Sachdokumentation:

Signatur: DS 4039

Permalink: www.sachdokumentation.ch/bestand/ds/4039

Zitierweise für graue Literatur

Elektronische Broschüren und Flugschriften (DS) aus den Dossiers der Sachdokumentation des Sozialarchivs werden gemäss den üblichen Zitierrichtlinien für wissenschaftliche Literatur wenn möglich einzeln zitiert. Es ist jedoch sinnvoll, die verwendeten thematischen Dossiers ebenfalls zu zitieren. Anzugeben sind demnach die Signatur des einzelnen Dokuments sowie das zugehörige Dossier.

LI-Paper

Zur Zukunft der Privatsphäre

DARCY ALLEN, CHRIS BERG, SINCLAIR DAVIDSON * • Juli 2022

Zusammenfassung

- Es ist schwierig, ein individuelles Freiheitsrecht zu finden, das die Spannungen zwischen Privatautonomie und staatlicher Macht besser verkörpert als die Privatsphäre. Ein Kernelement des klassisch liberalen Verständnisses ist die fundamentale Unterscheidung zwischen öffentlichem Leben (der Raum der Gesellschaft und der Politik) und Privatleben (die Sphäre des Vergnügens, der Intimität und des Rückzugs). Doch auch wenn die Privatsphäre ein grundlegendes Freiheitsrecht ist, scheint sie dennoch eine Freiheit zu sein, die sich auf dem Rückzug befindet. Auch liberale Demokratien setzen mehr und mehr auf Überwachung.

- Zurzeit scheint es nicht gut bestellt zu sein um das Recht auf Privatsphäre, zumal sowohl Staaten als auch Unternehmen in unsere privaten Bereiche eindringen. Die Staatsgewalt überwacht ihre Bevölkerung, um alles Mögliche zu beobachten – es geht um Dinge wie etwa die nationale Sicherheit bis hin zu Verkehrsdelikten. Gleichzeitig legen wir gegenüber Firmen, mit denen wir interagieren, Tag für Tag grosse Mengen an Informationen über uns selbst offen. Natürlich sind die beiden Dinge moralisch nicht vergleichbar: Während die Offenlegung von Daten gegenüber Firmen auf einer freiwilligen Basis geschieht, damit wir im Gegenzug deren Produkte und Dienstleistungen (kostenlos) nutzen können, geschieht die staatliche Überwachung ohne unsere Einwilligung.

- Doch der Abgesang auf die Privatsphäre ist verfrüht. Eine neue Generation von Technologien verspricht die Landschaft zwischen privater Information und öffentlicher Sphäre radikal umzupflügen. Dies wird sowohl für die Art, wie wir unsere persönlichen Informationen schützen, als auch die Funktionsweise des Staats dramatische Konsequenzen haben. Viele der Bausteine dieser technologischen Revolution sind für die Benutzer von Smartphones und Computern bereits erhältlich.

* Darcy W. E. Allen ist Ökonom, Publizist und Forscher am RMIT Blockchain Innovation Hub, mit Sitz an der RMIT University in Melbourne. Chris Berg ist Principal Research Fellow und Co-Direktor des RMIT Blockchain Innovation Hub in Melbourne. Sinclair Davidson ist Professor für Institutional Economics am Blockchain-Departement an der RMIT University in Melbourne.

Es ist schwierig, ein individuelles Freiheitsrecht zu finden, das die Spannungen zwischen Privatautonomie und staatlicher Macht besser verkörpert als die Privatsphäre. Ein Kernelement der klassisch liberalen Vision ist die fundamentale Unterscheidung zwischen öffentlichem Leben (der Raum der Gesellschaft und der Politik) und Privatleben (die Sphäre des Vergnügens, der Intimität und des Rückzugs).[1] Hayek schrieb dazu in seinem Werk *Verfassung der Freiheit*:

> *«Die Anerkennung einer geschützten individuellen Sphäre beinhaltet in Zeiten der Freiheit normalerweise ein Recht auf Privatheit und Geheimhaltung, die Vorstellung, dass das Haus eines Menschen seine Burg ist und dass niemand ein Recht hat, seine Aktivitäten darin auch nur zur Kenntnis zu nehmen.»*[2]

Repressive Staaten arbeiten hart daran, diese wichtige Unterscheidung zu untergraben. Sie fühlen sich allein schon durch die Idee bedroht, dass es eine Sphäre gibt, in welche sie nicht vordringen dürfen. Die schlimmsten Diktaturen des 20. Jahrhunderts waren Überwachungsstaaten. Im sowjetischen Russland wurden Familien in gemeinsame Appartements getrieben, wo sich die Nachbarn gegenseitig überwachten und bei Ordnungswidrigkeiten an die Autoritäten verpfiffen.[3] Die Roten Khmer, eines der brutalsten Regimes in der menschlichen Geschichte, deportierten die Bevölkerung Kambodschas in Gemeinschaftswohnräume, wo sie Gemeinschaftsmahlzeiten zu sich nahmen und in Gemeinschaftszeremonien verheiratet wurden. Eine Parole der Roten Khmer lautete: «Hege keine privaten Gedanken!».[4]

Doch auch wenn die Privatsphäre ein grundlegendes Freiheitsrecht ist, scheint sie dennoch eine Freiheit zu sein, die sich auf dem Rückzug befindet. Sogar liberale Demokratien setzen mehr und mehr auf Überwachung. Eine Schätzung geht davon aus, dass es allein in London mehr als 620 000 Videoüberwachungskameras gibt – das macht eine Kamera pro vierzehn Einwohner.[5] Die Entwicklung hin zu «Smart Cities» – also zur Städteplanung anhand von Datenanalysen – hat zu einer starken Verbreitung von Sensoren geführt, die etwa den Strassenverkehr, die Fussgängerströme und die Nutzung von Gebäuden und öffentlichen Plätzen messen. Diese Kameras sind zu immer mehr fähig. Das heisst, sie können z. B. die Nummernschilder identifizieren und sie mit anderen Datenbanken abgleichen. Auch ist die neue Generation dieser Überwachungskameras in der Lage, Gesichter zu erkennen.

