Antrag 180/I/2024 Jusos LDK
Hände weg von meinen Chats! - Gegen Chatkontrolle und Überwachung im Internet

Beschluss:

Der Kongress der Party of European Socialists möge beschließen:

„Privacy is the right to a free mind" - Was bisher geschah

Vor 10 Jahren, im Sommer 2013, versetzte der NSA-Mitarbeiter Edward Snowden die Welt in Aufruhr: Mit der Veröffentlichung geheimer Daten und Materialien konnte er beweisen, dass die Geheimdienste der USA ihre eigenen und auch fremde Staatsbürger*innen gezielt – auch das Handy der damaligen Bundeskanzlerin Angela Merkel wurde überwacht – aber auch großflächig und ungerichtet abhörten. Diese permanente Überwachung und Aufzeichnung von Bewegungsdaten, Kommunikation und Bildern erlaubte es den Geheimdiensten, auch Jahre nach der Aufzeichnung detaillierte Profile über Personen zu erstellen. Diese Form der unbegründeten und rechtswidrigen massenhaften Überwachung und Vorratsdatenspeicherung stieß damals zu Recht auf weltweite massive Empörung.

Seit den Leaks von Edward Snowden hat sich an der Praxis der Geheimdienste wahrscheinlich wenig geändert. Die Möglichkeiten, die eigene Kommunikation zu verschlüsseln und so vor dem Zugriff Dritter zu schützen, wurden aber ausgeweitet. Was vor 10 Jahren noch ein Hobby von wenigen Personen war, ist spätestens mit der Einführung von Ende-zu-Ende-Verschlüsselung bei Messengerdiensten in der Breite der Gesellschaft angekommen. Ende-zu-Ende-Verschlüsselung erlaubt es Nutzer*innen, private Kommunikation zu führen, ohne dass die Nachrichten von Messengerdiensten, Regierungen oder anderen unbefugten Personen gelesen werden kann – ein riesiger Fortschritt für Privatsphäre und sichere Kommunikation im Internet.

Im Mai 2022 stellte die schwedische EU-Kommissarin Ylva Johansson einen Gesetzvorschlag vor, der das Ende für verschlüsselte Kommunikation und Anonymität im Internet bedeuten könnte. „Child Sexual Abuse Reduction" nennt sich dieses Vorhaben und das Ziel ist es, Kindesmissbrauch und die Verbreitung von diesen im Netz einzudämmen. Wir unterstützen das grundlegende, obligatorische Anliegen, der Unterbindung von Darstellungen sexuellen Kindesmissbrauchs, jedoch nicht diesen Weg dorthin. Denn dazu sollen neben der massenhaften Kontrolle von Chats auch Altersverifikation und Netzsperren eingesetzt werden.

Meine Chats gehören mir – und nicht einer KI oder den Behörden!

Ylva Johansson schlägt in ihrem Gesetzentwurf verschiedene Maßnahmen vor, die technische Umsetzung bleibt dabei unklar.

Zentral in der Debatte um diesen Entwurf ist die sogenannte Chatkontrolle: die Kommission hat das Ziel formuliert, alle Chats auf Kindesmissbrauch zu scannen.

Die Einführung einer Chatkontrolle würde dazu führen, dass die private Kommunikation jeder Person zu jeder Zeit gescannt würde. Dies würde einen massiven Einschnitt in die Bürger*innenrechte bedeuten.

Dass man verschlüsselte Kommunikation nicht einfach verbieten kann, ist zum Glück selbst Ylva Johansson klar. Die Alternative heißt „client-side scanning": jede Nachricht würde, bevor sie verschickt wird, auf dem eigenen Gerät gescannt und mit einer zentralen Datenbank aus Darstellungen sexuellen Kindesmissbrauchs verglichen. In der Logik der EU-Kommission wird dadurch die Verschlüsselung der Kommunikation nicht angegriffen, schließlich wird die Nachricht erst gescannt und erst danach verschlüsselt.

