Die Verschlüsselung schlägt zurück

Kommen neue Kommunikationstechnologien auf, bleibt die Privatsphäre oft aussen vor. Doch kommt Zeit, kommt Rat: Schon bald werden wir uns der Staatskontrolle entziehen können.

von Chris Berg

Es ist eine der grossen Eigenarten der Geschichte der Kommunikationstechnologie: Der Schutz der Privatsphäre wird einer Technologie erst dann hinzugefügt, wenn diese schon lange und weitreichend verbreitet ist. Das erste Telefon zum Beispiel war ein technologisches Wunderwerk, aber nutzlos für diejenigen, die ihre Gespräche vertraulich behandeln wollten: Die geringe Verbindungsqualität bedeutete, dass die Benutzer oft schreien mussten, um am anderen Ende der Linie auch gehört zu werden. Partylines, bei denen sich Gruppen von Haushalten eine einzige Leitung teilten, hatten zur Folge, dass Nachbarn problemlos mitlauschen konnten. Auch musste man darauf vertrauen, dass die Telefonzentralenbetreiber selbst nicht mithörten.

Der frühe Telegraf war sogar noch schlimmer: Die Telegrafenbeamten wandelten Nachrichten manuell in Codes um. Eine Mitteilung wurde zwischen zahlreichen Beamten ausgetauscht, bevor sie schliesslich bei ihrer Zielperson ankam. Die Populärkultur im frühen 20. Jahrhundert kannte zahlreiche Geschichten von Telegrafisten und Telefonisten, die das Leben ihrer Kunden voyeuristisch mitverfolgten. Die Neuerungen, die es den Benutzern schliesslich erlaubten, andere von privaten Gesprächen auszuschliessen, wurden erst viel später entwickelt. Bei den Telefonen entwickelte man Privatleitungen und automatische Telefonzentralen. Für den Telegrafen lag die Innovation in der Kryptografie, die es den Korrespondenten schliesslich ermöglichte, die Bedeutung ihrer Nachrichten vor den Vermittlern der Telegrafengesellschaft zu verbergen.

Was heute auf dem Spiel steht

Zunächst die Technologie, erst später dann die Privatsphäre; zwei Jahrzehnte nach Beginn des 21. Jahrhunderts lässt sich diese Abfolge erneut beobachten. Doch dieses Mal steht viel mehr auf dem Spiel: Während der Wirkungsbereich vom Telegrafen und dem frühen Telefon eher begrenzt ausfiel, hat die neuste Generation der Kommunikationstechnologien jeden Aspekt unseres Lebens durchdrungen. Fast alles, was wir tun – jede Interaktion mit unseren Arbeitskollegen, mit dem Handel, mit unseren Familien und Ehepartnern –, hinterlässt eine Spur von Daten, die zusammengenommen ein intimes, nahezu vollständiges Bild unseres Lebens ergeben.

Die Privatsphäre wird oft als Schutz vor der eigenen Regierung betrachtet – was einige Konservative dazu veranlasst, kleinlaut zu argumentieren, man habe nichts zu befürchten, wenn man nichts zu verbergen habe. Doch Privatsphäre in einem modernen Kontext bedeutet viel mehr: In der globalisierten und digitalen Welt von heute sollten wir genauso darauf achten, unsere Daten auch vor ausländischen Regierungen geheim zu halten. Möglicherweise möchten wir verhindern, dass der Arbeitgeber von einer Bürobeschwerde Wind bekommt. Oder vielleicht wollen wir Geld vor einem kontrollsüchtigen Lebenspartner verbergen. Die Krise der Privatsphäre im 21. Jahrhundert besteht darin, dass die Instrumente, mit denen wir tagtäglich unser Leben organisieren, beunruhigend unsicher und wir infolgedessen in verstörendem Ausmass exponiert sind – gegenüber Regierungen, Unternehmen und unseren Mitmenschen.

Kryptografische und zensursichere Technologien bieten uns einen Ausweg aus dem digitalen Chaos unserer Gegenwart. Die allgegenwärtige Ende-zu-Ende-Verschlüsselung für den Verbraucher, der Einsatz mathematischer Techniken wie Zero-Knowledge-Proofs und Differential Privacy sowie die Entwicklung digitaler Infrastrukturen wie der Blockchain und der Distributed-Ledger-Technologie bieten ein leistungsfähiges Instrumentarium, um unsere Daten zu sichern, unsere Geheimnisse zu verbergen und unsere privaten Informationen zu schützen. Diese Innovationen versprechen uns nicht nur eine grössere Kontrolle über persönliche Informationen und den Schutz der Privatsphäre. In vielerlei Hinsicht stellen sie eine grundlegende Machtverschiebung vom Staat zum Bürger dar – sie schaffen private Bereiche, in die nicht eingegriffen werden kann.

