Zeitschrift: Schweizer Monat : die Autorenzeitschrift für Politik, Wirtschaft und Kultur

Band: 102 (2022)

Heft: 1093

Artikel: Wovon selbst Diktatoren nur träumen können

Autor: Berthélémy, Chloé

DOI: https://doi.org/10.5169/seals-1035431

Wovon selbst Diktatoren nur träumen können

Die Europäische Union ermuntert Tech-Unternehmen, Straftaten für sie aufzudecken. Das öffnet Tür und Tor für autoritäre Kontrollwut.

von Chloé Berthélémy

Technologisch gesehen ist die moderne Verschlüsselung heute bereits Norm: Alle unserer beliebtesten Websites sind durch HTTPS geschützt. Wir unterhalten uns mit unseren Liebsten über WhatsApp und chatten mit unseren Freunden über Signal – beide Applikationen sind «Ende-zu-Ende» verschlüsselt. Wir wickeln Zahlungen für neue Kleidung, Möbel oder Lebensmittel bequem und sicher online ab. Menschen, Unternehmen und Regierungen verlassen sich heute überall auf die Verschlüsselungstechnologie, um ihre Privatsphäre, Daten und Ressourcen zu schützen.

Die europäischen Regierungen haben sich in der Vergangenheit schwergetan, eine einheitliche Position zur technischen und praktischen Realität von Verschlüsselungsmethoden zu finden. Während die Europäische Kommission in ihrem Bericht zur Sicherheitsunion 2017 einräumte, dass Verschlüsselung für die Gewährleistung der Cybersicherheit und des Schutzes personenbezogener Daten «von wesentlicher Bedeutung» sei, beschrieb sie die Verschlüsselungstechnologie im gleichen Dokument auch als eine grosse Bedrohung für die Aufdeckung, Untersuchung und Verfolgung von Straftaten.[1] Im Anschluss an terroristische Angriffe oder Akte organisierter und schwerer Kriminalität haben Regierungen die Europäische Kommission wiederholt dazu gedrängt, eine EU-weite Lösung für eine mögliche Umgehung der Verschlüsselung zu schaffen: Nach den Terroranschlägen von 2015 und 2016 beispielsweise forderten der französische und der deutsche Innenminister bei einem Treffen in Paris eine Gesetzgebung, die Unternehmen zur Schwächung ihrer Verschlüsselungsstandards zwingen wollte, um so Nachrichten von «islamistischen Extremisten» abzufangen.[2] Ein gleichermassen hoher Druck kommt von Seiten der Polizeibehörden: Sie behaupten, eine «starke Verschlüsselung» zwar zu unterstützen, wenden sich aber gegen eine «unregulierte Verschlüsselung» – ohne näher auf diesen scheinbaren Widerspruch einzugehen oder zu spezifizieren, ab welchem Punkt Verschlüsselung nun ein Verbrechen erleichtert oder strafrechtliche Ermittlungen erschwert.[3]

Das unlösbare Problem

Inmitten dieser Unschärfe des politischen Willens steht die Europäische Kommission vor einem scheinbar unlösbaren Problem: Schenkt sie den Forderungen Gehör und erzwingt eine Aushöhlung nur schon einer Komponente der Verschlüsselung, so würde sie gleich das Funktionieren ganzer digitaler Systeme gefährden. Wenn Regierungen die Einführung von bewussten Schwachstellen anordnen – sei es im Verschlüsselungsalgorithmus, in der Verwaltung von «Private Keys» oder anderen Komponenten –, setzen sie die Sicherheit aller Nutzer aufs Spiel, und das nicht nur in der Europäischen Union, sondern weltweit. Die Kommission würde mit ihrem Vorgehen einen unrechtmässigen Zugang durch böswillige Akteure ermöglichen, da diese die erwünschten Sicherheitslücken ebenfalls ausnutzen können. Damit steht die Agenda auch im Widerspruch zu den eigenen Datenschutz- und Privatsphärestandards der EU.