Nur ein Bruchteil der Überwachungskameras befindet sich im Besitz oder unter der Kontrolle des Staats. Die meisten dieser Kameras werden vom Privatsektor eingesetzt – genau genommen im Verhältnis 70 zu 1.[6] Einige davon werden durch das

[1] Chris Berg (2018). The Classical Liberal Case for Privacy in a World of Surveillance and Technological Change. Palgrave Macmillan.
[2] Friedrich A. von Hayek (1960). The Constitution of Liberty: The Definitive Edition. Chicago, Illinois: University of Chicago Press. S. 209.
[3] Orlando Figes (2008). The Whisperers: Private Life in Stalin's Russia. London: Penguin Books; Lynne Attwood (2017). Gender and Housing in Soviet Russia: Private Life in a Public Space. Manchester: Manchester University Press.
[4] H. Locard (2004). Pol Pot's Little Red Book: The Sayings of Angkar. Chiang Mai, Thailand: Silkworm Books.
[5] Jonathan Ratcliffe (29. Mai 2019). How Many CCTV Cameras Are There in London 2019? CCTV.co.uk.
[6] British Security Industry Association (2013). The Picture Is Not Clear: How Many CCTV Surveillance Cameras Are There in the UK? British Security Industry Association.

Gesetz vorgeschrieben: Mehrere Städte verpflichten etwa die Nachtclubs, Videokameras an Ein- und Ausgängen zu installieren. Die meisten jedoch werden dazu eingesetzt, Eigentumsverletzungen präventiv entgegenzuwirken oder diese aufzuklären.

Ist die Privatsphäre tot?

Zurzeit scheint es nicht gut bestellt um das Recht auf Privatsphäre, zumal sowohl Staaten als auch Unternehmen in unsere privaten Bereiche eindringen. Die Staatsgewalt überwacht ihre Bevölkerung, um alles Mögliche zu beobachten – es geht um Dinge wie etwa die nationale Sicherheit bis hin zu Verkehrsdelikten. Gleichzeitig legen wir gegenüber Firmen, mit denen wir interagieren, Tag für Tag grosse Mengen an Informationen über uns selbst offen. Wir veröffentlichen persönliche Dinge auf Social-Media-Plattformen. Mobilfunkanbieter wissen ganz genau, wo wir uns gerade aufhalten, weil unser Mobiltelefon unseren Standort übermittelt. Kreditkartenanbieter erfahren, was wir wo, wann und bei wem zu welchen Preisen gekauft haben. Intime Daten über unsere Beziehungen und Präferenzen, die von uns besuchten Websites wie auch die von uns angeschauten Videoclips werden gespeichert.

Natürlich sind die beiden Dinge moralisch nicht vergleichbar: Während die Offenlegung von Daten gegenüber Firmen auf einer freiwilligen Basis geschieht, damit wir im Gegenzug deren Produkte und Dienstleistungen (kostenlos) nutzen können, geschieht die staatliche Überwachung ohne unsere Einwilligung. Was Edward Snowden 2013 über die massive Überwachungstätigkeit der Staatsgewalt ans Tageslicht brachte, offenbarte sogar ihren unrechtmässigen Charakter. Der klassische Liberalismus unterscheidet hier klar zwischen diesen beiden Situationen und Organisationsformen. Nichtsdestotrotz sorgen sich viele hinsichtlich der staatlichen Überwachung, während sie gleichzeitig relativ bedenkenlos «Smart Home Devices» wie etwa Google Home oder Alexa bei sich zu Hause einrichten, die passiv bei allen intimen Konversationen mithören.[7]

Es ist also kein Wunder, dass man heute oft zu hören bekommt, die Privatsphäre sei tot. In der Tat fällt es angesichts der Berichterstattung, in welcher regelmässig von Datenschutzverletzungen und Datenmissbrauch berichtet wird, nicht schwer, eine pessimistische Sichtweise zu entwickeln.

Doch der Abgesang auf die Privatsphäre ist verfrüht. Eine neue Generation von Technologien verspricht die Landschaft zwischen privater Information und öffentlicher Sphäre radikal umzupflügen. Dies wird sowohl für die Art, wie wir unsere persönlichen Informationen schützen, als auch die Funktionsweise des Staats dramatische Konsequenzen haben. Viele der Bausteine dieser technologischen Revolution sind für die Benutzer von Smartphones und Computern bereits erhältlich. Um aber diese neuen Technologien der Freiheit zu verstehen, müssen wir uns anschauen, wie sich die Welt seit der Enthüllung des wohl grössten Privatsphären-Skandals entwi-

[7] Manchmal kann allerdings auch von «passiv» keine Rede sein. Siehe dazu beispielsweise Matt Day, Giles Turner und Natalia Drozdiak (11. April 2019). Amazon Workers Are Listening to What You Tell Alexa. Bloomberg.

ckelt hat, nämlich die 2013 von Edward Snowden publik gemachte Überwachungsaktivität durch die National Security Agency (NSA) zur Beobachtung der Internetkommunikation des ganzen Planeten.