Doch das Gegenteil ist der Fall. Die Einführung dieser Technologie einen massiven Einschnitt in die Privatsphäre darstellen und nach Einschätzung des legal councils der EU die Essenz der fundamentalen Rechte verletzen. Auch die Expert*innen, die der Digitalausschuss des Bundestages im März zu einer Anhörung eingeladen hat, haben sich einmündig gegen client-side-scanning ausgesprochen. Von Kinderschutzbund und Internet-Ermittler bis Chaos Computer Club – nicht einmal der Union ist es gelungen, eine*n Expert*in aufzutreiben, der*die sich für die vorgeschlagenen Maßnahmen ausspricht. Auch der wissenschaftliche Dienst des Bundestags sieht im aktuellen Verordnungsentwurf “unverhältnismäsige Eingriffe in die geprüften Grundrechte der GRCh (EU-Grundrechtecharta).

Auch technisch zeigen sich Problematiken: damit eine KI Missbrauchsabbildungen erkennen kann, muss sie vorher auf einer Sammlung von solchen Abbildungen trainiert werden. Dabei werden der KI Abbildungen gezeigt und die KI soll die Abbildungen als Missbrauch oder nicht deklarieren. Die Entscheidungen der KI im Trainingsprozess müssen von Menschen kontrolliert werden, die sich ebenfalls diese Abbildungen ansehen und die Entscheidung der KI bestätigen müssen. Eine solche unbekannte KI bietet massives Missbrauchspotential. Verbrecher*innen könnten Zugriff auf Trainingsdaten erlangen und diese Abbildungen weiter nutzen oder sich durch die KI selbst Bilder generieren lassen. Weiterhin kann von Bürger*innen nicht kontrolliert werden, ob die eigenen Nachrichten tatsächlich nur in diesem Rahmen kontrolliert oder ob auch andere Inhalte gesucht werden.

Jede*r Bürger*in wäre davon betroffen, dass sämtliche private Kommunikation ständig durchsucht würde. Von einer zentralen unbekannten Entität. Neben echten Missbrauchsabbildungen würde diese Kontrolle auch jede Menge falsche Meldungen produzieren, also Nachrichten, die fälschlich als Missbrauch gekennzeichnet werden und dann von den Behörden kontrolliert werden. Dies kann sowohl das Versenden von Kinderfotos in Familiengruppen als auch Nachrichten betreffen, die sich Jugendliche einvernehmlich schicken. Studien zeigen zudem, dass Inhalte, die die queere Community betreffen, deutlich häufiger fälschlich als Pornographie erkannt werden.

Zudem ist fragwürdig, ob die Einführung der Chatkontrolle tatsächlich einen Beitrag zu weniger Kindesmissbrauch leisten würde. Missbrauchsabbildungen werden in der Regel nicht per Messenger versendet. Stattdessen werden Links auf Seiten im „dark net“ geteilt, von denen das Material anonym abgerufen werden kann.

Die Einführung einer Chatkontrolle würde das zugrundeliegende Problem also nicht lösen, sondern unverhältnismäßig in die Privatsphäre aller eingreifen.

Keine Stoppschilder im Internet – Löschen, statt sperren!

Schon 2009 sagte Ursula von der Leyen, damals noch als Familienministerin, Abbildungen von sexualisierter Gewalt gegen Kinder im Internet den Kampf an. Ihr Vorschlag: Seiten, auf denen Darstellungen sexuellen Kindesmissbrauchs zu finden sind, sollen gesperrt und mit einem großen Stoppschild versehen werden. Dieser Vorschlag wurde damals nach langen Protesten aufgegeben. Zu Recht! Netzsperren sind nicht nur schwer umzusetzen und lassen sich leicht umgehen. Wird eine Seite mit einem großen roten Stoppschild versehen, wird auch noch aktiver Täter*innenschutz betrieben. Alle Materialien existieren noch auf den Servern der gesperrten Seite und können von Betreiber*innen einfach auf eine andere Seite übertragen werden.