Nichtsdestotrotz hat die Kommission in der jüngeren Vergangenheit versucht, mit Hilfe der Mitgliedstaaten «rechtliche und technische Massnahmen» zu finden, um den Zugang zu verschlüsselten Daten «mit minimalen Auswirkungen auf die Grundrechte» freizumachen – sie will also das Unmögliche möglich machen.[4] Für die Polizeibehörden wurden Ressourcen freigemacht, insbesondere mit der Finanzierung einer Entschlüsselungsplattform von Europol, der EU-Agentur für polizeiliche Zusammenarbeit. Intensiviert hat sich die Debatte seit 2019, als Facebook (jetzt Meta) ankündigte, bald eine Ende-zu-Ende-Verschlüsselung für sämtliche seiner Instant-Messaging-Dienste einzuführen. Die Ankündigung alarmierte Strafverfolgungs- und Kinderschutzorganisationen: Sie befürchteten, dass durch den zusätzlichen Verschlüsselungsschutz eine beträchtliche Anzahl von Fällen sexuellen Kindesmissbrauchs nicht mehr auffindbar sein würde. Auf Druck hin erklärte Facebook schliesslich, die Einführung zusätzlicher Verschlüsselung bis 2023 hinauszögern zu wollen.

Big Tech in der Pflicht

Der Kampf gegen sexuellen Kindesmissbrauch ist seither zum Hauptantrieb der Debatte über Verschlüsselung in Europa geworden. Mittlerweile werden sogar Lösungen jenseits der traditionellen «Hintertüren» für Dritte, also

«Sobald das Argument zugunsten des Kinderschutzes gewonnen ist, werden Politiker mit Leichtigkeit argumentieren, dass damit auch zum Beispiel Terrorismus ausgemerzt werden solle.»

Chloé Berthélémy

Chloé Berthélémy, zvg.