Die Snowden-Enthüllung

Die Terroranschläge vom 11. September 2001 offenbarten ernsthafte Schwächen der US-Geheimdienste, teilweise auch, weil die Geheimdienstkreise in den USA immer noch auf den – durch den Kalten Krieg dominierten – Wettbewerb der Grossmächte ausgerichtet waren.[8] Im Nachgang der Anschläge leistete die NSA, die bedeutende staatliche Geheimdienstagentur der USA, einen konzentrierten Effort zur Ausweitung ihrer Überwachungsmöglichkeiten des Telefon- und Internetverkehrs. Zwischen 2005 und 2014 wurde die NSA von General Keith B. Alexander geleitet, der den Fokus auf eine massive Datensammlung legte. Einer seiner früheren Mitarbeiter meinte gegenüber *Foreign Policy*: «Alexanders Strategie ist die gleiche wie jene von Google: Ich muss alle Daten sammeln.»[9]

Die extrem breite Interpretation des 2001 erlassenen «Patriot Act» ermöglichte es der NSA, alle Telekommunikationsanbieter zu zwingen, ihre kompletten Anrufdaten und Telefonaufnahmen der NSA zur Verfügung zu stellen, damit diese die Daten durchsuchen und abrufen konnte – unabhängig davon, ob die Daten im Zusammenhang mit einem Terrorverdacht standen oder nicht.[10] Ähnliche Arrangements wurden mit Internetservice-Dienstleistern, Digitalplattformen, Software-Firmen, Telekommunikationsinfrastruktur-Anbietern und Hardware-Entwicklern aufgegleist. Das Resultat war, dass die NSA massive und umfangreiche Datensätze sammeln und auswerten konnte.

Das Ausmass dieses Programms wurde 2013 vom Computersystem-Manager Edward Snowden enthüllt, der verschiedentlich für die CIA und als privater Auftragnehmer für die NSA arbeitete. Er spielte mehreren prominenten Medien interne NSA-Dokumente zu, darunter dem *Guardian*, dem *Spiegel* und der *Washington Post*. Dieser Leak führte zu einer globalen Entrüstungswelle und einer breitflächigen Debatte über Internetsicherheit und Privatsphäre, die von demokratischen Staaten bedroht wurden.

Die Antwort kam vom Privatsektor, nicht von der Politik

Bemerkenswert ist, dass politische Reformen als Antwort auf diese globale Entrüstung grösstenteils ausblieben. Die gesetzlichen Rahmenbedingungen, die es der

[8] Amy B. Zegart (2006). An Empirical Analysis of Failed Intellligence Reforms before September 11. Political Science Quarterly 121 (1): S. 33–60.
[9] Shane Harris (9. September 2013). The Cowboy of the NSA. Foreign Policy.
[10] Eine nützliche Übersicht über die politische und rechtliche Basis des Programms lieferte: Julian Sanchez (5. Juni 2014). Snowden: Year One. Cato Unbound. Siehe dazu auch: Glenn Greenwald (2014). No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State. Henry Holt and Company; Timothy H. Edgar (2017). Beyond Snowden: Privacy, Mass Surveillance, and the Struggle to Reform the NSA. Brookings Institution Press; Edward Snowden (2019). Permanent Record. UK: Pan Macmillan.

NSA ermöglichen, eine enorme Masse von Daten zu sammeln, gibt es auch heute noch. Und diverse weitere Staaten, unter anderem auch die Schweiz, erliessen sogar neue Gesetze, die es ihnen erlauben, noch mehr Daten zu erheben und diese noch länger zu speichern.

Die überzeugendste Antwort auf die Snowden-Enthüllungen kam vom Privatsektor. Snowden führte uns vor Augen, wie eng Technologiefirmen mit dem Staat im Bereich der Massenüberwachung der Bevölkerung kooperierten. Der öffentliche Druck – oder auch nur das öffentliche Bewusstsein – hat diese Beziehung erschüttert. Das gilt zumindest für viele der prominentesten, verbrauchernahen Firmen. Wie der Kryptograf Matthew Green schreibt: «Es ist einfach zu vergessen, wie viele Dinge sich seit den Snowden-Enthüllungen geändert haben.»[11] Vor 2013 wurden Internet- und Telekommunikationsnachrichten grösstenteils im sogenannten «Plaintext» verschickt – also unverschlüsselt, sodass nicht nur diejenigen, die einen Schlüssel für die Nachricht besassen, darauf zugreifen konnten. Als Snowden enthüllte, dass die NSA in der Lage war, die Verschlüsselung vieler gängiger Kommunikationsdienstleister zu knacken, griff ein bedeutender Anteil der digitalen Kommunikation noch nicht einmal auf solche Verschlüsselungsmethoden zurück.

Die Jahre nach der Snowden-Enthüllung waren jedoch geprägt von einer grossen Anzahl neuer Dienstleistungen, welche die Privatsphäre der Nutzer in der Internetkommunikation stark ausweiteten. Beispielsweise ermutigten Digitalplattformen wie Google die Website-Administratoren, vom HTTP-Protokoll (dem traditionellen Kommunikationsstandard, der von Websites benutzt wurde) zum sichereren HTTPS-Protokoll zu wechseln, bei welchem die Kommunikation zwischen Browser und Website verschlüsselt wird. Eine weitere grosse Veränderung war die Ablösung von SMS durch Messaging-Services, die eine End-zu-End-Verschlüsselung anbieten. Diese stellt sicher, dass der Inhalt der Nachricht nur vom Absender und vom Empfänger gelesen werden kann, nicht jedoch vom Messaging-Provider. Heute gibt es eine enorme Menge an zentralisierten und dezentralisierten Messaging-Apps – beispielsweise Signal, Telegram, Keybase und Threema – die damit begonnen haben, den Kundenwunsch nach einer sicheren Kommunikation zu befriedigen.

