Es klingt fürsorglich, fast harmlos. Wer könnte schon dagegen sein, Kinder vor Missbrauch zu schützen? Mit diesem moralischen Schutzschild treibt die Europäische Union derzeit ein Projekt voran, das unsere digitale Welt für immer verändern könnte: die sogenannte Chatkontrolle. Offiziell soll sie helfen, Bilder und Videos von Kindesmissbrauch im Netz aufzuspüren. In Wahrheit aber bedeutet sie nichts anderes als die Abschaffung privater Kommunikation, wie wir sie kennen. Von **Günther Burbach**.

Dieser Beitrag ist auch als Audio-Podcast verfügbar.

https://www.nachdenkseiten.de/upload/podcast/250924_Chatkontrolle_Der_groesste_Angriff_auf_unsere_Privatsphaere_seit_der_Vorratsdatenspeicherung_NDS.mp3

Podcast: Play in new window | Download

Denn was geplant ist, sprengt jedes Maß. Künftig sollen sämtliche privaten Nachrichten – ob bei WhatsApp, Signal, Threema oder in der E-Mail – vor der Verschlüsselung auf den Geräten selbst durchsucht werden. Algorithmen würden Fotos, Texte und Videos scannen, angeblich nur nach verdächtigen Inhalten. Doch einmal etabliert, könnte dieses System beliebig erweitert werden. Im Klartext: Die EU arbeitet an einem Mechanismus, der jede Nachricht eines jeden Bürgers präventiv kontrolliert. Das ist nichts anderes als eine digitale Hausdurchsuchung, flächendeckend, anlasslos und dauerhaft.

Die Heuchelei der EU

Deutschland und Luxemburg haben sich zwar offiziell gegen den Vorstoß gestellt, Datenschützer warnen vor einem Dammbruch, Bürgerrechtler sprechen vom größten Angriff auf die Privatsphäre seit der Vorratsdatenspeicherung. Doch die Erfahrung mit Brüssel zeigt: Was einmal auf den Tisch gelegt wird, verschwindet nicht mehr. Auch die Vorratsdatenspeicherung wurde nach ihrer verfassungsrechtlichen Schlappe immer wieder neu aufgelegt, leicht modifiziert, umetikettiert, politisch weichgespült. Dasselbe droht nun mit der Chatkontrolle. Heute heißt es noch „nur gegen Kindesmissbrauch“, morgen könnte es um Terrorismus gehen, übermorgen um „Hassrede“ und bald um jede Form politisch unliebsamer Kommunikation.

Die Heuchelei der EU ist dabei kaum zu überbieten. Auf der einen Seite brüstet man sich mit der DSGVO als weltweitem „Goldstandard für Datenschutz“. Auf der anderen Seite plant man ein System, das den Kern des Datenschutzes zerstört: die Ende-zu-Ende-Verschlüsselung. Was auf dem Handy, Tablet oder PC der Bürger passiert, soll künftig kein

privater Raum mehr sein, sondern ein überwachter Bereich, in dem Algorithmen alles durchsuchen dürfen. Man verkauft es als Schutz, in Wirklichkeit ist es der Einstieg in eine Überwachungsinfrastruktur, wie sie autoritäre Staaten seit Jahren anstreben.

Natürlich gibt es Profiteure. Die Sicherheitsbehörden sehen sich in ihrem alten Traum bestätigt: Ein System, das keine Schlupflöcher mehr kennt, das jede Kommunikation vorsorglich durchleuchtet, das ausnahmslos alle Bürger in Verdacht stellt. Big Tech darf sich ebenfalls freuen, denn die Umsetzung von „Client-Side-Scanning“ erfordert gigantische Investitionen in Technik und Infrastruktur. Kleine Anbieter wie Threema oder ProtonMail könnten daran zerbrechen. Apple, Meta und Microsoft hingegen haben die Ressourcen und würden ihre Monopolstellung weiter ausbauen. Unter dem Banner „Kinderschutz“ entstünde so eine Marktbereinigung zugunsten der größten US-Konzerne.

Das technische Fundament ist zudem alles andere als zuverlässig. Fehlalarme sind unvermeidlich, wenn Maschinen intime Fotos scannen. Das harmlose Urlaubsfoto vom Strand könnte plötzlich zum „Verdachtsfall“ werden. Gleichzeitig werden Kriminelle immer Wege finden, solche Scans zu umgehen. Leidtragende sind nicht die Täter, sondern die normalen Bürger, deren Kommunikation überwacht, katalogisiert und im Zweifel falsch interpretiert wird. Und noch gefährlicher: Ist das System einmal installiert, wird es nicht beim Kindesmissbrauch bleiben. Jeder Staat, der Zugriff darauf hat, wird es für seine Zwecke nutzen, sei es zur Kontrolle politischer Aktivisten, zum Ausspionieren von Journalisten oder zur Verfolgung unliebsamer Opposition.

