TAGESSPIEGEL
BACKGROUND

Cybersecurity

Warum die Chatkontrolle nutzlos, aber gefährlich ist

Anke Domscheit-Berg, digitalpolitische Sprecherin der Linksfraktion FOTO: FOTO: JANNIS FUNK, CC BY SA 4.0

Die Vorratsdatenspeicherung ist zwar weitgehend vom Tisch, aber nun droht ihre jüngste Schwester, bekannt als „Chatkontrolle“, per Europäischer Regulierung eine gefährliche Zensur-Infrastruktur zu schaffen, die von undemokratischen Regierungen, aber auch in der EU selbst missbraucht werden kann, ohne wirksame Kontrollmöglichkeiten durch Wissenschaft, Zivilgesellschaft, Journalismus oder Politik.

von Anke Domscheit-Berg veröffentlicht am 21.11.2022

Lernen Sie den Tagesspiegel Background kennen

Die EU-Verordnung soll Kinder vor sexualisierter Gewalt schützen, in dem Bilder davon oder Cybergrooming eher entdeckt werden. Weitreichende Eingriffe in Grundrechte werden immer mit Zielen durchgesetzt, bei denen der gesellschaftliche Widerstand klein ist, wer will schon als jemand da stehen, der Kindervergewaltiger vor Strafverfolgung schützt? Nach 9/11 war es der Kampf gegen den Terrorismus, davor war die Angst groß und deshalb der Widerstand klein gegen Überwachung im Netz.

Aber die Hürde für Grundrechtseinschränkungen liegt hoch, drei Anforderungen müssen erfüllt sein, unabhängig davon, wie edel die erklärten Ziele sind. Genau diese Prüfung nahm der unabhängige Wissenschaftliche Dienst des Bundestages in meinem Auftrag vor, denn jede Grundrechtseinschränkung muss sowohl geeignet, als auch angemessen und verhältnismäßig sein. Nach aktuellem Stand würde die Verordnung Diensteanbieter dazu verpflichten, eine Risikobewertung ihres Dienstes hinsichtlich der Verbreitung dieser speziellen Inhalte vorzunehmen. Dazu muss ein Diensteanbieter aber wissen, ob sein Dienst dafür genutzt wird, wozu er alle Inhalte kontrollieren muss. Das erfordert wiederum algorithmische Filter, da Milliarden von Inhalten zu prüfen wären.

Das ginge in zwei Varianten: entweder man baut Löcher in verschlüsselte Kommunikation ein, was ein klarer Verstoß gegen den Koalitionsvertrag wäre, der ein Bekenntnis zur Unantastbarkeit sicherer Verschlüsselungen enthält. Oder man nutzt Client Side Scanning (CSS), bei dem noch vor dem Verschlüsseln die Inhalte überprüft werden. Laut Wissenschaftlichem Dienst des Bundestages erfordert das CSS den Einbau „kodifizierter,

werkseitiger Hintertüren“ in den genutzten Geräten, also absichtliche Schwachstellen, die auch Dritte für Cyberangriffe nutzen können. Das reduziert die IT-Sicherheit in Zeiten hoher Angriffswahrscheinlichkeiten.

Auf meine Fragen nach ihrer Haltung zum CSS antwortete die Bundesregierung stets ausweichend. Hält Innenministerin Nancy Faeser eine Überwachung privater Kommunikationen per CSS etwa für vereinbar mit dem Koalitionsvertrag? Auch CSS macht verschlüsselte Kommunikation kaputt, denn ihr Zweck, vertrauliche und private Kommunikationen vor Kenntnisnahme Dritter zu schützen, ist nicht mehr erreichbar. Der Wissenschaftliche Dienst des Bundestages kommt daher zu der klaren Einschätzung, dass die verpflichtende Risikobewertung sichere Kommunikationswege faktisch abschafft.

Wäre die Chatkontrolle eine geeignete Maßnahme?

Schon bei der Prüfung der Eignung der Maßnahme dafür, ob sie Kinder vor sexualisierter Gewalt schützt, hat der Wissenschaftliche Dienst des Bundestages Bedenken und verweist u.a. auf den Kinderschutzbund, der die Verordnung für überzogen und in der Sache für nicht hilfreich hält. Das Hauptproblem sei nicht, dass es an Anzeigen fehlte, sondern dass es an Ressourcen fehlt, bei Anzeigen schnell und effektiv zu ermitteln. Es braucht schlicht mehr Personal. Die steigenden Fallzahlen der vergangenen Jahre liegen vor allem an der bereits stattfindenden Erhellung des Dunkelfeldes.

So arbeiteten in der zuständigen Stelle in NRW noch vor vier Jahren nur zwölf Fachkräfte, inzwischen sind es 90. Mit der Chatkontrolle bekämen diese bereits überlasteten Fachkräfte eine Welle Tausender falscher Meldungen zusätzlich, weil die Algorithmen auch bisher unbekannte Bilder flaggen und legales Sexting unterscheiden sollen von Cybergrooming, was hohe Fehlerraten unvermeidbar macht. Das bindet Ressourcen, die bei echten Fällen fehlen werden – das wirkt sogar gegen das erklärte Ziel.

Wäre die Chatkontrolle angemessen?

