uns selber. Im schlimmsten Fall. Dieses Anpassungsbestreben, den vorauseilenden Gehorsam, nennt man auch «Chilling Effect».

Mit staatlichen Überwachungsgelüsten beschäftigen sich auch Datenschützerinnen ausserhalb der Schweiz. In der EU gab es ab 2006 ebenfalls eine Richtlinie zur Vorratsdatenspeicherung, diese schrieb den Mitgliedstaaten sogar eine Speicherdauer von bis zu 24 Monaten vor. Am 8. April 2014 wurde sie vom Europäischen Gerichtshof per sofort für ungültig erklärt. Die Digitale Gesellschaft schreibt dazu: «Sämtliche Verfassungsgerichte, welche eine zur Schweiz vergleichbare Regelung zu prüfen hatten, haben die Vorratsdatenspeicherung als unrechtmässigen Eingriff in die Grundrechte eingestuft – und sie aufgehoben: Rumänien (2009, 2014), Deutschland (2010), Tschechien (2011), Österreich (2014), Niederlande (2015), Bulgarien (2015). 2018 erklärte der Europäische Gerichtshof für Menschenrechte, was gemäss EuGH gegen die EU-Grundrechtecharta verstosse, sei auch mit der Europäischen Menschenrechtskonvention (EMRK) nicht vereinbar.»

Die Digitale Gesellschaft hat darum ebenfalls ein Gerichtsverfahren gegen die Vorratsdatenspeicherung angestrengt. 2018 unterlag sie vor dem Bundesgericht, hat die Klage aber weitergezogen. Derzeit ist sie am EGMR hängig. Zudem ist die Digitale Gesellschaft im Juli 2019 mit einer Beschwerde gegen die Funk- und Kabelaufklärung ans Bundesgericht gelangt, nachdem das Bundesverwaltungsgericht in St.Gallen diese abgelehnt hat.

100 Franken für die eigenen Daten

Doch was genau wird eigentlich gespeichert, wie kommt man an diese Daten heran und was lässt sich aus ihnen ableiten? Zum Beispiel die Telefonanbieterinnen. Wir – Franziska Ryser von den St.Galler Grünen und ich – haben die Probe aufs Exempel gemacht, ähnlich wie Balthasar Glättli 2014. Der Politiker aus Zürich ist damals «unter der Hand» an seine Daten gekommen, hat sich dann zusammen mit der Digitalen Gesellschaft bis vors Bundesgericht durchgestritten und so immerhin erreicht, dass heute auch wir Konsumentinnen und Konsumenten Einsicht in unsere Handydaten erhalten müssen – auf Anfrage versteht sich.

Wir haben die Mustervorlage für Datenauskunftsbegehren von der Digitalen Gesellschaft verwendet für unsere Anfrage, diese eingeschrieben und mit einer Kopie unserer Identitätskarte abgeschickt. Franziska Ryser hat bei der Swisscom-Tochter Wingo angeklopft, ich bei Salt. Knapp zwei Wochen später kam die Antwort. Ryser erhielt eine CD mit ihren Daten plus Passwort von Swisscom. Ich hingegen bekam nur einen eingeschriebenen Brief mit einer Auflistung aller Datenarten, die Salt über mich sammelt. Für die eigentlichen Daten – meine Daten – hätte ich 100 Franken zahlen müssen, wie mir ein Herr aus der Salt-Rechtsabteilung in Renens auf Französisch und später noch per Brief erklärte.

Die Swisscom-Abteilung Legal & Regulatory, Lawful Interception gibt mit freundlichen Grüssen an, folgende Daten über Franziska Ryser zu sammeln: allgemeine Kundinnendaten wie Name, Adresse und Bonitätsangaben, Verbindungs- und Rechnungsdaten der letzten sechs Monate sowie die sogenannten Randdaten, oder, weniger schönfärberisch, Metadaten. Dazu gehört ein Bewegungsprofil jeder Person auf Grund der Handy-Daten und wer wen wie lange und von wo aus anruft oder wem eine Nachricht schreibt. Ganz abschliessend lässt sich nicht klären, welche Metadaten genau gesammelt werden (mehr dazu in der Randspalte). Das bestätigt auch Hernâni Marques vom Chaos Computer Club (CCC) Zürich auf Anfrage. «Es ist unfassbar, dass der Gesetzestext nicht schlüssig erklärt, welche Metadaten gesammelt werden und sich eine Exekutivbehörde darüber hinaus anmasst, via Merkblatt rechtssetzend zu wirken»,

Seit dem 1. März 2018 müssen auch Schweizer Email-Anbieter festhalten, wer wem zu welcher Zeit und mit welchem Betreff eine Nachricht schreibt. Auch Webseitenbesuche hinterlassen Metadaten, namentlich die Information, mit welchem Server man sich zu welcher Zeit verbunden hat (wie Art. 8 Bst. B im BÜPF-Gesetz suggeriert). Allerdings erhält man diese Daten mittels Datenauskunftsbegehren zumindest bei der Swisscom nicht genau aufgeschlüsselt, obwohl diese technisch vorliegen und sehr wahrscheinlich den Strafverfolgungsbehörden und dem NDB auf Anfrage mitgeteilt werden.

