PARTEI DES FORTSCHRITTS

PDF

Positionspapier der PdF zum Thema ”Chatkontrolle”

Inhaltsverzeichnis

Positionspapier der PdF zum Thema ”Chatkontrolle”

1. Einführung

In der heutigen digitalen Welt ist die Privatsphäre ein Grundrecht, das geschützt werden muss. Die Einführung der Chatkontrolle stellt jedoch eine ernste Bedrohung für dieses Recht dar. Wir sprechen uns entschieden gegen jegliche Form der Chatkontrolle aus, sei sie umfassend oder rein anlassbezogen, und plädieren für den Erhalt der Privatsphäre und der digitalen Freiheit.

1.1. Erklärung - Was ist die “Chatkontrolle“

Die “Chatkontrolle“ ist ein umstrittenes Gesetzesvorhaben der EU-Kommission, das darauf abzielt, die Bekämpfung von Kindesmissbrauch und die Verbreitung von Missbrauchsdarstellungen im Internet zu verbessern. Es sieht vor, dass Anbieter von Kommunikationsdiensten wie Messenger-Apps und E-Mail-Diensten verpflichtet werden, private Nachrichten und Inhalte auf verdächtige Inhalte zu scannen und gegebenenfalls an die Behörden weiterzuleiten. Diese Maßnahmen sollen ohne konkreten Verdacht erfolgen, was einen erheblichen Eingriff in das Recht auf Privatsphäre darstellt. [1,2,3]

2. Unsere Gründe gegen die Chatkontrolle

2.1. Eingriff in die Privatsphäre

Die Chatkontrolle würde es staatlichen Stellen ermöglichen, private Nachrichten und Kommunikation ohne hinreichenden Verdacht zu überwachen. Dies stellt einen massiven Eingriff in die Privatsphäre der Bürger dar und kann das Vertrauen in digitale Kommunikationsmittel erheblich untergraben. Eine solch weitreichende Überwachung ist unverhältnismäßig und unvereinbar mit den Grundrechten. Die Möglichkeit, dass private Gespräche und Nachrichten ohne rechtlichen Anlass überwacht werden, gefährdet nicht nur die Privatsphäre, sondern auch die Freiheit der Meinungsäußerung. [1,3]

2.2. Gefahr der Selbstzensur

Eine Studie von Jon Penney zeigt, dass massive Überwachung Angst und konformistisches Verhalten fördert, was die Meinungsfreiheit und den offenen Austausch von Ideen erheblich schädigt [4]. Daher könnte die Überwachung privater Kommunikation im Zuge der "Chatkontrolle" zu einer Selbstzensur führen. Menschen könnten aus Angst vor Überwachung und möglichen Konsequenzen aufhören, ihre Meinungen frei zu äußern. Dies stellt eine ernsthafte Gefahr für die Meinungsfreiheit dar, die ein fundamentales Element einer demokratischen Gesellschaft ist.

2.3. Massive Gefahren durch Hintertüren

Ende-zu-Ende-Verschlüsselung ist eine Methode, bei der Daten so verschlüsselt werden, dass nur der Absender und der Empfänger sie lesen können, während sie auf ihrem Weg durch das Internet vor unbefugtem Zugriff geschützt sind. Auch die Anbieter der Messenger selbst (WhatsApp, Signal, Threema, ...) können so verschlüsselte Nachrichten nicht mitlesen [5].

Private Kommunikation findet in vielen Fällen Ende-zu-Ende verschlüsselt statt, um die Vertraulichkeit und Integrität der jeweiligen Kommunikation zu wahren. Eine gesetzlich verankerte Möglichkeit zum "Abhören/Überwachen" würde dieses Prinzip aushebeln und unmöglich machen. Um diese nun doch zu überwachen, ist es nötig, die sicheren Ende-zu-Ende Verschlüsselungsmechanismen zu umgehen und sogenannte "Hintertüren" einzubauen. Das Einbauen solcher Hintertüren zwecks der Überwachung kann Tür und Tor für jeglichen auch ungewollten Missbrauch öffnen. Denn auch Cyberkriminelle oder Nachrichtendienste könnten solche Hintertüren früher oder später ausnutzen, um an sensible Informationen zu gelangen. Anstatt die Sicherheit zu erhöhen, würde die Chatkontrolle somit potentiell das Gegenteil bewirken und die Sicherheit der Bürger gefährden. Im Missbrauchsfall der Sicherheitslücke wäre eine solche Hintertür aufgrund der hohen Verbreitung der Plattformen mit einem erheblichen Risiko und potentiellen Schaden für die betroffenen Nutzer verbunden.