Stattdessen wird in Deutschland inzwischen das Prinzip „Löschen, statt Sperren“ verfolgt. Stoßen Ermittler*innen im Internet auf Darstellungen sexuellen Kindesmissbrauchs, wird dies an die Serverbetreiber*innen gemeldet, die die Seite mit allen Inhalten löschen. Dieses Verfahren ist „einfach und wirksam“, so berichtet es das Justizministerium. Und doch werden viele Seiten nicht direkt gelöscht. Den Behörden fehlt häufig Personal, um alle Seiten zu löschen. Es ist nicht hinnehmbar, dass einfache Mittel, die ausschließlich Täter*innen betreffen, durch Ermittlungsbehörden nicht ausgeschöpft werden.

Netzsperren sind auch auf europäischer Ebene zu verhindern. Stattdessen müssen Missbrauchsabbildungen wo immer sie auftreten, gelöscht werden. Behörden müssen ausreichend Personal ausgestattet sein, um Seiten zu löschen.

Alter, geht‘s noch? - Ein Internet ohne Altersverifikation und Ausweispflicht

Die Kommission geht in ihrem Gesetzesvorhaben aber noch weiter, als bestehendes Material zu erkennen. Auch dem sogenannten „grooming“ - also versuchter Kontaktaufnahme von Erwachsenen bei Kindern mit dem Ziel des Missbrauchs soll Einhalt geboten werden. Dafür könnten Anbieter*innen künftig dazu gezwungen werden, Alterskontrollen einzuführen.

Heute schon verhindern manche Anbieter*innen, dass Kinder von Erwachsenen angeschrieben werden können. TikTok beispielsweise stellt Accounts von 13- bis 15-jährigen grundsätzlich privat. Solche Maßnahmen basieren meist auf Selbstauskünften der Nutzer*innen, dies wird der EU-Kommission sicher nicht ausreichen.

Möglichkeiten der Altersverifikation reichen von der Identifikation mit Ausweisen bis zur KI-gestützten Berechnung des Alters durch biometrische Daten. Nicht nur aus Datenschutzperspektive ist dabei eine Variante schlimmer als die nächste.

Die Verifikation des Alters durch Kontrolle des Personalausweises würde das Ende der Anonymität im Internet bedeuten. Nutzer*innen jeder Plattform, auf der Chats möglich sind, müssten den Anbieter*innen persönliche Daten übermitteln. Ein Datenleak oder ein Hackerangriff auf die Datenbanken der Anbieter*innen wäre fatal. Durch die AusweisApp ist es theoretisch möglich, nur die Daten zu übermitteln, die tatsächlich gebraucht werden. Es ist jedoch abzusehen, dass sich Plattformen mit dieser Einschränkung nicht zufriedengeben werden, sondern unter den Deckmantel gesetzlicher Legitimierung weitere Daten zu Werbezwecken sammeln werden und so weitere Daten von Nutzer*innen sammeln können, die sie eigentlich nicht haben sollten.

Der Angriff auf die Anonymität im Internet hat aber auch weitere Auswirkungen, die zu kritisieren sind. Die Pflicht, für jede Form der Online-Kommunikation den Personalausweis vorlegen zu müssen, wird massive Auswirkungen auf die Kommunikationsfreiheit im Internet haben. Wenn Nutzer*innen bei jeder Anmeldung und Nachricht im Internet befürchten müssen, dass Inhalte gelesen und zurückverfolgt werden können, hat dies messbare Folgen für das individuelle Verhalten und die Meinungsfreiheit. Es ist zudem unverhältnismäßig: Niemand würde auf die Idee kommen, vor jedem Gespräch, Telefonat oder Museumsbesuch einen Personalausweis anzufordern.

Personen, die keinen Ausweis besitzen, wären so komplett von digitaler Teilhabe ausgeschlossen. Auch Betreiber*innen von Open-Source-Programmen wären von einer solchen Regelung bedroht. Open-Source-Programme ermöglichen es Nutzer*innen, Programme kostenlos zu nutzen, weiterzuentwickeln und zu testen. Dabei gibt es keine zentrale Datenbank von Nutzer*innen, sondern Programme oder Quellcode können aus verschiedenen Quellen genutzt werden. Der Schutz der persönlichen Daten von Nutzer*innen muss auch im Internet gelten!

Überweisen an

ASJ, FA III - Innen- und Rechtspolitik, Forum Netzpolitik