

EDRi: Beschämende Kriminalisierung von Menschen, die ihre Daten schützen, in Frankreich

Die Verschlüsselung von Kommunikation ist eine gängige Praxis, um sicherzustellen, dass die eigene Korrespondenz nur von den Empfänger:innen und nicht von Dritten gelesen wird. Das Recht auf Verschlüsselung ist eine Erweiterung unseres Rechts auf Privatleben, festgeschrieben in Artikel 8 der Europäischen Menschenrechtskonvention, die jeder und jedem einzelnen von uns „Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs“ verleiht.

Jeder, der seine Nachrichten schützen möchte, kann verschlüsselte Korrespondenz nutzen – Aktivist:innen, Menschenrechtskämpfer:innen, Aufdeckungsjournalist:innen, jungen Menschen, Bürokraten, Eltern, Freunde und Sie selbst – alle verwenden Dienste wie WhatsApp und Signal, in deren Messengern sichere Verschlüsselung integriert ist.

Im Laufe der Geschichte haben Menschen auf der ganzen Welt Verschlüsselung genutzt, um Korruption aufzudecken, sich zu organisieren und Unterdrückerregimes zu bekämpfen, gesellschaftliche Veränderungen zu bewirken und unsere Welt zu einem Raum für alle zu machen. Mit Stand 2022 nützen über zwei Milliarden Menschen auf der ganzen Welt Verschlüsselung. Der Grund ist einfach: Privatsphäre stärkt uns alle.

Jetzt jedoch greifen Strafverfolgungsbehörden und Gesetzgeber in Frankreich, der EU, dem Vereinigten Königreich und den Vereinigten Staaten die Ende-zu-Ende-Verschlüsselung an. Wir als Gesellschaft stehen vor der Entscheidung: Akzeptieren wir eine Zukunft, in der unsere privaten Nachrichten und unsere Kommunikation jederzeit mitgelesen werden können und wir unter Generalverdacht gestellt werden?

Eine französische Tragikomödie: vertraulich, daher verborgen, daher terroristisch?

Die französische Nichtregierungsorganisation La Quadrature du Net hat kürzlich Informationen zum sogenannten „Fall 8. Dezember“ enthüllt, bei dem gegen sieben „ultra-linke“ Personen wegen Bildung einer „terroristisch kriminellen Vereinigung“ ermittelt wird. Der Fall zeigt einen nie zuvor dagewesenen Willen der Polizei, den Einsatz digitaler Technologien durch strafrechtlich verfolgte Personen zu kriminalisieren.

Die veröffentlichten Unterlagen zeigen, dass die französischen Strafverfolgungsbehörden vollkommen rechtmäßige und verantwortungsvolle digitale Sicherheitsvorkehrungen wie die Verwendung von Verschlüsselung kriminalisieren. In der Vergangenheit wurde sichere Verschlüsselung von zahlreichen Institutionen wie den Vereinten Nationen, der CNIL (französische Datenschutzbehörde), der ANSSI (französische Cybersicherheitsbehörde), der EU-Agentur ENISA und auch der EU-Kommission empfohlen und unterstützt.

Neben der Kriminalisierung von verschlüsselten Instant-Messengern gehen die französischen Strafverfolgungsbehörden auch gegen die Verwendung von Diensten wie Proton Mail, die die Vertraulichkeit von Email gewährleistet, den Einsatz von Tools zum Schutz der Privatsphäre im Internet (VPN, Tor, Tails), die Verwendung von Techniken zum Schutz vor Überwachung durch die großen Internetkonzerne (GAFAM), die Verschlüsselung von digitalen Medien und sogar gegen Veranstaltungen, bei denen digitale Schutzmaßnahmen gelernt werden können (Kryptopartys), vor.