Damit nicht genug der Unklarheit: In einem Merkblatt vom April 2018 – «Abgrenzung zwischen Fernmeldedienstanbieterinnen (FDA) und Anbieterinnen abgeleiteter Kommunikationsdienste (AAKD)» – masst sich der Dienst ÜPF an, den Geltungsbereich weiter auszudehnen, so dass auch Schweizer Chat- und Anbieter von Telefonielösungen über das Internet von der Vorratsdatenspeicherung betroffen sein sollen, obwohl sie keine Zugangsanbieterinnen zum Telefonnetz oder Internet sind. Es ist somit nicht klar, welche Metadaten in der Schweiz überhaupt gesammelt werden und was davon legal ist.

sagt er. «Das müsste viel einfacher und für alle verständlich formuliert sein.»

Verschiedene Betten und nächtliche Anrufe

Geliefert wurden die Daten verschlüsselt im Format .csv (Comma-separated values). Darin enthalten waren – soviel wir uns zusammenreimen konnten, denn unsere Nachfrage bei Swisscom blieb bis Redaktionsschluss unbeantwortet – die einkommenden Anrufe (anonymisiert), die ausgehenden Anrufe (mit Rufnummer), Zeit und Dauer der Anrufe sowie die Standorte der Anfangs- und Endantennen. In einem zweiten File waren die Surf-Daten aufgelistet, also wann Rysers Smartphone wie aufs Internet zugegriffen hat, von wo aus und wie lange. Suchabfragen, besuchte Websites und andere Daten zu ihrem Surfverhalten haben wir nicht erhalten. Hat uns Swisscom überhaupt die vollständigen Daten geliefert? Auch darauf gab es bis Redaktionsschluss keine Antwort.

Aus dem Datensatz lässt sich trotzdem einiges ablesen. Zum Beispiel, dass Ryser manchmal in St.Gallen und manchmal in Zürich nächtigt, also offenbar zwei Wohnungen, ein Sofa oder einen Partner oder eine Partnerin in Zürich hat. Dass sie oft im Zug surft oder sich einen Hotspot macht. Dass sie gerne abends telefoniert, manchmal auch spät nachts. Dass sie im letzten Halbjahr am meisten mit einer bestimmten Person telefoniert hat. Dass sie im April in Italien und Frankreich war und Ende Juni in Fribourg.

Ergänzt man Rysers Handydaten mit einer Abfrage in der Schweizerischen Mediendatenbank SMD und den Einträgen auf Facebook, Twitter, Instagram & Co., erfährt man noch um einiges mehr über ihr Leben und ihre Termine, beispielsweise in den letzten zwei Maiwochen: Am 20. Mai war die Hauptversammlung der Grünen in der Projektwerkstatt beim St.Galler Güterbahnhof, am 21. Mai war Ryser an einer Diskussionsrunde zum Thema 5G in Rorschach, tags darauf wieder in Wil an einem Podium zum selben Thema, am 24. Mai hielt sie eine Rede am internationalen Klimastreik in St.Gallen und am 25. Mai war sie in der Stadt am Unterschriften sammeln mit ihren Grünen-Kolleginnen.