Seit der Entstehung der Informatik war die Kommunikation von Person zu Person mit Sicherheitslücken behaftet. Die E-Mail-Verschlüsselung hat sich zum Beispiel noch nicht im grossen Stil durchgesetzt.[12] Die plötzliche und rasche Post-Snowden-Adoption der verschlüsselten Online-Kommunikation stellt daher eine fundamentale Veränderung in der Architektur des Internets dar. Diese kommt allen Nutzern digitaler Technologien zugute, weil sie nicht nur dem masslos invasiven Staat Grenzen setzt, sondern die Akteure auch vor anderen feindseligen Akteuren und Kriminellen schützt.

[11] Matthew Green (24. September 2019). Looking Back at the Snowden Revelations. A Few Thoughts on Cryptographic Engineering.
[12] LaFleur, Kendal Stephens und Lei Chen (2014). Email Encryption: Discovering Reasons Behind Its Lack of Acceptance. Vortrag auf der Internationalen Konferenz für Sicherheit und Management (SAM) in Las Vegas, 21.–24. Juli.

Hintertür für den Überwachungsstaat?

Natürlich können diese Verschlüsselungstechnologien nicht nur von guten, sondern auch von bösen Akteuren benutzt werden. Wer jedoch nun dafür argumentiert, dass die Verschlüsselungs-Codes so programmiert sein müssten, dass sie staatlichen Überwachungsorganen einen Zugang durch die Hintertür ermöglichen, der denkt einseitig an die guten Seiten der Staatsgewalt in liberalen Demokratien. Doch vertraut man auch den Regierungen in unfreien Ländern, die ebenso Zugang zu unseren, am globalen Internet angeschlossenen Geräten haben? Will man wirklich, dass diese Mächte durch solche Hintertüren ebenfalls Zugang zu unserer privaten Kommunikation erhalten? Die Bemühungen der Technologieanbieter zu behindern, ihre Kunden vor *allen* ungebetenen Mitlesern zu schützen, schwächt letztlich die Sicherheit von uns allen.[13]

Dieser Disput zwischen Verschlüsselungs-Befürwortern und Technologiefirmen auf der einen Seite und Strafverfolgungsbehörden und Geheimdiensten auf der anderen Seite hat eine grössere Bedeutung, als es zunächst erscheinen mag. Entgegen der Behauptung von Strafverfolgungsbehörden befinden wir uns heute in Wahrheit in einem «goldenen Zeitalter» der Überwachung, wie es der Akademiker Peter Swire genannt hat.[14] Weil unsere Internetaktivitäten Spuren hinterlassen und unsere Geräte mehr und mehr Daten über uns aufzeichnen, werden diese Aufnahmen zum Ziel von staatlichen und nichtstaatlichen Instanzen.

Niemals zuvor in der Geschichte waren Strafverfolgungsbehörden in der Lage, an eine komplette Aufzeichnung unserer Bewegungen zu kommen, die durch GPS-basierte Landkartensoftware und das konstante Anpeilen durch Mobilfunkmasten ermöglicht wird. Noch nie zuvor in der Geschichte konnten die Überwachungsorgane derart genau sagen, womit wir uns den ganzen Tag so beschäftigen. Heute können sie das sehr präzise aufgrund unserer Internetsuchanfragen, E-Mails, Textnachrichten, des dichten Netzes an Überwachungskameras, unserer Interaktion mit «Smart Home Devices», «Car Sharing Apps» … Diese Liste könnte noch sehr lange weitergeführt werden.

Die australische Regelung zur Vorratsdatenspeicherung zum Beispiel, die von Internetanbietern verlangt, Metadaten über Internetaktivitäten für mindestens zwei Jahre zu speichern, erfordert von den Strafverfolgungsbehörden keinen Durchsuchungsbefehl, um auf einige der persönlichsten Daten zuzugreifen – etwa mit wem die Bürger E-Mails austauschen und welche Websites sie aufrufen.

In diesem Kontext sind Tools, die das unberechtigte Zugreifen auf Informationen von Konsumenten oder Bürgern durch den Staat, Firmen, Arbeitgeber, Mitarbeiter und sogar unsere Freunde und Familie verhindern wollen, wichtige Waffen im Arsenal der Freiheit. Als die klassischen Ideen über die Privatsphäre in der ersten Hälfte des

[13] Hal Abelson et al. (1997). The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption. World Wide Web Journal 2 (3), S. 241–257.
[14] Peter Swire (8. Juli 2015). Going Dark: Encryption, Technology, and the Balance between Public Safety and Privacy. Hearing by Senate Judiciary Committee.

20. Jahrhunderts entwickelt wurden, lautete die Kernfrage, welche rechtlichen Rahmenbedingungen dieses komplexe Recht am besten zu schützen vermögen.[15] Jetzt, im dritten Jahrzehnt des 21. Jahrhunderts lautet die Frage vielmehr, wie man Technologien am besten nutzt, um die Privatsphäre zurückzuerobern – und wie der Staat darauf reagieren sollte.

Privatsphäre ohne Geheimhaltung

1985 veröffentlichte der Computer-Wissenschaftler David Chaum ein Paper im Journal «IEEE Security & Privacy» mit dem Titel *Security without Identification: Transaction Systems to Make Big Brother Obsolete*. In den 1980er-Jahren lag die weitverbreitete Nutzung des Internets noch mindestens ein Jahrzehnt in der Zukunft. Doch Chaum schrieb schon damals vorausschauend: «Die Digitalisierung raubt dem Einzelnen die Möglichkeit, die Art und Weise zu überwachen und zu kontrollieren, wie Informationen über ihn verwendet werden.»[16]

Chaum identifizierte zwei mögliche Zukunftsszenarien: Im ersten Szenario führt die Digitalisierung der Wirtschaft zu einer ökonomischen Zentralisierung. Grosse Firmen und grosse Staaten würden dann enorme Mengen an Informationen über die Individuen sammeln und diese dafür nutzen, um an Grösse und Einfluss hinzuzugewinnen. Im zweiten Zukunftsszenario hingegen gibt es eine Möglichkeit, persönliche Informationen in «separate und unverbundene Beziehungen aufzuteilen», indem Kryptografie verwendet wird, um die Verbindung zwischen einem Individuum und seinen persönlichen Daten undurchsichtig zu gestalten. Diese Technologie könne nicht nur die ökonomische Zentralisierung rückgängig machen, sondern auch zu einer radikalen Dezentralisierung führen.