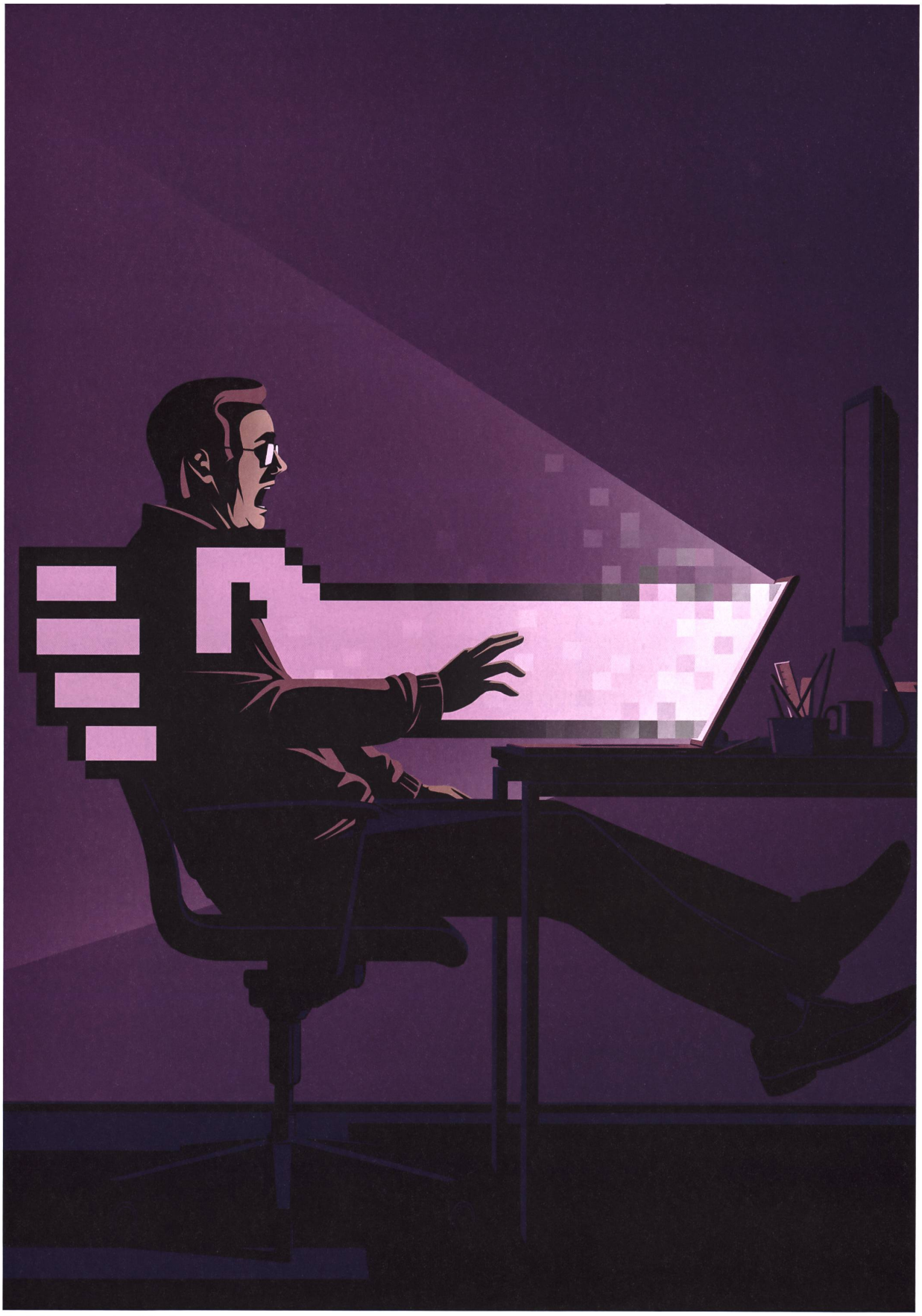

Illustration von Stephan Schmitz.

jenseits eines Umgehens der Verschlüsselung und des erlaubten Zugangs zu einem von Technologieunternehmen gehosteten System, vorangetrieben. Im Jahr 2020 veröffentlichte die Europäische Kommission ihre Strategie für eine wirksamere Bekämpfung des sexuellen Missbrauchs von Kindern – sie argumentierte darin, dass die Anwendung von Verschlüsselung die Identifizierung von Tätern erschwere, wenn nicht gar verunmögliche. Sie kündigte sodann die Einführung eines gemeinsamen Expertenprozesses mit der Tech-Industrie an: Unternehmen sollen technische Lösungen entwickeln, die ihnen eine Detektion von Beweismaterial des sexuellen Kindesmissbrauchs auf ihren Ende-zu-Ende-verschlüsselten Plattformen erlauben. Die Unternehmen sollen das entsprechende Material dann der zuständigen Strafbehörde übermitteln. Diese neue Ausrichtung hin zu einem Auftrag zur Selbstregulierung durch private Anbieter wurde einige Monate später in einer Resolution von den EU-Ministern bestätigt.

2021 richteten die EU-Politiker erneut ihr Augenmerk auf die Scan- und Filterkapazitäten der Technologieunternehmen: Sie erkannten, dass die geplante Aktualisierung der EU-Datenschutzvorschriften den Tech-Anbietern verboten hätte, die private Kommunikation ihrer Nutzer auszuspionieren. Rasch verabschiedete die EU eine Interimsgesetzgebung, die den Unternehmen ein Weiterführen ihrer freiwilligen Filterpraktiken ermöglichte. Nun soll die Übergangslösung durch eine ständige Rechtsvorschrift abgelöst werden – und das bis anhin freiwillige Scannen privater Kommunikation durch den Anbieter zu einer Verpflichtung geformt werden. Im Sommer 2021 kündigte Apple seine Unterstützung im Kampf gegen den sexuellen Kindesmissbrauch an: Alle Bilder, die von Kinderkonten verschickt werden, und sämtliche Fotos, die User auf den iCloud-Dienst hochladen, sollen durch das Unternehmen überprüft werden. Auch wenn sich Apple nach einem öffentlichen Aufschrei der Zivilgesellschaft gezwungen sah, seine Pläne vorerst aufzuschieben, hat die Bereiterklärung des Big-Tech-Anbieters den Gesetzgebern gezeigt, dass Kontrolle durch die Macht eines privaten Unternehmens möglich ist.

