Digitale Selbstverteidigung

Wanze im Hosensack

Die Schweiz hat die Überwachung der Bevölkerung systematisch ausgebaut. Das Kernstück ist dabei unser treuer Begleiter: das Mobiltelefon. Dank ihm können Behörden immer wissen, wo wir sind.

Text: Hernâni Marques, CCC Schweiz | Illu: daf

Wir sind heute praktisch immer und überall erreichbar. Das hat diverse Folgen, denen sich auch Aktivist*innen bewusst sein müssen. Jeder eingehende oder ausgehende Anruf und jedes SMS ist den involvierten Providern – wie Swisscom oder auch ausländischen Anbietern – unmittelbar bekannt. Dabei ist es nicht von Belang, ob der Anruf tatsächlich aufgebaut wurde. Bereits die Information, dass ein Aufbauversuch stattgefunden hat, wird gespeichert. Hinzu kommt: Wird der Aufruf aufgebaut, so ist nicht nur prinzipiell bekannt, an welchem Ort man sich aufhält, sondern auch, mit wem wie lange telefoniert wurde.

Trägt man diese Informationen systematisch zusammen, entsteht ein detailliertes Kommunikations- und Bewegungsprofil eines jeden Menschen. Es wird damit nicht nur klar, welche Kontakte wir besonders häufig bedienen, sondern auch, wo sich der Lebensmittelpunkt befindet und wohin besondere Ausflüge erfolgen. Durch die sehr gute Netzabdeckung in der Schweiz bleiben damit selbst Ausflüge in die Berge nicht unregistriert.

Wir sind Nummern

Seit 2000 herrscht darüber hinaus in der Schweiz eine Registrationspflicht für SIM-Karten. Damit ist zentral bekannt, welcher Person diese gehört und welche Telefonnummer damit verknüpft ist. Damit wird praktisch jede Person in der Schweiz zu einer Nummernsammlung. Aber nicht nur SIM-Karten haben mit der sogenannten IMSI (International Mobile Subscriber Identity) eine eindeutige Kennziffer. Auch die Endgeräte wie Smartphones oder Tablets sind mit der IMEI (International Mobile Equipment Identity) eindeutig identifiziert.

Im Kontext der fortschreitenden Totalüberwachung erstaunt die Schweizer Praxis: Ausgerechnet in Ländern wie Grossbritannien oder den USA, aber auch in Singapur und Hong Kong ist es möglich, SIM-Karten unregistriert an Flughäfen oder am Kiosk zu kaufen. Damit ist es – zumindest für eine gewisse Zeit – möglich, pseudonym mit einer SIM-Karte unterwegs zu sein. Trotzdem muss damit gerechnet werden, dass Überwacher*innen wissen, wem welche IMEI (also wem welches Endgerät) gehört. Darum ist es kein Zufall, dass organisierte Kriminelle nicht nur mit wechselnden SIM-Karten, sondern auch mit sogenannten «Burner-Phones» hantieren – Mobilgeräte, die nur einmalig zum Einsatz gebracht werden.

Smartphones sind Wanzen

Wanzen sind Smartphones nicht nur deswegen, weil sie im Kontakt mit den Antennen der Provider Daten generieren, sondern weil sie über Mikrofon und Kamera verfügen. Heute kommen nur simple Mobilgeräte ohne Kamera aus. Deren Funktionalität ist meist wesentlich eingeschränkt: Sie lassen sich nur zum Telefonieren sowie für den SMS- und allenfalls MMS-Versand nutzen. Solche Geräte sind aufgrund ihres geringen Preises insbesondere als Burner-Phones im Drogenhandel beliebt. Bei Strafuntersuchungen werden daher oft dutzende solcher Geräte untersucht.

Doch Handys macht etwas Weiteres höchst verdächtig. Abgesehen vom Betriebssystem, das man an der Oberfläche sieht – also z. B. Android oder iOS – ist in Handys ein vollwertiger Computer unter der Haube. Dieses System ist vordergründig dafür zuständig, in einheitlicher Form mit den weltweiten Telekommunikationsprovidern Verbindungen aufbauen zu können. Tatsächlich aber lässt sich über diesen Computer im Computer prinzipiell das Mikrofon einschalten und Gespräche mithören, selbst wenn keine Schadsoftware im engeren Sinne installiert ist. Es ist dementsprechend kein Zufall, dass selbst bei Bundesratssitzungen Mobilgeräte draussen bleiben müssen. Und es ist auch kein Zufall, dass Geheimdienste, andere Überwacher*innen oder das Militär gerne in elektronisch abgeschirmten Räumen operieren, damit Signale zumindest nicht unmittelbar nach aussen dringen können.

Faktisch ist die gesamte Schweizer Bevölkerung auf Schritt und Tritt überwacht.