Chaums Essay war eines der frühen Dokumente der sogenannten «Cypherpunk-Bewegung», die mit dem Begriff «Cyberpunk» spielt und die politische sowie ökonomische Rolle der Kryptografie betont. Schon diese frühen Cypherpunks waren also davon überzeugt, dass das Schützen persönlicher Daten eine radikale Veränderung in der Beziehung zwischen Individuen und Organisationen bewirken wird. Chaum zog am Ende seines Essays das folgende Fazit:

> *«Fortschritte in der Informationstechnologie gingen schon immer mit grossen Veränderungen in der Gesellschaft einher: Der Übergang von Stammesgesellschaften zu grösseren hierarchischen Formen wurde zum Beispiel von der Schriftsprache begleitet, und die Drucktechnik trug zur Entstehung grosser Demokratien bei. Die Koppelung von Computern mit der Telekommunikation schafft das, was als das ultimative Medium bezeichnet wurde – es ist sicherlich*

[15] Zum Beispiel: Alan F. Westin (1967). Privacy and Freedom. New York: Atheneum.
[16] David Chaum (1985). Security without Identification: Transaction Systems to Make Big Brother Obsolete. Communications of the ACM 28 (10). S. 1030.

ein grosser Fortschritt im Vergleich zum Papier. Man könnte nun fragen: Zu welchen Gesellschaftsformen könnte diese neue Technologie führen? Die beiden Ansätze scheinen ganz unterschiedliche Antworten zu enthalten.»[17]

Andere Cypherpunks gingen noch einen Schritt weiter. In seinem 1988 veröffentlichten *Crypto Anarchist Manifesto* verglich Timothy May die Verbreitung von Kryptografie in der digitalen Kommunikation mit der Entwicklung von Eigentumsrechten:

«So wie die Technologie des Buchdrucks die Macht der mittelalterlichen Zünfte reduzierte und das gesellschaftliche Machtgefüge umpflügte, so werden auch kryptografische Methoden das Wesen von Unternehmen und die staatliche Einmischung in wirtschaftliche Transaktionen grundlegend verändern. In Kombination mit den entstehenden Informationsmärkten wird die Krypto-Anarchie einen liquiden Markt für alles schaffen, was sich in Worte und Bilder fassen lässt. Und so wie eine scheinbar unbedeutende Erfindung wie der Stacheldraht die Umzäunung riesiger Ländereien und Farmen ermöglichte und damit die Konzepte von Land und Eigentumsrechten im Wilden Westen für immer veränderte, so wird auch die scheinbar unbedeutende Entdeckung aus einem geheimnisvollen Zweig der Mathematik die Möglichkeiten des geistigen Eigentums verändern.»[18]

Ins Geld eingebaute Privatsphäre

In seinen frühen Jahren schien der Bitcoin, der eindeutig aus diesem Cypherpunk-Milieu hervorging, die Manifestation dieser ideologischen Ziele zu sein. Bitcoin offerierte eine digitale Währung, die unabhängig sowohl von Staaten und ihren Zentralbanken wie auch vom privaten Bankensystem war. Die Nutzer interagieren lediglich durch digitale Adressen, «Peer to Peer», ohne zentrale Autorität, die das ganze unter Kontrolle hält. Diese Erfindung war ein institutioneller Schock. Als Staatsautoritäten zum ersten Mal auf Bitcoin aufmerksam wurden, war ihre Hauptbefürchtung, dass dies das Ende der Finanzmarkt- und Steueraufsichtsbehörden sein könnte. Auch heute noch ist eine oft gestellte Frage der Steuerämter, wie man Transaktionen in Bitcoin erfolgreich besteuern könne.

Doch bei aller Innovation, die der Bitcoin mit sich brachte, steht er nicht für eine wasserdichte Privatsphäre im Bereich der finanziellen Transaktionen. In Tat und Wahrheit schafft sich der Bitcoin das Vertrauen gerade durch seine öffentliche Natur: Jeder Nutzer des Bitcoin-Netzwerks kann, wenn er das will, jede einzelne Bitcoin-Transaktion nachverfolgen – und das bis zur allerersten Transaktion von Satoshi Nakamoto. Zwar ist eine Bitcoin-Adresse nicht direkt an die Identität einer Person geknüpft. Doch für Steuer- und Strafverfolgungsbehörden ist es relativ einfach, Transaktionen nachzuverfolgen und Bitcoin-Adressen Individuen zuzuordnen. Bitcoin ist deshalb wesentlich weniger anonym als Bargeld.

[17] Ebd., S. 1044.
[18] Timothy C. May (22. November 1992). The Crypto Anarchist Manifesto.

Unter anderem aus diesem Grund begannen viele Unternehmer und Hobby-Programmierer, mit der Struktur der von Satoshi initiierten Kryptowährung zu spielen, um so die Privatsphäre der Nutzer besser zu schützen. Frühe Versuche hantierten mit sogenannten «Mixern» oder «Tumblern», die verschleiern, woher eine gewisse Transaktion stammt und wohin diese gesendet wird, indem die Überweisung mit anderen Überweisungen zusammengemischt wird. Die 2014 lancierte Kryptowährung Monero baute die Privatsphäre direkt ins Protokoll ein: Der Sender, Empfänger und die Summe der Transaktion sind privat, während Monero dennoch ein öffentlich überprüfbares Hauptbuch bleibt.