Der Wissenschaftliche Dienst prüfte auch, ob die Chatkontrolle angemessen ist, der EuGH meint damit, dass es keine andere Maßnahme gibt, die mit weniger Grundrechtseinschränkung das gleiche Ziel erreicht. Auch diese Prüfung besteht die Chatkontrolle nicht. Mehr Ressourcen für Strafverfolgung und vor allem für Prävention im Bereich Kinder-und Jugendschutz bereitzustellen, wären zum Beispiel grundrechtsfreundlichere Maßnahmen. Ich kenne selbst Fälle aus meinem Umfeld, wo weder von Cybergrooming betroffene Jugendliche noch deren Eltern und Lehrkräfte wussten, was zu tun war, wie groß potenzielle Gefahren sind und wie oft Täter mit falschen Identitäten unterwegs sind. Als Teil der Prävention zum Thema Cybergrooming könnte zum Beispiel der hervorragende Film „Gefangen im Netz“ in allen Schulen gezeigt und sein Material bearbeitet werden.

Wäre die Chatkontrolle verhältnismäßig?

Bei einer Grundrechtseinschränkung muss weiterhin der mit ihr erzielbare Nutzen in einem sinnvollen Verhältnis zu den unerwünschten Nebenwirkungen stehen, um vereinbar zu sein mit der EU-Grundrechtecharta (Art. 7, 8, 11 GRCh) und mit der EU Richtlinie 2002/58/EG, die die Vertraulichkeit der Kommunikation schützt. Der Wissenschaftliche Dienst des Bundestages kommt auch bei dieser Prüfung zu einer eindeutigen Einschätzung: die Verhältnismäßigkeit sei nicht gegeben, da bereits der Nutzen fraglich sei, die zu erwartenden negativen Effekte sowohl für die gesamte Gesellschaft (Stichworte Chilling Effect, geminderte IT-Sicherheit u.a.) aber auch für die eigentlich zu schützenden Jugendlichen gravierend sind.

So stammen nach einem Bericht der „Frankfurter Allgemeinen Zeitung“ von 5. Oktober 2022 inzwischen schon etwa 50 Prozent der illegalen Verbreitung pornografischer Inhalte von Jugendlichen selbst. Da das Strafrecht in Deutschland nicht unterscheidet, ob ein 50-Jähriger mit einer 15-Jährigen explizite Bilder austauscht oder zwei 15-Jährige untereinander, werden Heranwachsende schon heute kriminalisiert. Da Algorithmen der Chatkontrolle Cybergrooming von Sexting zwischen Minderjährigen nicht unterscheiden können, geraten Jugendliche künftig noch häufiger unter Verfolgungsdruck. Der Wissenschaftliche Dienst des

Bundestages verweist daher explizit auf die zu erwartenden negativen Folgen für die Entwicklung Heranwachsender.

Last but not least möchte ich auf die mangelnden Kontrollmöglichkeiten der Chatkontrolle hinweisen, denn schon in seinem Urteil zur Vorratsdatenspeicherung lehnten sowohl der EuGH als auch das Bundesverfassungsgericht deren Verhältnismäßigkeit auch mit dem Argument ab, dass es an hinreichendem Schutz vor Missbrauchsrisiken der Überwachung fehle.

Bei der Chatkontrolle wird ein als illegal identifiziertes Bild mit einem Algorithmus in einen Hash-Wert umgerechnet, der nicht wieder rückwärtsgerechnet werden kann. Dieser Hash-Wert wandert in eine Datenbank aller dorthin gemeldeten Hash-Werte. Ab da kann niemand mehr feststellen, was für ein Bild hinter einem solchen Hash steckt, es sei denn, man hat das Bild bereits und rechnet damit selbst einen Hash-Wert aus und kann dann beide Hash-Werte miteinander vergleichen. Will jemand die Verbreitung eines legalen, aber missliebigen Bildes behindern, bräuchte man nur den Hash-Wert dieses Bildes in die Datenbank laden und der Filter-Algorithmus der Chatkontrolle verhindert die Verbreitung dieses Bildes selbst in privaten Chats. Diese Eigenschaften machen die Chatkontrolle zu einer potenziell mächtigen Zensurmaschine, die sich externer Kontrolle entzieht. Bereits 2019 beschrieb die Electronic Frontier Foundation diese Missbrauchsmöglichkeiten von Client Side Scanning.

Ausblick

Viel Zeit bleibt nicht, um diese gefährliche Verordnung zu verhindern, sie soll den Digital Services Act ergänzen und voraussichtlich Anfang 2024 in Kraft treten. Mit an Sicherheit grenzender Wahrscheinlichkeit wäre eine Klage dagegen vor dem EuGH erfolgreich, aber bis zu einem Urteil vergingen Jahre, in denen Grundrechte verletzt werden, Diktaturen einen Blueprint für Zensurinfrastrukturen erhalten und den Einsatz mit Verweis auf die EU rechtfertigen können und in denen sinnlos Ressourcen gebunden werden, die für den wirksamen Schutz von Kindern vor sexualisierter Gewalt fehlen.

Anke Domscheit-Berg ist digitalpolitische Sprecherin der Bundestagsfraktion Die Linke.