2.4. Industriespionage

Nicht nur Privatpersonen müssten um die Sicherheit ihrer persönlichen Daten bangen. Auch Unternehmen müssten damit rechnen, dass Kriminelle die Sicherheitslücken nutzen, um Industriespionage zu betreiben, was eine Gefährdung für alle in Europa tätigen Unternehmen darstellt. Unklar ist auch, wie der Missbrauch dieser Hintertüren durch (staatlich veranlasste)(Industrie-)Spionage verhindert werden soll.

2.5. Abhörsicherheit der Bundeswehr

Wie viele Privatpersonen und auch einige Unternehmen, stützt sich die Bundeswehr auf eine leicht angepasste Version von "Matrix", einem Ende-zu-Ende verschlüsselten Messenger, der als sehr abhörsicher gilt. Das Besondere: Die Server-Infrastruktur wird hierbei nicht zentral von einem Hersteller-Unternehmen betrieben sondern von den Nutzern (also hier der Bundeswehr) selbst. So betreibt auch die Bundeswehr ihre eigene Instanz, die nach außen selbstverständlich abgeschirmt ist. Bei einer Einführung der Chatkontrolle müsste allerdings der Betrieb von Matrix-Instanzen ohne staatliche Hintertüren verboten werden, da deren sichere Verschlüsselung dem klaren Ziel (alle Kommunikation zu überwachen) entgegen steht.

Für staatliche Stellen wie die Bundeswehr wurde - mit Blick auf die massiven Risiken einer bewussten Schwächung der eigenen sicheren Kommunikation - bereits eine Ausnahme geschaffen. Für uns als Partei des Fortschritts ist es nicht nachvollziehbar, dass ein solches Risiko für die breite Öffentlichkeit als akzeptabel eingestuft und Sicherheitsbedenken derart vernachlässigt werden.

2.6. Technische und rechtliche Herausforderungen

Die Einführung der Chatkontrolle würde immense technische und rechtliche Herausforderungen mit sich bringen. Die Ende-zu-Ende Verschlüsselung von Nachrichten, die zur Sicherheit der Kommunikation beiträgt, müsste kompromittiert werden. Zudem stellt sich die Frage, wie eine solche Überwachung rechtlich umgesetzt und kontrolliert werden könnte, ohne die Grundrechte zu verletzen.

Die Schwächung der Verschlüsselung würde nicht nur die Privatsphäre der Bürger, sondern auch sensible staatliche und wirtschaftliche Kommunikation gefährden, solange hierfür keine Ausnahmeregelung geschaffen wird. Es ist wichtig zu verstehen, dass eine Schwächung der Verschlüsselung an einem Punkt unweigerlich alle Nutzer betrifft. Verschlüsselung funktioniert nach dem Prinzip "alles oder nichts" - sobald eine Hintertür eingebaut wird, ist die gesamte Sicherheit kompromittiert. Dies würde bedeuten, dass nicht nur die Kommunikation der Bürger, sondern selbst bei Ausnahmeregelungen für staatliche Stellen noch immer die Wirtschaft anfällig für Angriffe und Überwachung durch unbefugte Dritte wäre.

2.7. Globale Kooperationen behindert

Europäische Staaten könnten im Falle eines Inkrafttretens der Chatkontrolle aus technischer Sicht nicht länger als verlässliche Partner angesehen werden, da mit dem Abfluss jeglicher Kommunikation und sämtlicher mit "uns" geteilten Daten an fremde Geheimdienste gerechnet werden muss. Da Ermittlungsbehörden und Geheimdienste aus aller Welt oft auf Kooperationen und die Weitergabe sensibler Informationen zur Verfolgung gemeinsamer Ziele angewiesen sind, könnten diese in ihrer Arbeit behindert werden.