Eine andere Kryptowährung, die sich auf den Schutz der Privatsphäre seiner Nutzer fokussiert, ist Zcash. Obwohl sie eine öffentlich einsehbare Blockchain ist, benutzt sie einen sogenannten «Zero-Knowledge Proof», um die Transaktionsdetails vor Drittparteien geheim zu halten. «Zero-Knowledge Proofs» sind eine Art mathematischer Beweis, welcher es einem Transaktionsteilnehmer erlaubt, einem anderen Transaktionsteilnehmer zu beweisen, dass er über eine gewisse Tatsache Bescheid weiss, ohne dass er diese Tatsache offenlegen muss. Es ist ein Weg, anderen zu beweisen, dass man im Besitz eines konkreten Wissens ist, ohne die Details dieses Wissens verraten zu müssen.

«Zero-Knowledge Proofs» stellen damit generell eine grosse Chance dar, die Privatsphäre besser zu schützen. Es gibt viele Situationen im Leben, in denen wir etwas beweisen wollen oder müssen. Nehmen wir beispielsweise an, dass wir das Recht erlangt hätten, Autofahren zu dürfen, oder dass wir alt genug seien, um ein alkoholisches Getränk zu erwerben. Wir müssen uns dazu in vielen Fällen mit einem Führerschein oder einer ID ausweisen. Doch wenn wir unsere Identifikationskarten jemandem zeigen, offenbaren wir dieser Person oder Stelle viel mehr als nur die Tatsache, dass wir das Recht haben, ein Auto zu fahren oder etwas zu kaufen. Wir teilen dem Polizeibeamten oder dem Clubbetreiber auch unseren Namen, unser genaues Geburtsdatum und je nach Land auch unsere Adresse mit. Dies sind wesentlich mehr Informationen, als nötig wären, um den entsprechenden Beweis zu erbringen. «Zero-Knowledge Proofs» erlauben uns, die Menge an Informationen, die wir mit anderen teilen, drastisch zu reduzieren.

Was diese Technologie bietet, ist die Möglichkeit, weniger Informationen mit anderen auszutauschen und gleichzeitig weiterhin in vollem Umfang am gesellschaftlichen und wirtschaftlichen Leben teilzunehmen. Das ist ein potenziell radikaler Wandel. Bislang waren Entscheidungen betreffend die Privatsphäre immer «Trade-offs» zwischen der Offenlegung von Informationen über uns selbst und des Führens eines normalen Lebens. Um tauschen zu können, müssen wir Informationen teilen. Wenn wir einen Club betreten wollen, müssen wir unsere ID vorweisen. Wenn wir einen Kredit von einer Bank bekommen wollen, müssen wir unsere finanziellen Details offenlegen. Doch Technologien, die unsere Privatsphäre schützen, erlauben es uns, zu wesentlich tieferen Kosten (aufgrund der wegfallenden Nachteile der ungewollten Offenlegung von Informationen) zu tauschen.

Privatsphären-Technologien ermöglichen es, die Art und Weise neu zu denken, wie wir mit Firmen, Behörden und zivilgesellschaftlichen Einrichtungen interagieren. Im Moment bleibt uns oftmals keine andere Wahl, als unsere persönlichen Informationen preiszugeben, obwohl wir nicht wollen, dass diese Informationen in die Hände von spezifischen Personen gelangen. Banken wollen einerseits wissen, ob wir kreditwürdig sind, andererseits wollen wir nicht, dass die Bankmitarbeiter unsere individuellen Transaktionen einsehen können. Krankenversicherer müssen einerseits wissen, ob und weshalb wir schon einmal unter medizinischer Behandlung standen, andererseits wollen wir diese intimen Informationen nicht mit einem konkreten Angestellten dieser Versicherung teilen. Die Steuerbehörden wollen wissen, in welcher Steuerklasse wir uns bewegen, doch einem individuellen Steuerbeamten wollen wir nicht alle finanziellen Details wie etwa Herkunft der Einkommen oder von uns unterstützte Organisationen (zur Gewährung von Steuerabzügen) teilen. Die staatlichen Sozialversicherungen wollen wissen, ob uns IV-Gelder zustehen, doch wir wollen die Details unseres Leidens nicht mit den jeweiligen Mitarbeitern teilen.

Unsere aktuelle Weise des ökonomischen Handelns verlangt von uns allen, viele redundante Informationen gegenüber anderen offenzulegen. Die neuen Technologien der Freiheit ermöglichen es, dies künftig anders handhaben zu können. Es wird nun möglich, wesentlich weniger Informationen mit anderen zu teilen, ohne dass man sich hierfür vom wirtschaftlichen und gesellschaftlichen Leben zurückziehen müsste.

Bis heute musste man Informationen geheim halten, damit sie auch privat blieben. Doch die neuen Technologien erlauben es nun, Privatsphäre und Geheimhaltung voneinander zu trennen. Diese beiden Dinge sind nicht mehr länger Synonyme. Informationen vor dem unberechtigten Zugriff zu schützen, ist nicht das Gleiche, wie Informationen zu verheimlichen.

Privatsphäre ist ein wünschenswertes Gut, genauso wie es die Interaktion mit unserer Umwelt ist. Wenn wir tauschen, verlangen unsere Tauschpartner oftmals, dass wir gewisse Informationen über uns selbst offenlegen – unsere Kreditfähigkeit oder unsere medizinische Geschichte zum Beispiel –, weil das Risiko besteht, dass wir falsche Tatsachen vorspielen. In einem Umfeld, wo sich die Leute nicht vollständig gegenseitig vertrauen, ist die Privatsphäre schwierig aufrechtzuerhalten. Die neuen Privatsphären-Technologien geben Unternehmern und Entwicklern die Möglichkeit, eine vertrauenswürdige Privatsphäre zu schaffen.