Chatkontrolle und digitale Identität

Die Parallelen zur Vorratsdatenspeicherung sind unübersehbar. Auch damals versprach man Schutz vor Terror. Heraus kam eine riesige Datensammlung über die gesamte Bevölkerung, die weder Anschläge verhinderte noch Kriminalität ernsthaft eindämmte. Heute wissen wir, dass sie mehr Schaden anrichtete, als sie Nutzen brachte. Genau das wiederholt sich jetzt, nur eine Stufe gefährlicher, weil es nicht mehr um Verbindungsdaten, sondern direkt um Inhalte geht.

Man muss den Vorstoß zudem im größeren Kontext sehen. Parallel zur Chatkontrolle treibt Brüssel die Einführung einer digitalen Identität voran. Offiziell soll sie „Bequemlichkeit und Sicherheit“ bieten. In Wahrheit bedeutet sie, dass künftig jede digitale Handlung eindeutig einer Person zugeordnet werden kann. In Kombination mit der Chatkontrolle entstünde eine Infrastruktur, die es erlaubt, jede Nachricht einer identifizierten Person zuzuordnen, sie auszuwerten und zu speichern. Ein System, das jeder Diktatur die Arbeit erleichtern würde und das jetzt ausgerechnet in der Europäischen Union gebaut werden soll.

„Massenüberwachung durch die Hintertür“

Kritiker warnen seit Monaten. Der Chaos Computer Club spricht von „Massenüberwachung durch die Hintertür“. Die Organisation European Digital Rights nennt die Pläne ein „Orwell’sches Projekt“. Selbst die Vereinten Nationen haben Bedenken geäußert, was Pressefreiheit und den Schutz von Whistleblowern betrifft. Doch wie so oft werden kritische Stimmen in den großen Medien an den Rand gedrängt. Stattdessen dominieren Schlagzeilen, in denen „Kinderschutz“ und „Sicherheit“ im Vordergrund stehen. Das Framing funktioniert: Wer sich gegen die Chatkontrolle ausspricht, läuft Gefahr, als Gegner des Kinderschutzes diffamiert zu werden.

Dabei ist es genau andersherum: Wer sich gegen diesen Eingriff stellt, verteidigt die Grundrechte. Kinderschutz ist notwendig, ohne Frage. Aber er darf nicht als Vorwand dienen, die Kommunikation aller Bürger zu durchleuchten. Das wäre, als würde man alle Wohnungen permanent durchsuchen, nur weil irgendwo ein Verbrechen stattfinden könnte.

Die politische Verantwortung liegt bei den Mitgliedsstaaten. Deutschland hat sich bisher klar gegen die Pläne positioniert. Aber wie lange bleibt es dabei? Der Druck aus Brüssel ist enorm, und auch in Berlin selbst gibt es Stimmen, die sich offen für eine „modifizierte Variante“ zeigen. Wer die Geschichte kennt, weiß: Einmal eingeführte Überwachung verschwindet nicht wieder. Sie wird zur Normalität, zum Standard, zum „neuen Normal“.

Freiheit darf nicht im Namen der Sicherheit geopfert werden

Am Ende geht es um eine Grundsatzfrage: Wollen wir in einer Gesellschaft leben, in der jede private Nachricht potenziell mitgelesen wird? Die EU beantwortet diese Frage gerade mit Ja. Es liegt an uns, ob wir dieses Ja akzeptieren oder ob wir endlich erkennen, dass Freiheit nicht im Namen der Sicherheit geopfert werden darf. Denn wer heute glaubt, man könne die Privatsphäre Stück für Stück einschränken und am Ende doch frei bleiben, der irrt gewaltig. Die Geschichte lehrt das Gegenteil.

Die Chatkontrolle ist kein harmloser Gesetzesvorschlag. Sie ist der Einstieg in ein Überwachungssystem, das die Grundrechte in Europa auf Jahrzehnte hinaus verändern würde. Es geht nicht um Kinderschutz. Es geht um Kontrolle. Und wenn wir sie zulassen, geben wir nicht nur unsere digitale Privatsphäre auf, sondern auch ein zentrales Stück Freiheit.

Quellen:

- TechRadar: „Chat Control: Germany joins opposition against mandatory scanning of private chats“ (September 2025)
- EU-Kommission: „Proposal for a regulation laying down rules to prevent and combat child sexual abuse“ (2022, aktuell in Verhandlungen)
- Chaos Computer Club kritisiert Chatkontrolle (2023)
- EDRi-Archiv zur Chatkontrolle

Titelbild: Creativan / Shutterstock