— FZI-Position zur Chatkontrolle

Initiative gefährdet Grundrecht auf Sicherheit und Vertraulichkeit der digitalen Kommunikation

Version: 1
Veröffentlichung: 26.09.2024
Bearbeitet von: Aline Vugrincic, Maria Rill, Samuel Kalbfleisch

Inhaltsverzeichnis

1 Unsere Forderung: Sicherheit und Vertraulichkeit der digitalen Kommunikation schützen

Der derzeit vom Rat der Europäischen Union vorbereitete Entwurf einer „Verordnung zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern“[1] soll Kinder und Jugendliche besser vor sexuellem Missbrauch im digitalen Raum schützen. Dieses Ziel ist unumstritten. Nach unserer wissenschaftlichen Analyse wird jedoch genau dieses Ziel mit der geplanten Umsetzung verfehlt. Es wird eine technische Lösung suggeriert, die es nach dem Stand der Technik derzeit nicht gibt.

Stattdessen ermöglicht die Umsetzung der besser als CSA-Verordnung oder Chatkontrolle bekannten EU-Initiative staatlichen Sicherheitsbehörden zukünftig vom Gesetzgeber nicht-intendierte Möglichkeiten wie Massenüberwachung. Bei Inkrafttreten des Verordnungsentwurfs wird ein massiver Eingriff in das Grundrecht auf Sicherheit und Vertraulichkeit der digitalen Kommunikation aller Einwohner*innen der Europäischen Union (EU) vorgenommen. Dies wird einen Grundpfeiler unserer demokratischen Wertegemeinschaft ins Wanken bringen.

Deshalb fordern wir: Das Grundrecht auf Sicherheit und Vertraulichkeit der digitalen Kommunikation muss erhalten bleiben und weiterhin geschützt werden. Die geplante technische Umsetzung einer Chatkontrolle gefährdet massiv die Vertraulichkeit selbst von Ende-zu-Ende verschlüsselten Chatnachrichten. Deshalb sollte die Europäische Union die CSA-Verordnung in der jetzigen Form nicht in eine EU-Richtlinie oder -Verordnung überführen.

[1] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52022PC0209, zuletzt abgerufen am 25.09.2024

2 Die Bitte und der Aufruf an Sie

Die CSA-Verordnung darf aus unserer Sicht in der vorliegenden Fassung nicht in Kraft treten. Eine funktionierende Demokratie braucht auch im digitalen Raum eine sichere, private Kommunikation.

Die Umsetzung der geplanten Chatkontrolle schafft einen massiven Eingriff in individuelle Freiheitsrechte. Sie ermöglicht eine staatliche Massenüberwachung, die jede*n Einwohner*in der EU angreifbar macht.

Wir sehen derzeit keine Möglichkeit einer technisch sinnvollen und dabei grundrechtskonformen Umsetzung einer Chatkontrolle. Stattdessen sehen wir im zur Abstimmung vorliegenden Entwurf der CSA-Verordnung eine Gefahr für die Demokratie und der persönlichen Freiheit durch die Schwächung von Grundrechten. Der eigentlich angestrebte effektivere Schutz von Kindern und Jugendlichen als erklärtes Ziel der Chatkontrolle wird nach unserer Überzeugung nicht erreicht werden.

Bereits am 10. Oktober 2024 will der Rat der Europäischen Union über den Entwurf der CSA-Verordnung abstimmen. Deshalb bitten wir Sie und rufen Sie dazu auf:

- Sofern Sie im Rat der Europäischen Union für die entsprechende Abstimmung stimmberechtigt sind, fordern wir Sie aus den im Folgenden dargelegten Gründen auf, für den Erhalt der Grundrechte in der EU und gegen den Entwurf der CSA-Verordnung zu stimmen.
- Unterstützen Sie die Justiz- und Innenpolitiker*innen in Exekutive und Legislative mit den im Weiteren dargestellten Hintergründen.
- Sensibilisieren Sie Kolleg*innen im Europäischen Parlament, im Deutschen Bundestag und in den Landtagen für die Gefährdung des Grundrechts auf Sicherheit und Vertraulichkeit der digitalen Kommunikation.
- Machen Sie darauf aufmerksam, dass ein hochrelevantes gesellschaftliches Problem nicht durch dafür ungeeignete technische Mittel gelöst werden kann, und welche Gefahr für die Demokratie und die persönliche Freiheit aus einer Umsetzung der CSA-Verordnung erwächst.