Regulierung ist nicht die Lösung

Es ist ein Leichtes, im digitalen Zeitalter pessimistisch auf die Zukunft unserer Privatsphäre zu blicken. Viele öffentliche Kommentatoren haben bereits postuliert, dass die Privatsphäre tot sei und es sinnlos wäre, sich darüber zu beschweren, weil sie ohnehin nicht mehr zurückerobert werden könne. Man versucht uns weiszumachen, wir müssten uns nun einfach an diese neue Realität gewöhnen.

Versuche, die Privatsphäre durch staatliche Regulierungen zurückzuerobern, waren in der Tat meistens vergeblich. Ambitionierte Massnahmen wie etwa die Datenschutzgrundverordnung der Europäischen Union – ein Versuch, ein Recht auf persönlichen Datenschutz mit quasiweltweiter Wirkung zu konstruieren – brachte eine ganze Reihe unbeabsichtigter Konsequenzen und Probleme mit sich: extrem hohe Compliance-Kosten, eine Konsolidierung von Unternehmen (weil nur grosse Firmen dazu in der Lage sind, die enormen Compliance-Kosten zu tragen) und eine verringerte Innovation.[19] Wissenschaftler haben herausgefunden, dass sich die Privatsphäre der EU-Bürger unter einigen Umständen, in denen man nicht explizit von der Datenschutzgrundverordnung Gebrauch macht, sogar verschlechtert hat.[20] Und natürlich helfen uns staatliche Regulierungen auch nicht dabei, uns vor dem Überwachungsstaat selbst zu schützen.

Doch wie wir in diesem Beitrag gezeigt haben, erweist sich die Befürchtung, die Privatsphäre sei tot, als falsch. Die Geschichte der Privatsphäre gibt uns nicht nur einen Leitfaden und einen Grund, optimistisch zu sein, sondern sollte uns auch zu entsprechenden Innovationen inspirieren. Innovation in der Kommunikationstechnologie tendiert dazu, einem klaren Pfad zu folgen. Zunächst schaffen neue Technologien neue Risiken für die Privatsphäre.[21] Doch wenn diese für mehr und mehr kritische Anwendungen verwendet werden, bauen Innovatoren und Unternehmer Funktionen zum Schutz der Privatsphäre in diese neuen Technologien ein.

Die Geschichte des Telegrafen liefert uns ein prototypisches Beispiel für diese Dynamik. Ein elektrischer Telegraf sendet Stromimpulse durch einen Draht und ermöglicht die Kommunikation, indem er Informationen mithilfe der Impulse und der dazwischen liegenden Stille überliefert. Die standardisierte Verschlüsselung war der Morsecode, welcher menschliche Sprache in eine Serie von Punkten und Strichen konvertierte. Der wirtschaftlichen Bedeutung der Verbreitung des Telegrafen kann kaum zu hohe Bedeutung beigemessen werden. Genauso wie die Verbreitung der Eisenbahn dem Güterhandel einen grossen Schub verlieh, war der Telegraf die Grundlage für die Informationsökonomie.[22] Es kommt nicht von ungefähr, dass der Autor Tom Standage den Telegrafen als das «viktorianische Internet» bezeichnet hatte.[23]

Doch trotz seiner Möglichkeiten war der Telegraf alles andere als sicher. Das Abfangen von Nachrichten war extrem einfach. Dies konnte mit simplem Equipment bewerkstelligt werden. Die Nachfrage nach Telegrafenämtern und entsprechenden

[19] Siehe dazu: Adam Thierer (25. April 2018). How Well-Intentioned Privacy Regulation Could Boost Market Power of Facebook & Google. The Technology Liberation Front; Adam Thierer (9. Juli 2018). GDRP Compliance: The Price of Privacy Protections. The Technology Liberation Front. Darcy W. E. Allen et al. (2019). Some Economic Consequences of the GDPR. Economics Bulletin 39 (2):
S. 785-797.
[20] Guy Aridor et al. (2020). The Economic Consequences of Data Privacy Regulation: Empirical Evidence from GDPR. SSRN 3522845.
[21] Siehe für eine ausführliche Diskussion hierzu: Chris Berg. The Classical Liberal Case for Privacy in a World of Surveillance and Technological Change.
[22] Richard B. DuBoff (1980). Business Demand and the Development of the Telegraph in the United States, 1844–1860. Business History Review 54 (4): S. 459–479.
[23] Tom Standage (1998). The Victorian Internet. New York: Bloomsbury Publishin.

Angestellten, welche die Kommunikation managten, führte dazu, dass man lediglich einen Angestellten zu bestechen brauchte, um die Kommunikation anderer Leute abzufangen und zu überwachen. Diese Schwäche bedeutete, dass das wirtschaftliche Potenzial des Telegrafen limitiert war: Firmen, die vertrauenswürdige Informationen übermitteln wollten, konnten sich nicht sicher sein, dass ihre Daten nicht von der Konkurrenz abgefangen wurden.