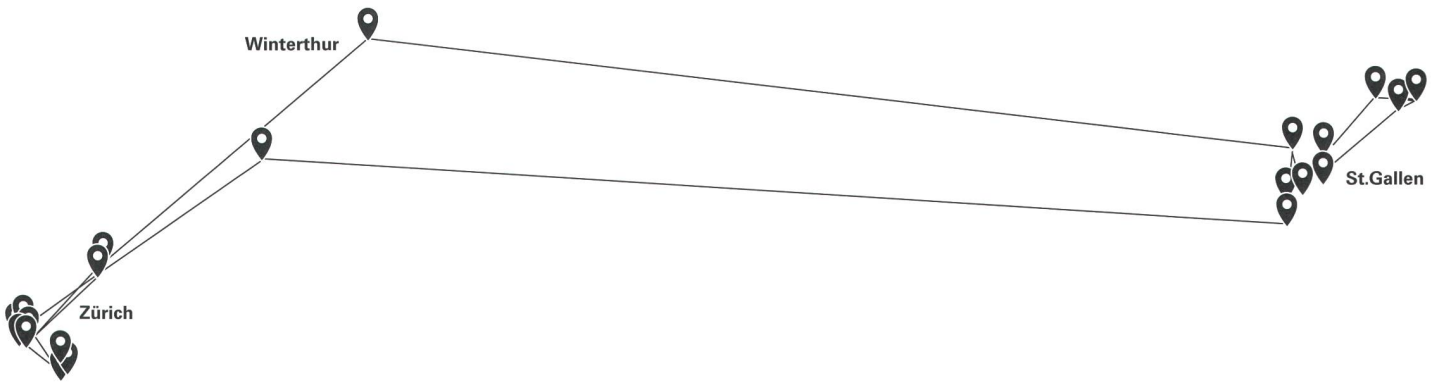
Es geht sogar noch genauer, nehmen wir den 16. Mai: Zum ersten Mal online war Ryser morgens um 5:20 Uhr, irgendwo in der Nähe der Antenne Zürcher Strasse 301A in St.Gallen. Ob sie da schon am Surfen war oder einfach ihr Smartphone eingeschaltet hat, lässt sich nicht sagen. Dann fuhr sie, vermutlich mit dem 6:25-Uhr-Zug, nach Zürich, wo sie sich bis etwa 16 Uhr nahe der Antenne an der Forchstrasse 340 in Zürich aufhielt – eine kurze Suchmaschinenabfrage verrät, dass sie seit 2016 am Rehabilitation Engineering Laboratory der ETH arbeitet. Danach ging es nach Wil. In den sozialen Medien ist nachzulesen, was genau sie dort gemacht hat: an der Klimademo teilgenommen und die Schwestern-Fraktion im Wiler Stadtparlament besucht. Offline gegangen ist Ryser an diesem Tag erst spät, nämlich um halb drei in der Nacht. Den Anruf, der um 2:43 Uhr eingegangen ist, hat sie nicht mehr beantwortet.

Alles, was heikel ist, lieber eins zu eins besprechen

Ryser ist von diesen Ergebnissen verblüfft. «Ich trage mein Handy zwar immer bei mir, telefoniere aber eher selten und habe eingeschränkte Standortnutzungen. Ich hatte gehofft, das verzerre das Bild ein wenig», sagt sie. «Und ja, ich habe tatsächlich einen Partner in Zürich. Und arbeite in einem Schlaflabor. Das erklärt die nächtlichen Anrufe.» Erstaunt hat sie auch, wie einfach es ist, die Daten anzufordern. Deren Interpretierbarkeit lasse allerdings zu wünschen übrig. «Wir bekamen keine Erklärungen, keine Legenden, dafür Abkürzungen, auf die auch Google kaum Antworten liefert. Trotzdem erkennt man rasch, wie exakt ein Tagesablauf allein auf den Antennenstandorten basierend rekonstruiert werden kann, von den Telefongesprächen ganz zu schweigen. Erstaunlich, wie zwei Excel-Tabellen meinen Alltag ähnlich gut nachbilden können wie mein Kalender oder Tagebuch.»

Ryser bezeichnet sich als sensibilisiert. Heikle Nachrichten schreibt sie bewusst nicht vom Handy aus, sondern verschlüsselt am Computer. Ausserdem achtet sie darauf, dass keine Namen oder vertraulichen Informationen in der Betreffzeile stehen. Bei den Messengern verwendet sie – der Convenience geschuldet – meist die Nachrichten-App von Apple oder WhatsApp, erklärt Ryser. «Aber auch da gilt: Alles, was heikel ist, lieber eins zu eins besprechen. Man muss sich bewusst sein, welche Informationen überwacht werden können und den Kommunikationskanal entsprechend anpassen. Bei heiklen Informationen und bei unverschlüsselten, personenbezogenen Daten sollte man auf Emails verzichten und sich stattdessen mit einem USB-Stick – oder nach Möglichkeit in Ruhe zu einem Kaffee – verabreden.»

Bewegungsprofil 21. Mai 2019



Das Konzept der Vorratsdatenspeicherung kritisiert Ryser massiv. «Sie führt zu einer verdachtsunabhängigen Überwachung der gesamten Bevölkerung, 24 Stunden, sieben Tage die Woche. Und wie das Experiment mit Saiten gezeigt hat, braucht man nicht einmal grossartige Informatikkenntnisse, um die Daten zu interpretieren. Excel und Kartenmaterial reichen aus, um unser Leben bis ins Detail zurückzuverfolgen.» Diese Informationen von allen vorsorglich zu speichern, sei einer Demokratie, basierend auf Rechtsstaatlichkeit, nicht würdig.