3 Die Chatkontrolle als Lösungsansatz?

Aus den gemeldeten Zahlen zur Herstellung und Verbreitung von Missbrauchsdarstellungen von Kindern und Jugendlichen erstellt das Bundeskriminalamt (BKA) jährlich ein „Bundeslagebild Sexualdelikte zum Nachteil von Kindern und Jugendlichen“. Die Anzahl dieser Fälle[2] ist in den letzten Jahren kontinuierlich angestiegen. Im Jahr 2023 gingen laut BKA rund 180.300 Hinweise ein. Das sind 32 Prozent mehr als im Vorjahr 2022. Knapp die Hälfte dieser Meldungen, rund 89.350 Hinweise, waren nach deutschem Recht strafrechtlich relevant. Das massive Problem der sexuellen Belästigung von Minderjährigen, wie zum Beispiel durch Cyber-Grooming[3], ist also evident.

Die Diskussion um mögliche Lösungen für die Belästigung von Kindern und Jugendlichen im Internet dauert schon viele Jahre. Die EU-Kommission hat im Jahr 2022 die CSA-Verordnung als ihren Vorschlag für ein Angehen des Problems veröffentlicht. Allgemein ist diese unter dem Stichwort „Chatkontrolle“ bekannt.

Wissenschaftler*innen des FZI Forschungszentrum Informatik haben sich mit der CSA-Verordnung intensiv auseinandergesetzt. Sie haben untersucht, inwiefern der von der EU-Kommission vorgeschlagene Lösungsansatz in Form der sogenannten Chatkontrolle die Situation der zunehmenden Belästigung von Kindern und Jugendlichen im Internet verbessern könnte und wie er adäquat technisch umsetzbar ist. Als unabhängige, gemeinnützige Stiftung für angewandte IKT-Forschung mit einem gesellschaftlichen Auftrag haben wir den Textentwurf der CSA-Verordnung sowohl aus technischer als auch juristischer Sicht auf diesen Gesichtspunkt hin betrachtet.

3.1.1 Privatheit von Chats und Ende-zu-Ende-Verschlüsselung aufheben

Bereits im Juni 2024 sollte der Rat der Europäischen Union über den Entwurf der CSA-Verordnung abstimmen. Dann wurde dieser Punkt wieder von der Tagesordnung gestrichen[4]. Nun sollten sich die verschiedenen EU-Regierungen bis zu einem informellen Vorbereitungstreffen am 23. September 2024 zu einem neuen Textentwurf der CSA-Verordnung positionieren. Diesen hat die ungarische Ratspräsidentschaft erarbeitet und eingebracht[5]. Eine formelle Abstimmung im Rat der EU-Justiz- und Innenminister*innen[6] soll bei dessen nächsten Treffen am 10./11. Oktober 2024 stattfinden[7].

Der durch die ungarische Ratspräsidentschaft der EU vorangetriebene Entwurf einer EU-Verordnung

- zielt darauf ab, dass Nachrichten verschiedener Messenger wie zum Beispiel WhatsApp, Threema oder Signal, generalpräventiv nach Darstellungen sexuellen Kindesmissbrauchs gescannt werden sollen und
- Social-Media-Plattformen wie Instagram oder TikTok dazu verpflichtet werden, Maßnahmen zu ergreifen, um das Hochladen und Verbreiten von Missbrauchsmaterial im Internet zu verhindern.

---

[2] https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/SexualdeliktezNvKindernuJugendlichen/2023/BLBSexualdelikte.html, zuletzt abgerufen am 25.09.2024
[3] https://www.bka.de/cybergrooming.html, zuletzt abgerufen am 25.09.2024
[4] https://data.consilium.europa.eu/doc/document/ST-11222-2024-INIT/en/pdf#page=30, zuletzt abgerufen am 25.09.2024
[5] https://www.parlament.gv.at/dokument/XXVII/EU/195500/imfname_11406149.pdf, zuletzt abgerufen am 25.09.2024
[6] https://www.consilium.europa.eu/en/meetings/jha/2024/10/10-11, zuletzt abgerufen am 25.09.2024
[7] https://background.tagesspiegel.de/digitalisierung-und-ki/briefing/chatkontrolle-neue-abstimmung-fuer-10-oktober-angesetzt, zuletzt abgerufen am 25.09.2024

Dafür soll auch die Verschlüsselung von Chatnachrichten umgangen werden. Bereits auf dem Endgerät der Nutzenden sollen Inhalte mittels der Technik des sogenannten „Client-Side-Scanning“ überwacht werden[8].

