REGARDS

THEMA

CHATKONTROLLE

Europäische Massen-überwachung

Joël Adami

Mit der „Chatkontrolle“ plant die EU-Kommission die Einführung einer europaweiten Massenüberwachung. Datenschützer*innen schlagen Alarm.

Ist „Zensursula“ zurück? Diesen Spitznamen gaben Netzaktivist*innen 2009 der damaligen deutschen Familienministerin Ursula von der Leyen. Die heutige Präsidentin der Europäischen Kommission machte sich damals für Netzsperren stark. Nun will die Kommission sämtliche Privatnachrichten, Chats und verschickte Bilder überwachen. Vorgeblicher Grund ist heute wie damals der Kampf gegen sogenannte „Kinderpornografie“. Die Kritik an der geplanten Chatkontrolle ist laut - sie würde eine umfassende Massenüberwachung einführen.

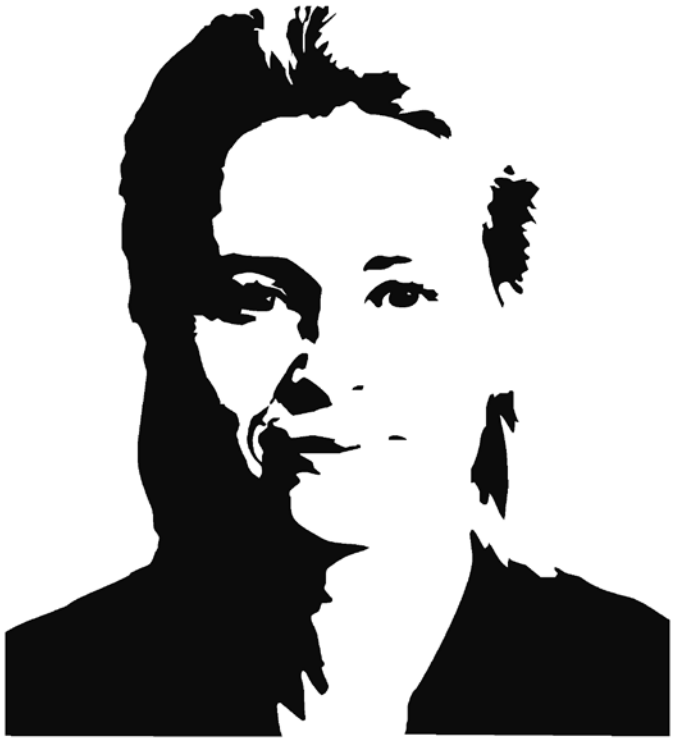
Bisher ist es „nur“ ein gemeinsamer Gesetzesvorschlag von Kommission und Rat, der also noch durch das Europäische Parlament muss. Über 130 Seiten umfasst der Entwurf, der dennoch viele technische Details ausspart und somit den wildesten Überwachungsfantasien Tür und Tor öffnet. Kein Wunder also, dass viele Netzaktivist*innen sich jetzt gegen die geplanten Überwachungsmaßnahmen stemmen.

Um gegen Kindesmissbrauch vorzugehen, sollen Handys, Laptops und Kommunikationsinhalte insgesamt automatisch durchsucht werden können. Laut der Kommission soll das „auf Basis von Anordnungen“ passieren, wenn Behörden feststellen, dass ein „erhebliches Risiko“ besteht, dass Material über sexuellen Kindesmissbrauch über einen Dienst verschickt wird. Auch das sogenannte „Grooming“, also die sexuelle Kontaktanbahnung von Erwachsenen bei Kindern oder Jugendlichen, sollen die Anbieter automatisiert erkennen und unterbinden.

Das geht jedoch nicht, ohne dass eine Infrastruktur für die massenhafte Überwachung eingeführt wird. Auch die Ende-zu-Ende-Verschlüsselung von Chatnachrichten würde ausgehebelt werden. Ende-zu-Ende bedeutet: Die Nachricht wird am Gerät des*der Sender*in verschlüsselt, als „Buchstabensalat“ durch das Internet geschickt und erst am Gerät des*der Empfänger*in wieder entschlüsselt. Ein Einblick in die Inhalte ist ohne Aushebelung dieser entscheidenden Sicherheitstechnik überhaupt nicht möglich. Grundsätzlich gibt es zwei Optionen: Aufbruch der Verschlüsselung oder vorheriges Scannen.