Genau dieses Problem führte zur Entwicklung der Kryptografie. Wie David Kahn schreibt, «machte der Telegraf die Kryptografie zu dem, was sie heute ist».[24] Natürlich war die Idee, Nachrichten zu verschlüsseln, damit nur der intendierte Adressat diese lesen konnte, nicht neu. Substitutions-Chiffren, bei denen Buchstaben gegen andere Buchstaben ausgetauscht werden, reichen bis weit in die Antike zurück, und die berühmteste davon ist die «Caesar-Chiffre». Doch mit dem Telegrafen kam ein plötzlicher und konzentrierter Effort, die Techniken der privaten Kommunikation zu erneuern. Wie Kahn schreibt, gab es in den 1800er-Jahren eine Vielzahl von professionellen und Amateur-Chiffrieren:

> *«Das grosse und verbreitete Bedürfnis nach Geheimhaltung weckte das latente Interesse an Chiffren. Dutzende von Personen versuchten, ihre eigenen unknackbaren Chiffren zu entwickeln ... Überraschend viele dieser Tüftler waren intellektuelle und politische Führungspersönlichkeiten der damaligen Zeit, die ihre einflussreichen und originellen Köpfe dem fesselnden Gebiet der Kryptologie widmeten. Ihre Beiträge bereicherten die Kryptologie mit Dutzenden von neuen Chiffriersystemen.»*[25]

Der moderne Bereich der Kryptografie geht also sowohl auf die Entdeckung einer wichtigen wirtschaftlichen Innovation – den Telegrafen – zurück als auch auf die Feststellung, dass der Telegraf nicht dazu in der Lage war, eine sichere Kommunikation zu ermöglichen, die nötig war, um sein volles wirtschaftliches Potenzial zu entfalten.

Der Markt richtet es

Nachfolgende Kommunikations-Revolutionen weisen ähnliche Verläufe auf. Als das Telefon in den ersten Jahrzehnten des 20. Jahrhunderts eingeführt wurde, haben Telefonzentralen Anrufer und Angerufene zusammengeführt. Obwohl es ihnen nicht gestattet war, mitzuhören, war es für sie ein Leichtes, dies zu tun – eine weitere Konstante in der Geschichte. Automatische Telefonzentralen sorgten für einen Fortschritt in der Privatsphäre der Kommunikation.

Ebenso erlaubte die Verbreitung von Gruppenleitungen – Telefonleitungen, die von Gruppen von Teilnehmern gemeinsam benutzt wurden – den Nachbarn, Gespräche nach eigenem Gutdünken abzuhören. Einer der Haupttreiber für die Nachfrage nach privaten Telefonlinien war die Möglichkeit, medizinischen Rat über das Telefon

[24] David Kahn (1996). The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet. New York: Sribner's and Sons. S. 189.
[25] Ebd.

einzuholen, insbesondere in ländlichen Gebieten. Diese sensiblen Angelegenheiten wollte man natürlich nicht mit den Nachbarn teilen.

Bei der digitalen Kommunikation scheinen sich diese Muster nun zu wiederholen. Die frühe E-Mail-Kommunikation tendierte zur Nutzung gemeinsamer Terminals (die auch für Kollegen einsehbar waren) und offener Diskussionslisten. Über die Zeit setzten sich vom Nutzer kontrollierte, personalisierte und passwortgeschützte E-Mail-Konten durch, die der zunehmend an Bedeutung gewinnen-den Online-Kommunikation mehr Privatsphäre hinzufügten. In den 1970er- und 80er-Jahren begann man damit, durchgängig verschlüsselte E-Mailsysteme zu entwickeln. Doch bis heute haben vollprivate E-Mail-Anbieter nie einen signifikanten Marktanteil erlangen können. Während ein individueller Nutzer zwar seine Nachrichten hinter einem Passwort und eine PIN verstecken kann, ist es typischerweise so, dass Angestellte und E-Mail-Anbieter einen relativ freien Zugang zu diesen Informationen haben (auch wenn dieser Zugang manchmal durch das Gesetz oder die Praxis limitiert ist). Erst in den letzten Jahren kam es zu einem signifikanten Schub an Privatsphäre in der digitalen Kommunikation. Das Aufkommen von Smartphones in den 2010er-Jahren führte zu einer grossen Verbreitung von Instant-Messaging- und Chat-Dienstleistungen, die sich mit der Zeit an der Marktnachfrage nach einem besseren Schutz der Privatsphäre ausrichteten.

In diesem Sinne lehrt uns die Geschichte und Evolution der Privatsphäre eine wichtige Lektion für die Geschichte der Freiheit im Allgemeinen: Erfolge bei der Sicherung oder Rückeroberung der Privatsphäre wurden nicht durch staatliche Regulierungen oder vor Gerichten erzielt. Während die meisten Advokaten der Privatsphäre sich auf Politik und Gesetze fokussieren, sollten wir unsere Aufmerksamkeit vielmehr Innovationen schenken, die einen verbesserten Schutz der Privatsphäre mit sich bringen. Diese Innovationen kommen von kreativen Unternehmern, die auf die Marktnachfrage reagieren (z. B. die Nachfrage von Patienten, mit ihren Ärzten via Telefon zu kommunizieren, oder die Nachfrage von Unternehmen, Informationen zu teilen, ohne dass diese von Konkurrenten aufgeschnappt werden). Sie werden aber auch von unabhängigen Tüftlern vorangetrieben, die den Konsumenten etwas anbieten, wovon diese zuvor noch gar nicht gewusst haben, dass sie es wollen.

Die Aufgabe von freiheitsorientierten Unternehmern und Innovatoren ist es also nicht nur, die Menschen davon zu überzeugen, dass Privatsphäre ein wichtiges und schützenswertes Gut ist, sondern auch die entsprechenden Tools zu entwickeln und zur Verfügung zu stellen, um diese aufrechtzuerhalten.

LIBERALES INSTITUT

Impressum

Liberales Institut
Hochstrasse 38
8044 Zürich, Schweiz
Tel.: +41 (0)44 364 16 66
institut@libinst.ch

Bei diesem Beitrag handelt es sich um einen Auszug aus dem Buch *Liberalismus 2.0: Wie neue Technologien der Freiheit Auftrieb verleihen* von Olivier Kessler (Hrsg.), 2021, Edition Liberales Institut.

Alle Publikationen des Liberalen Instituts finden Sie auf www.libinst.ch.

Disclaimer