Es kann davon ausgegangen werden, dass Personen, die Missbrauchsdarstellungen besitzen und versenden wollen, sich der Chatkontrolle entziehen werden. Diese werden auf alternative Messenger-Dienste oder Versandarten ausweichen oder Daten manuell verschlüsseln. Damit wären die Personen weiterhin nicht oder nur schwer greifbar, die man mittels der Chatkontrolle ermitteln möchte. Hingegen müssten andere Nutzer*innen unverhältnismäßige Rechtseingriffe hinnehmen.

Die Chatkontrolle sei auch deshalb nicht zielführend, da ein Gros der „Kindesmissbrauchsinhalte[n] über Plattformen und Foren geteilt“ werde, so in einem Interview der Vizepräsident des Kinderschutzbundes[9], Joachim Türk.

3.1.2 Praktische Bedeutung und Umsetzung

Viele moderne Messenger-Dienste verwenden Ende-zu-Ende-Verschlüsselung, um die Vertraulichkeit und den Datenschutz beim Versenden von Nachrichten zu gewährleisten.

Dieses Verfahren schützt Nachrichten bei der Übermittlung über das Internet. Nur Sender*innen und Empfänger*innen der Nachricht können diese lesen. Weder der Anbieter des Messengers, Internet-Service-Provider, Hacker oder staatliche Akteure können den Inhalt der Nachricht entziffern.

Die Bestrebungen der EU-Institutionen und aktuell der ungarischen Ratspräsidentschaft um die Einführung der Chatkontrolle konterkarieren diesen Schutz. Zukünftig würden alle Nachrichten von jedem Menschen in der Europäischen Union automatisiert auf strafbare Inhalte überprüft und im Verdachtsfall die Nachricht unverschlüsselt ausgeleitet.

Um eine solche Chatkontrolle technisch umzusetzen, hätten die Anbieter zwei Möglichkeiten:

- Die Ende-zu-Ende-Verschlüsselung aufgeben. Der Messenger-Betreiber könnte zukünftig alle Nachrichten auf dem eigenen Server auslesen und dort das Scanning ausführen. Diese Variante würde die Vertraulichkeit aller Chatnachrichten deutlich verschlechtern und gegenüber dem Betreiber vollständig aufheben.
- Beim Client-Side-Scanning werden die Nachrichten schon auf dem Gerät der Endnutzer*innen gescannt, zum Beispiel auf dem eigenen Smartphone. Bei einem Verdachtsfall wird dann die Vertraulichkeit der Chatnachrichten umgangen und die Nachricht unverschlüsselt ausgeleitet. Es wird also eine Überwachungssoftware in allen kooperierenden Messenger-Apps integriert.
  Diese zweite Variante des Client-Side-Scannings kann von technisch versierten Nutzenden umgangen werden. Dies ist insbesondere bei Apps wie Signal oder Threema möglich, da deren Quellcode öffentlich verfügbar ist.

Der geplante Ansatz der Chatkontrolle ist also ineffektiv. Er verfehlt das Ziel, Kinder und Jugendliche vor Missbrauch zu schützen.

[8] ebd.; https://www.bundestag.de/resource/blob/984702/6757ed249bcad12a6e00864d7a410fda/30-Sitzungsprotokoll-mit-Anlagen-OeA.pdf, zuletzt abgerufen am 25.09.2024
[9] https://www.deutschlandfunk.de/chatkontrolle-eu-messenger-kindesmissbrauch-scanning-durchsuchung-kommission-gesetzentwurf-100.html, zuletzt abgerufen am 25.09.2024

Stattdessen beschneidet dieser Ansatz der Chatkontrolle die Grundrechte aller Einwohner*innen der EU. Er legt das Fundament für eine tiefgehende Massenüberwachung, die die Privatsphäre aushöhlt und einen Grundpfeiler der Demokratie untergräbt. Denn die Ende-zu-Ende-Verschlüsselung schützt auch vor staatlicher Massenüberwachung. Diese ist in Gegenwart und Vergangenheit immer wieder von Regierungen, Regimen und Geheimdiensten etwa zur Überwachung und zur Unterdrückung der eigenen Bevölkerung angewandt. Sogar für private Interessen werden staatlich erhobene Daten wiederkehrend zweckentfremdet[10] genutzt.[11]

Zusätzlich verlangt der Entwurf der CSA-Verordnung, dass Messenger-Dienste alle über sie versendeten Nachrichten auf entsprechende Inhalte überwachen. In der Vorstellung der Autor*innen soll automatisiert entschieden werden, ob eine Nachricht unerwünschtes Material enthält. Bei einem Treffer soll die Nachricht ausgeleitet werden zur weiteren Überprüfung.