Kampf der Regierungen ums Überleben

Snowdens Enthüllungen im Jahr 2013 haben den Ball ins Rollen gebracht: Dass der amerikanische Auslandsgeheimdienst NSA die Fähigkeit von Technologieunternehmen ausnutzte, um so auf Da-

ten ihrer eigenen Kunden zuzugreifen, führte nämlich nicht nur zu einem öffentlichen Aufschrei. Vielmehr war die Entlarvung der Auslöser einer stillen technischen Revolution, bei der einige dieser Unternehmen sich selbst den Zugang zu Kundendaten entzogen. Ende-zu-Ende-Verschlüsselung beschreibt eine Methode zur Verschlüsselung von Nachrichten, bei der nur der Absender und der Empfänger über die Möglichkeit zur Entschlüsselung verfügen. Die Firmen, die die Nachricht weiterleiten (wie z.B. Internet-Service-Provider oder Messaging-Anwendungen), können sie nicht lesen. Beliebte Kommunikationsclients wie WhatsApp, Telegram und sogar Facebook Messenger bieten diese Art der Verschlüsselung jetzt standardmässig oder als Zusatzfunktion an.

«Die Regierungen in aller Welt verlieren ihre Fähigkeit, uns zu beobachten.»

Chris Berg

Der massenhafte Einsatz von Ende-zu-Ende-Verschlüsselung hat den Zugang, den Regierungsbehörden bisher zu unserer Kommunikation hatten, dramatisch erschwert. Viele westliche Sicherheitsbehörden plädieren darum für einen privilegierten Zugang zu verschlüsselter Kommunikation («Hintertüren»). Die Europäische Union zum Beispiel möchte neuerdings die Kommunikationsdienstleister dazu verpflichten, einen ausserordentlichen Zugang zu verschlüsselten Nachrichten zu schaffen. Die verzweifelten Argumente beweisen vor allem eines: Die Regierungen in aller Welt verlieren ihre Fähigkeit, uns zu beobachten. Die technisch anmutende Diskussion über Verschlüsselung ist ein Vorgeschmack auf eine viel grössere Debatte rund um die Staatsmacht, die bald schon stattfinden wird.

Bedenken Sie die langfristigen Auswirkungen einer der aufregendsten Neuerungen im Bereich der Kryptowährungen: der sogenannten Zero-Knowledge-Proof-Protokolle. Hierbei handelt es sich um eine kryptografische Technik, die es den Benutzern erlaubt, mit mathematischer Sicherheit zu beweisen, dass sie eine Information kennen, ohne etwas über die Information selbst weiterzugeben. Bei Bitcoin kann jeder Nutzer alle Transaktionen mit einem Webbrowser verfolgen und auf ihre Richtigkeit untersuchen – es ist diese kollektive Überprüfbarkeit, die Bitcoin seine Sicherheit gibt. In Zcash, einer auf den Schutz der Privatsphäre ausgerichteten Variante von Bitcoin, sind Sender, Empfänger, Betrag und sogar Datum jeder Transaktion kryptografisch verborgen; Zero-Knowledge-Proof-Protokolle ermöglichen es Beobachtern, diese Transaktionen auf ihre Legitimität zu prüfen. Die Existenz privater digitaler Transaktionen ist an sich schon potentiell revolutionär und hat enorme Auswirkungen auf die Besteuerung und Regulierung: Werden Regierungen in der Lage sein, etwas zu besteuern, das sie gar nicht sehen können?

Die Gunst der Stunde nutzen

Der Silicon-Valley-Investor Marc Andreessen schrieb einmal, dass «Software die Welt frisst»: Früher oder später wird alles digitalisiert werden. Wenn die Wirtschaft online geht – wenn Verträge, Unternehmen und das Finanzsystem digitalisiert und automatisiert werden –, wird es möglich sein, den Datenschutz von Anfang an in unser Wirtschaftssystem miteinzubauen. Sogenannte «Smart Contracts» ermöglichen es uns, algorithmische Geschäftsvereinbarungen zu schreiben, die sich auf der Blockchain selber durchsetzen. Durch das Hinzufügen von Zero-Knowledge-Proof-Protokollen entsteht eine Vision digitaler Geschäftsaktivitäten, die vollständig privat und für Regierungen nicht regulierbar sind.

Viele der frühen Internetpioniere bedauern heute, dass die Privatsphäre nicht von Anfang an in das Internet eingebaut wurde. Es ist leicht, sich einen alternativen Weg vorzustellen, den die Digitalisierung des Alltagslebens in ihrer knapp 25jährigen Wirkungsgeschichte hätte nehmen können – einen Weg, der sich um den Schutz persönlicher Informationen kümmert, bei dem Sicherheit ebenso im Mittelpunkt steht wie Zugänglichkeit. Und bei dem das Verstecken von Information ähnlich bequem und unkompliziert wie das Teilen ist. Doch dank den neuen technologischen Möglichkeiten rückt das Ziel einer datenschutzzentrierten Welt näher – und mit ihm auch die Aussicht auf menschliche Freiheit. ‹

Aus dem Englischen übersetzt von Jannik Belser.

Chris Berg
ist Postdoctoral Fellow beim RMIT Blockchain Innovation Hub in Melbourne. Er ist Co-Autor von «The New Technologies of Freedom» (American Institute for Economic Research, 2020).