Max-Planck-Studie: Vorratsdatenspeicherung bringt nichts

Die Vorratsdatenspeicherung wird in etwa so verkauft: als notwendiges Übel, um die Sicherheit aller zu erhöhen. Aber bringt der teure Überwachungszirkus überhaupt etwas in der Verbrechensbekämpfung? Nicht sehr viel, wie es scheint. 2012 wurde dem CCC ein wissenschaftliches Gutachten zum Thema Vorratsdatenspeicherung zugespielt. Es wurde vom Max-Planck-Institut (MPI) im Auftrag des deutschen Bundesamtes für Justiz erstellt und legt nahe, dass die Vorratsdatenspeicherung für eine effektive Strafverfolgung und Gefahrenabwehr unnötig ist.

Unter anderem war im Bericht eine direkte Gegenüberstellung der Aufklärungsquoten in der Schweiz (mit Vorratsdatenspeicherung) und in Deutschland (ohne) zu finden: In Deutschland war die Quote – bis auf eine Ausnahme im Tausendstelbereich – in allen Deliktskategorien deutlich höher. «Im Vergleich der Aufklärungsquoten, die in Deutschland und in der Schweiz im Jahr 2009 erzielt worden sind, lassen sich keine Hinweise darauf ableiten, dass die in der Schweiz seit etwa 10 Jahren praktizierte Vorratsdatenspeicherung zu einer systematisch höheren Aufklärung geführt hätte», heisst es auf Seite 239.

«Die angebliche Notwendigkeit der Speicherung von 300 bis 500 Millionen Datensätzen pro Tag kann laut der Untersuchung nicht durch kriminologische Statistiken belegt werden», schreibt der CCC in seiner Auswertung. «Selbst beim Lieblingsthema der Sicherheitspolitiker, dem islamistischen Terror, liegen keinerlei Hinweise dafür vor, dass auf Vorrat gespeicherte Verkehrsdaten in den letzten Jahren zur Verhinderung eines Terroranschlags geführt hätten, wie die MPI-Untersuchung feststellt.»

Hernâni Marques vom CCC-Ableger in Zürich sieht das genauso. Für ihn stellt die flächendeckende Vorratsdatenspeicherung eine tiefgehende Verletzung der Grundrechte und der Privatsphäre dar. «Über den Nutzen dieser Vorratsdatenspeicherung brauchen wir uns gar nicht lange zu unterhalten», sagt er am Telefon. «Das ist ein Mittel des digitalen Totalitarismus und gehört in einem Rechtsstaat und in einer freiheitlichen Gesellschaft abgeschafft.»

Im Gegensatz zur Vorratsdatenspeicherung betrifft die Funk- und Kabelaufklärung zusätzlich den Inhalt der Kommunikation, wo der Schweizer Geheimdienst (NDB) ermächtigt wird, die Internetkommunikation zu Luft und zu Land nach Suchwörtern und anderen Mustern zu durchsuchen, also die Kommunikation, die über Satellitenverbindungen und Glasfaserleitungen abgewickelt wird. Letztere hat in den letzten Jahrzehnten an Bedeutung gewonnen, so dass mit dem Nachrichtendienstgesetz, das seit dem 1. September 2017 gilt, die Funk- um die Kabelaufklärung ergänzt wurde.

Aufklärungsquoten in Deutschland und in der Schweiz 2009*

	Schweiz		Deutschland	
	Absolut	Aufklärung %	Absolut	Aufklärung %
Pornografie	1.080	85,9	11.597	85,6
Computerbetrug	4.688	33,3	22.963	34,8
Tötungsdelikte	236	88,1	2277	96,7
Einbruchsdiebstahl**	51.758	12,7	1.108.766	14,9
Raub	3.530	36,9	49.317	52,6
Erpressung	349	74,5	5.776	84,8
Menschenhandel	50	74	811	88,7
Drohung	11.686	84,5	103.211	90,9

*) Quellen: Bundeskriminalamt: Polizeiliche Kriminalstatistik 2009. Wiesbaden 2010; Bundesamt für Polizei: Polizeiliche Kriminalstatistik 2009. Bern 2010;
**) für Deutschland wurde der Diebstahl unter erschwerenden Umständen insgesamt einbezogen, weil sich eine andere Kategorie nicht anbietet.

Franziska Ryser, 1991, ist Maschinenbauingenieurin und forscht im Rahmen ihres PhD an neuen Algorithmen, um Schlafdaten automatisch auszuwerten. Sie lebt in St.Gallen und arbeitet seit 2016 am Institut für Robotik und Intelligente Systeme der ETH. Zudem ist sie Co-Präsidentin der Grünen Stadt St.Gallen und seit 2013 Mitglied des Stadtparlamentes und National- und Ständeratskandidatin der Grünen.

franziskaryser.ch

Corinne Riedener, 1984, ist Saitenredaktorin.