In der Natur der Sache liegt, dass **alle** Nachrichten gescannt werden müssen, um etwaige strafbare Inhalte aufzudecken. Dem entspräche im analogen Briefgeschäft der Postdienste, dass diese täglich alle Briefe in allen Verteilerzentrum öffnen und auf unerwünschte Inhalte überprüfen.

Der ursprüngliche Verordnungsentwurf sieht vor, dass sowohl bekannte als auch neue Missbrauchsinhalte erkannt werden sollen. Außerdem soll auch Cyber-Grooming erfasst werden. Die Form des Inhalts wird in der Verordnung nicht beschränkt, was heißt, dass neben visuellen Inhalten auch Text- und Sprachnachrichten einbezogen werden. Der Kompromissvorschlag der ungarischen Ratspräsidentschaft sieht vor, dass Cyber-Grooming und das Scannen auf bislang unbekanntes Material vorerst ausgespart bleiben soll. Jedoch schlägt Ungarn vor, die Chatkontrolle in einer späteren Verordnung dahingehend zu erweitern[12].

Doch auch Anbieter von Messenger-Diensten selbst könnten die unverschlüsselten Informationen zukünftig für eigene Zwecke nutzen. Das ermöglichte ihnen beispielsweise, die Aufmerksamkeit von Nachrichteninhalten den eigenen Erwartungen oder jenen von Sponsoren und Werbepartnern anzupassen.

Je nach Qualität der technischen Umsetzung in Messenger-Apps besteht zudem die große Gefahr, dass Dritte die geplante Chatkontrolle ausnutzen können etwa für Spionage, Datendiebstahl, Manipulation oder Erpressung. Spätere Erweiterungen der CSA-Verordnung sind im vorliegenden Entwurf schon jetzt intendiert, wie etwa von der Ratspräsidentschaft Ungarn vorgeschlagen. Eine existierende rechtliche und technische Basis für das Mitlesen von Nachrichten erleichtert stark ein politisch gewünschtes kurzfristiges Anpassen des Überwachungsumfangs.

Fazit: Die Chatkontrolle beendet de facto die Vertraulichkeit von Chatnachrichten. Außerdem stellt sie mit der Ende-zu-Ende-Verschlüsselung einen der Grundpfeiler der Sicherheit digitaler Kommunikation in Frage. Einige Messenger-Dienste lehnen daher die Verordnung zur Chatkontrolle ab[13]. Sowohl Signal als auch

---

[10] https://www.behoerden-spiegel.de/2024/09/18/berliner-datenschutzbericht-veroeffentlicht, zuletzt abgerufen am 25.09.2024

[11] https://www.bpb.de/shop/zeitschriften/izpb/china-337/275566/situation-von-medien-und-internet; https://freedomhouse.org/country/china/freedom-world/2024, zuletzt abgerufen am 25.09.2024

[12] https://www.patrick-breyer.de/wp-content/uploads/2024/09/st12406.en_clean.pdf, zuletzt abgerufen am 25.09.2024

[13] Meredith Whittaker, Signal President, New Branding, Same Scanning: “Upload Moderation” Undermines End-to-End Encryption; https://signal.org/blog/pdfs/upload-moderation.pdf; EU’s Chat Control puts security and privacy at risk; https://element.io/blog/eus-chat-control-puts-security-and-privacy-at-risk; https://threema.ch/de/blog/posts/chatkontrolle-stoppen, zuletzt abgerufen am 25.09.2024

Threema kündigten bereits an, sich im äußersten Fall aus dem EU-Markt zurückzuziehen. Threema würde Unternehmensangaben zufolge gegen die Chatkontrolle rechtlich vorgehen oder diese gar umgehen[14].

3.1.3 Der Einsatz von Künstlicher Intelligenz ist voraussehbar

Wenn zukünftig auch bislang unbekannte Missbrauchsinhalte oder Grooming erkannt werden sollen, wie bereits vorausgedacht von der ungarischen Ratspräsidentschaft, ist abzusehen, dass fehleranfällige KI-Systeme als das üblich gebräuchliche Mittel zum Einsatz kommen werden. Während bekannte Bilddarstellungen über Hashes noch mit vergleichsweise niedriger Falsch-Positiv-Rate erkannt werden können, so müssen für die automatisierte Beurteilung unbekannter Inhalte deutlich fehlerbehaftetere Systeme wie KI-Klassifikatoren eingesetzt werden. Diese weisen hohe Falsch-Positiv-Raten auf. Auch zahlreiche Chatnachrichten mit legitimen Inhalten würden irrtümlicherweise als Missbrauchsmaterial oder Cyber-Grooming klassifiziert.