2.8. Diskriminierung und Missbrauch

Es besteht die Gefahr, dass bestimmte Gruppen oder Individuen gezielt überwacht und diskriminiert werden. Die Chatkontrolle könnte von Regierungen missbraucht werden, um politische Gegner oder Minderheiten zu überwachen und zu unterdrücken. Ein solcher Missbrauch würde das Vertrauen in den Rechtsstaat untergraben und die sozialen Spannungen verstärken. Vergangene Erfahrungen mit Überwachungspraktiken, insbesondere gegenüber politischen Gegnern und Journalisten, stimmen nicht optimistisch bezüglich der Missbrauchsmöglichkeiten, selbst in demokratischen Ländern. Beispiele wie der Einsatz staatlicher Spionagesoftware in Saudi-Arabien zur Verfolgung von Regimekritikern zeigen, wie leicht Überwachungstechnologien zweckentfremdet werden können. Diese Vorfälle mahnen zur Vorsicht und verdeutlichen, dass auch in vermeintlich stabilen Demokratien die Gefahr des Missbrauchs solcher Technologien nicht unterschätzt werden darf.

2.9. Fragwürdige Effektivität

Die Wirksamkeit der Chatkontrolle zur Bekämpfung von Kriminalität ist stark umstritten. Kriminelle Aktivitäten verlagern sich häufig in schwerer überwachbare Bereiche, sobald neue Überwachungsmaßnahmen eingeführt werden. Dies bedeutet, dass die Chatkontrolle nur begrenzten Einfluss auf die tatsächliche Verhinderung von Straftaten haben könnte. Stattdessen würden sie primär unbescholtene Bürger unter Generalverdacht stellen, deren Kommunikation überwachen und deren gesetzlich verankerten Grundrechte verletzen. Dabei würden die gewünschten Sicherheitsziele nicht erreicht werden. Es ist wichtiger, gezielte und gut durchdachte Maßnahmen zu ergreifen, die auf konkreten Hinweisen und Ermittlungen basieren, anstatt großflächige Überwachungsmechanismen einzuführen, die wenig zur tatsächlichen Kriminalitätsbekämpfung beitragen.

Die Einführung der Chatkontrolle würde die Grundrechte der Bürger auf unverhältnismäßige Weise einschränken und die Sicherheit und Freiheit der digitalen Kommunikation gefährden beziehungsweise sogar komplett abschaffen. Wir setzen uns daher entschieden gegen die Chatkontrolle ein und plädieren für den Schutz der Privatsphäre, die Stärkung der Meinungsfreiheit und die Förderung sicherer und freier digitaler Kommunikationsmittel. Nur so können wir eine demokratische und vertrauensvolle digitale Zukunft gestalten.

3. Quellen

[1] `https://freiheitsrechte.org/themen/freiheit-im-digitalen/chatkontrolle` (Zugriff am 30.7.2024)

[2] `https://netzpolitik.org/2023/chatkontrolle-eu-gesetzgebung-einfach-erklaert/` (Zugriff am 30.7.2024)

[3] `https://digitalcourage.de/blog/2024/die-chatkontrolle-droht-jetzt-anrufen` (Zugriff am 30.7.2024)

[4] Penney, Jonathon, Chilling Effects: Online Surveillance and Wikipedia Use (2016). Berkeley Technology Law Journal, Vol. 31, No. 1, p. 117, 2016, Available at SSRN: `https://ssrn.com/abstract=2769645`

[5] `https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-I`
`Onlinekommunikation/Verschluesselt-kommunizieren/verschluesselt-kommunizieren_`
`node.html` (Zugriff am 10.9.2024)

PdF– Partei des Fortschritts

Verwaltungssitz
Esserstr. 2
51105 Köln