Scan oder Zweitschlüssel

Wenn die Anbieter bereits gesendete Nachrichten mitlesen sollen, dann müssen diese unverschlüsselt sein oder die Anbieter einen „Zweitschlüssel“ haben. Eine solche Sollbruchstelle in der Verschlüsselung würde auch Geheimdiensten und Hacker*innen einen Zugang zu privaten Nachrichten verschaffen. Das sogenannte „Client-Side-Scanning“ (CSS) würde bedeuten, dass Nachrichten oder Bilder vor dem Verschlüsseln auf dem Gerät selbst gescannt werden. So würde lediglich verdächtiges Material an Behörden weitergeleitet. Apple arbeitete bereits an der entsprechenden Technik, verschob dies jedoch nach massiven Protesten auf unbestimmte Zeit. Bereits im Oktober 2021 erschien eine Studie führender



CC-BY-SA_JABB

Als Ursula von der Leyen 2009 als deutsche Familienministerin geheime Internetsperren einführen wollte, wurde sie als „Zensursula“ bezeichnet. Auch damals war die Motivation angeblich, gegen Kindesmissbrauch vorzugehen.

FOTO: CC-BY HOWTOSTARTABLOGONLINE.NET

Kommt die Chatkontrolle, geht das Grundvertrauen in die eigenen Geräte verloren, fürchten Datenschützer*innen.

Sicherheitsforscher*innen, die massive Kritik an CSS übten.

Sie halten die Tatsache, dass Nachrichten auf dem Gerät der Nutzer*innen gescannt werden, für ein erhebliches Sicherheitrisiko. „Da die meisten Benutzergeräte Schwachstellen aufweisen, können die Überwachungs- und Kontrollmöglichkeiten von CSS von vielen Gegnern missbraucht werden, von feindlichen staatlichen Akteuren über Kriminelle bis hin zu den Intimpartnern der Benutzer“, heißt es in der Studie. Die Einführung von CSS würde es potenziell nicht nur ermöglichen, Chatnachrichten zu durchsuchen, sondern auch jede andere Datei auf einem Handy, Laptop oder Tablet. Die Geräte würden noch viel mehr zu Wanzen, ihre Nutzer*innen transparent für staatliche Behörden - und für alle, die genug kriminelle Energie haben, diese Schwachstellen auszunutzen.

Hinzu kommt ein weiteres Problem: Automatisierte Erkennung von Kindesmissbrauch oder Grooming ist nicht fehlerfrei. Wie bei jeder Anwendung sogenannter künstlicher Intelligenz ist oft nicht transparent nachvollziehbar, warum ein Programm zu einer bestimmten Entscheidung gekommen ist. Bei einer massenhaften Überwachung aller Kommunikation innerhalb der EU würde es selbst bei einer kleinen Fehlerquote zu einer regelrechten Flut an Verdachtsfällen kommen, die sich dann im Endeffekt als unzutreffend herausstellen. Im Endeffekt wären die Behörden dann sehr damit beschäftigt, private Familienchats zu lesen - ohne dass dadurch notwendigerweise mehr Verbrecher*innen gefasst würden. Die Nutzer*innen müssten jedoch ständig befürchten, dass ihre ganz legal verschickten Fotos oder Flirt-Chats bei Behörden landen. Der österreichische Journalist Erich Moechel betonte in seiner Analyse des Kommissionsvorschlages für den Sender FM4, dass für die automatisierte Erkennung erst einmal große Mengen an Chats und anderer Kommunikation gespeichert werden müssen - ohne dass dies explizit im Kommissionsentwurf stünde.

Wer sind überhaupt die Täter*innen?