Schweiz überwacht umfassend

Seit dem Inkrafttreten des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) im Jahr 2000 gibt es in der Schweiz für die Provider nicht nur die erwähnte Pflicht, ihre Teilnehmer*innen zu kennen, sondern auch systematisch und für sechs Monate festzuhalten, wer mit wem, wie lange, von wo aus kommuniziert. Damit ist faktisch die gesamte Schweizer Bevölkerung auf Schritt und Tritt überwacht. Das Resultat ist nicht nur ein recht vollständiges Kontaktnetz der Bevölkerung, sondern auch eine Übersicht über alle Bewegungen der hier ansässigen Menschen.

Dabei liegt Überwachung nicht erst dann vor, wenn diese Daten von Polizei, Staatsanwaltschaft oder dem Geheimdienst NDB – was seit Inkrafttreten des Nachrichtendienstgesetzes (NDG) 2016 auch möglich ist – ausgewertet werden. Bereits die Erfassung dieser Informationen ist eine Form der Überwachung. Schliesslich hat der Umstand, dass uns Provider, Polizei, Staatsanwaltschaft und NDB jederzeit orten können, erheblichen Einfluss auf unsere Freiheit.

Dieser Überwachungsdruck ist auch die Grundlage einer Beschwerde von Aktivist*innen des Chaos Computer Club und der Digitalen Gesellschaft Schweiz gegen die Vorratsdatenspeicherung. Darin wird argumentiert, dass sich Aktivist*innen – gerade in linken Kreisen – bewusst überlegen müssen, ob sie ihr Handy an Treffen mitführen oder nicht. Solche Überlegungen sollten in einer Gesellschaft, die sich frei schimpft, keine Rolle spielen. Die Beschwerde wurde bereits vor vielen Jahren angestrengt und schliesslich Anfang 2018 vom Bundesgericht abgewiesen. Es bestehe eine gesetzliche Grundlage und das Mittel sei darüber hinaus für Behörden geeignet, um mögliche Muster zu erkennen.

Entsprechend wurde die Beschwerde nun an den EGMR – den Europäischen Gerichtshof für Menschenrechte – weitergezogen. Der CCC und die Digitale Gesellschaft rechnen sich eine erhöhte Chance aus, dass die Schweiz für diese totalitäre Praxis gerügt wird. Es besteht also die Hoffnung, dass die Vorratsdatenspeicherung in der Schweiz abgeschafft werden kann.

Legale Schadsoftware

Dennoch: Da das Referendum gegen die Totalrevision des BÜPF gescheitert ist, sind seit März 2018 weitere Überwachungspraktiken legal. So ist es Staatsanwaltschaften nun erlaubt, Schadsoftware – in der Behördensprache «Govware» – einzusetzen. Dabei handelt es sich um eigentliche Staatstrojaner, mit denen in Geräte eingedrungen werden kann, um z. B. Gespräche mitzuhören oder Textnachrichten auszulesen. Dabei ist es einerlei, ob diese verschlüsselt versandt oder empfangen wurden.

Es ist zwar nicht damit zu rechnen, dass alle Smartphones direkt von den Staatsanwaltsschaften oder dem NDB verwanzt werden. Doch es ist Vorsicht angebracht; insbesondere für Aktivist*innen in linken Milieus. So ist es mit BÜPF und NDG möglich, sogenannte IMSI-Catcher einzusetzen. Diese täuschen eine Handyantenne vor und können mobil von Polizei oder Geheimdienst eingesetzt werden, um Menschenansammlungen zu fichieren. Damit ist es möglich, Personenkontrollen durchzuführen, ohne Menschen anzuhalten. Auch können Gespräche und Nachrichten mitgehört werden, ohne den Umweg über den Überwachungsdienst des Bundes machen zu müssen.

Handy zuhause lassen oder abschalten

Wer sicherstellen will, dass das Handy nicht als Ortungsgerät mit Wanzenfunktion eingesetzt werden kann, muss die Batterie entfernen. Ist das nicht möglich, sollte das Gerät zumindest abgestellt und in einem Behälter versorgt werden – zum Beispiel in eine Keksdose. Es ist jedoch zu beachten, dass Überwacher*innen aus solchen Informationen Schlüsse ziehen. Beim deutschen Soziologen Andrej Holm – der verdächtigt wurde, ideologischer Kopf der «militante gruppe» (mg) in Deutschland zu sein – wurden genau solche «Überwachungslücken» ausgenutzt. Die Ermittler*innen konstruierten, er habe gemeinsam mit anderen, bei denen auch Lücken vorhanden waren, an konspirativen Treffen teilgenommen.

*Gerade für linke Aktivist*innen ist Vorsicht angebracht.*

Solche Behauptungen lassen sich zumindest zerstreuen, wenn das Handy häufiger ausgeschaltet bleibt. Wer es für Alltagsaktivitäten dennoch für vertretbar hält, mindestens geortet werden zu können, sollte trotzdem wichtige Verhaltensregeln beachten und Werkzeuge einsetzen, um die Überwachungskosten zu erhöhen. Dafür empfiehlt sich ein Blick in den WOZ-Ratgeber, der als Protest gegen den «Swiss Digital Day» 2018 in einer Neuaflage erschienen ist. ■

https://www.woz.ch/system/files/epaper/woz/pdf/woz_digi-ratgeber_okt18.pdf