Verhängnisvolle Auswirkungen auf die Freiheit

Beim sogenannten «Client-Side-Scanning» (CSS), einer der wichtigsten Filterlösungen, bei welcher die Inhaltsüberprüfung direkt auf dem Gerät des Nutzers stattfindet, sei gemäss der Europäischen Kommission eine «Achtung der Privatsphäre» gewährleistet. Tatsächlich birgt das CSS jedoch ernsthafte Risiken: Erstens torpediert es ein Grundprinzip der Ende-zu-Ende-Verschlüsselung, wonach nur der Absender und der Empfänger in der Lage sind, die jeweiligen Daten auszulesen. Da das Tool persönliche Geräte vollends durchsuchbar machen kann, beeinträchtigt es die Privatsphäre und Sicherheit aller – nicht zuletzt auch jene von Kindern. Die massenhafte Durchsuchung privater Daten ohne richterliche Anordnung oder individuellen Verdacht verstösst zudem mit grosser Wahrscheinlichkeit gegen bestehendes EU-Recht, da ein solcher Eingriff in die Privatsphäre unverhältnismässig ist und andere Freiheiten durch die Überwachung beeinträchtigt werden.

Zweitens wird mit der Filterlösung die Versuchung gross, die Technologie auch auf andere Arten von Inhalten auszuweiten: Sobald das Argument zugunsten des Kinderschutzes gewonnen ist, werden Politiker mit Leichtigkeit argumentieren, dass damit auch zum Beispiel Terrorismus ausgemerzt werden solle. Terroristische Äusserungen sind jedoch oft mit rechtlichen Unklarheiten verbunden, die ein automatisches Scanning-System unmöglich erfassen kann: Ungerechtfertigte Löschungen und missbräuchliche Zensur, vergleichbar mit den heutigen Moderationswerkzeugen in den sozialen Medien[5], wären dann an der Tagesordnung. Der Eingriff in die Grundrechte wird sich nur noch verstärken, wenn die Filterlösung die Kommunikation von Journalisten und Menschenrechtsverteidigern abfängt – insbesondere wenn die obligatorische Erkennung illegaler Inhalte mit einer Meldepflicht an die Behörden einhergeht. Ist das System erst einmal eingeführt, wird es für autoritäre Regierungen inner- und ausserhalb der EU ein gefundenes Fressen sein. Wie jedes andere technische Hilfsmittel kann es jederzeit missbraucht werden, falls es in böswillige Hände fällt. Betroffene Nutzer und die Zivilgesellschaft sollten sich dringend an dieser Diskussion beteiligen – bevor es zu spät ist. ‹

Aus dem Englischen übersetzt von Jannik Belser. Der Artikel ist auf schweizermonat.ch in der Originalsprache verfügbar.

[1] www.eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52017DC0608&from=EN
[2] www.edri.org/our-work/france-germany-fighting-terrorism-by-weakening-encryption/
[3] www.politico.eu/article/the-last-refuge-of-the-criminal-encrypted-smartphones-data-privacy/
[4] www.statewatch.org/media/1352/eu-council-security-despite-encryption-10728-20.pdf
[5] www.hrw.org/report/2020/09/10/video-unavailable/social-media-platforms-remove-evidence-war-crimes

Chloé Berthélémy
ist Policy Advisor bei European Digital Rights (EDRi), einer in Brüssel stationierten Vereinigung von europäischen Zivilorganisationen.