Es stellt sich überhaupt die Frage, wer mit einer Chatkontrolle überführt werden könnte. Laut dem Cyberkriminologen Thomas-Gabriel Rüdiger sind in Deutschland beispielsweise 54 Prozent der Tatverdächtigen bei der Verbreitung sogenannten „kinderpornografischen Materials“ minderjährig. Das sagte der Polizist gegenüber Netzpolitik.org. Diese Tatsache kommt laut Rüdiger daher, dass Jugendliche sich gegenseitig Nacktfotos schicken, diese aber auch in Chatgruppen geteilt werden. Die Jugendlichen seien sich meist nicht bewusst, dass sie damit eine Straftat begehen würden, weshalb die Ermittlungen gegen sie leicht seien. Pädokriminelle Erwachsene würden bei Einführung einer Chatkontrolle schnell auf andere Methoden umsteigen, schätzt der Kriminologe, der für mehr Medienkompetenz bei Kindern und Jugendlichen plädiert.

In Luxemburg kümmert sich Bee Secure sowohl um die Stopline, bei der illegale Inhalte gemeldet werden können, als auch um die Vermittlung digitaler Kompetenzen für Kinder und Jugendliche. Im Vorjahr wurden 2.562 Seiten bei der Stopline im Zusammenhang mit sexuellem Missbrauch Minderjähriger gemeldet, 1.388 - also 54 Prozent - erwiesen sich als illegal. In den pädagogischen Materialien von Bee Secure werden Jugendliche darauf hingewiesen, dass sie illegales, „kinderpornografisches“ Material erzeugen, wenn sie Nacktfotos von sich selbst machen.

Die Kritik an der geplanten Chatkontrolle ist groß. European Digital Rights (Edri), ein Netzwerk aus über 45 europäischen NGOs, wehrt sich gegen den Vorschlag der EU-Kommission. In einem Positionspapier, das bereits im Februar veröffentlicht wurde, stellte das Netzwerk klar: „Die automatische Durchsuchung der privaten Kommunikation eines jeden Menschen zu jeder Zeit stellt einen unverhältnismäßigen Eingriff in den Kern des Grundrechts auf Privatsphäre dar. Sie kann eine Form der undemokratischen Massenüberwachung darstellen und schwerwiegende und ungerechtfertigte Auswirkungen auch auf viele andere Grundrechte und Freiheiten haben.“

Inkompatibel mit europäischen Werten

Die Befürchtung liegt nahe, dass der Kampf gegen Darstellungen sexuellen Missbrauchs an Minderjährigen als Vorwand genutzt wird, um eine Plattform für Massenüberwachung einzuführen. Die könnte dann nach und nach auf andere Bereiche ausgeweitet werden, zum Beispiel auf Terrorismus oder organisierte Kriminalität. Dann wäre der Schritt, auf den totalüberwachten Geräten nach möglichen Urheberrechtsverletzungen zu suchen, auch nicht mehr weit hergeholt.

Das befürchtet auch der Chaos Computer Club Lëtzebuerg (C3L). Es sei klar, dass „so ein intransparentes System in der Zukunft erweitert“ würde, schrieb die Organisation am Montag in einer Pressemitteilung zur EU-Chatkontrolle. Nicht nur Journalist*innen und Whistleblower*innen seien auf vertrauenswürdige Kommunikation angewiesen, sondern alle.

„Dies ist ein massiver Einschnitt in die Privatsphäre der Nutzer, weil sie die Kontrolle darüber verlieren, welche Daten sie mit wem teilen. Eine vertrauliche Nachricht, ein Foto des letzten Kindergeburtstags oder ein Video der Großmutter an ihre Enkel. All das kann und wird gescannt werden müssen sowie von einem Dritten kontrolliert werden. Das Grundvertrauen in die eigenen Geräte ist damit zerstört!“, schrieb der C3L weiter. Auch der deutsche Datenschutzbeauftragte des Bundes, Ulrich Kelber, schloss sich der Kritik an. Auf Twitter schrieb er: „Der Entwurf der Kommission ist nicht vereinbar mit unseren europäischen Werten und kollidiert mit geltendem Datenschutzrecht.“