Kriminalisierung des Rechts auf Privatsphäre

Durch die Kriminalisierung von Verschlüsselung und anderen Schutzmaßnahmen versucht die französische Polizei eine Erzählung zu schaffen, die zeigen soll, dass die sieben verfolgten Personen „im Untergrund“ lebten. In Ermangelung eines nachweisbaren terroristischen Plans wird dieses „Leben im Untergrund“ zum Beweis der versteckten Existenz eines unbeweisbaren Plans.

Wir, Journalist:innen, Aktivist:innen, Tech-Diensteanbieter und gewöhnliche Bürger:innen, denen Datenschutz im digitalen Zeitalter wichtig ist, sind zutiefst empört darüber, wie französische Geheimdienste und die Anti-Terror-Justiz eine solche Vermischung von grundlegendem Datenschutz und Terrorismus fördern wollen.

Wir sind entrüstet, dass notwendige Maßnahmen zum Schutz persönlicher Daten und der Privatsphäre als Hinweise auf „verschwörerische Handlungen“ von Menschen, die angeblich in einem „Kult des Geheimnisses“ leben, angesehen werden. Wir verurteilen es, dass eine gewöhnliche und gutartige Ausbildung in der Nutzung von Tails – einem für die breite Öffentlichkeit zugänglichen Betriebssystem, das für den Schutz der Privatsphäre und den Kampf gegen Zensur konzipiert wurde – eine der „wesentlichen Tatsachen“ sein kann, die für eine „Teilnahme an einer Gruppe, die mit der Absicht gebildet wurde [...] terroristische Handlungen vorzubereiten“ spricht.

Aushöhlung von Verschlüsselung über Frankreich hinaus

Unter dem Vorwand des Terrorismus kriminalisiert die französische Justiz grundlegende Sicherheitsvorkehrungen. Aber das französische Beispiel ist nicht die einzige Bestrebung, Verschlüsselung zu unterminieren.

In Brüssel hat die EU-Kommission im Jahr 2022 ihren Vorschlag für eine Verordnung zur Bekämpfung von Kindesmissbrauch (Chatkontrolle) vorgelegt. Unter dem Vorwand der Bekämpfung von Kinderpornographie soll dieser Gesetzesentwurf Anbieter von verschlüsselten Nachrichtendiensten zwingen, unsere verschlüsselten Nachrichten zu scannen. Der Vorschlag wurde von vielen Seiten kritisiert, darunter von mehr als 130 Nichtregierungsorganisationen, insbesondere für seine mangelnde Einbeziehung von anderen Mitteln zur Bekämpfung dieses schrecklichen Verbrechens, die besser geeignet sind und unsere Rechte weniger einschränken. Kürzlich ist durchgesickert, dass Länder wie Spanien Ende-zu-Ende-Verschlüsselung überhaupt verbieten wollen. Gesetzesvorhaben wie die britische „Online Safety Bill“ und der „EARN IT Act“ in den USA zählen ebenfalls zu diesem besorgniserregenden Krieg gegen Verschlüsselung.

Während wir selbst tagtäglich Datenschutztools in der Forschung, zum Quellenschutz, für politische Beteiligung oder einfach zum Schutz unserer privaten Kommunikation mit unseren Familienmitgliedern und Freund:innen nutzen, sind wir äußerst besorgt über diese Versuche, weitverbreitete und nutzenstiftende Praktiken zu kriminalisieren.

Als Unterstützer und Verteidiger von Grundrechten in der digitalen Welt werden La Quadrature du Net und seine Verbündeten weiterhin Werkzeuge zum Schutz der Privatsphäre nutzen und herstellen. Wir lassen nicht zu, dass Geheimdienste, Gerichte oder die Polizei unsere Aktivitäten kriminalisieren, weil sie sie für „verdächtig“ halten. Unsere Vision ist der Schaffung eines freien, dezentralisierten und ermächtigenden Internets, das eine würdevollere Gesellschaft für alle ermöglicht. Der Kampf für Verschlüsselung ist der Kampf für eine gerechte und faire Zukunft.