Selbst wenn ein Objekt von einem KI-Klassifikator korrekt als Mensch erkannt wird, so ist die Interpretation dieser Darstellung eine weitere Herausforderung; etwa die Unterscheidung eines legitimen Urlaubsbildes eines Kindes am Strand von strafrechtlich relevanten, auf Missbrauch hindeutenden Bildern. die Einschätzung des Alters einer abgebildeten Person kann selbst für Menschen eine Herausforderung sein. Auch Jugendliche, die freiwillig und im Einvernehmen entsprechende Bilder oder Texte versenden, könnten vermehrt mit juristischen Problemen konfrontiert werden, wenn ihre Nachrichten als CSA-Material interpretiert wird (sogenannte „Schulhof-Fälle“[15]).

Die Anforderung, Cyber-Grooming zu erkennen, verlangt außerdem ein umfassendes automatisiertes Scannen und Interpretieren von Textnachrichten. Da ohne entsprechenden Kontext selbst Menschen unerwünschte von erwünschten Kontaktaufnahmen nur schwer unterscheiden können, ist bei der Klassifizierung mittels KI-Systemen von einer besonders hohen Falsch-Positiv-Rate auszugehen.

3.1.4 Aufhebung der Verschlüsselung könnte gegen mehrere Grundrechte verstoßen

Die CSA-Verordnung könnte zum einen unionsrechtswidrig sein, da sie möglicherweise gegen verschiedene Artikel der Charta der Grundrechte der Europäischen Union (GRCh) verstößt. Die Chatkontrolle widerspricht beispielsweise dem Recht auf Privatsphäre (Art. 7 GRCh), welches die Vertraulichkeit und Integrität der Kommunikation schützt. Nutzende könnten weiterhin verpflichtet werden, verschiedene Daten, wie beispielsweise den Klarnamen oder das Alter, zur Identifikation und Verifikation zu teilen. So wäre eine anonyme Kommunikation im Privaten aber auch für Whistleblower oder marginalisierte Gruppen erschwert, wenn nicht gar unmöglich gemacht.

Darüber hinaus könnte auch auf nationaler Grundrechtsebene eine Verletzung gegen das Recht auf informationelle Selbstbestimmung, Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG, vorliegen. Nutzende können nicht mehr darauf vertrauen, dass ihre Kommunikation geschützt ist und nicht von Dritten eingesehen werden kann[16]. „Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen

[14] https://threema.ch/de/blog/posts/chatkontrolle-stoppen; https://www.chip.de/news/Zieht-sich-Signal-aus-Europa-zurueck-Das-steckt-dahinter_185303157.html, zuletzt abgerufen am 25.09.2024
[15] https://www.heise.de/news/Nacktfotos-So-will-Justizminister-Buschmann-Schulhof-Faelle-entkriminalisieren-9532696.html, zuletzt abgerufen am 25.09.2024
[16] Marquard in ZD-Aktuell 2024, 01628

in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abschätzen kann, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden“[17]. So hat das Bundesverfassungsgericht bereits 1983 dahingehend argumentiert, dass es eine Gefährdung der freiheitlichen Grundordnung darstellt, wenn eine unbegrenzte Datenerhebung stattfände[18]. Dies durch die Chatkontrolle nun in einer Art und Weise (beinahe) auszuhebeln, ist eine starke Abkehr von den verankerten und garantierten Grundrechten. Die Kommunikation über E-Mails, SMS und Chats ist auch durch das Fernmeldegeheimnis nach Art. 10 Abs. 1 GG geschützt. Eine Beschränkung dieses Rechtes ist nur aufgrund eines Gesetzes möglich und muss dabei auch verhältnismäßig sein. Der Eingriff in den Schutzbereich dieser Grundrechte durch die Chatkontrolle ist jedenfalls nicht oder nur sehr unwahrscheinlich verhältnismäßig.

Im Rahmen der Prüfung muss der Schutz von Kindern und Jugendlichen im Verhältnis zum Schutz jeder einzelnen Person bezüglich einer Überwachung der Chatnachrichten betrachtet werden. Im Jahr 2023 wurden in der Polizeilichen Kriminalstatistik 2.580 Fälle von Cyber-Grooming erfasst, das Dunkelfeld ist dabei sehr viel größer einzuschätzen[19]. Im selben Zeitraum wurden schätzungsweise 400 Milliarden Nachrichten über verschiedene Messenger oder per SMS versendet[20]. Cyber-Grooming betrifft daher nur einen Bruchteil dieser riesigen Nachrichtenmenge. Dies wirft die Frage auf, ob es verhältnismäßig ist, dass dafür jede Person auf digitale Privatsphäre verzichten muss. Zudem bleibt eine Umgehung der Sicherheitsvorkehrungen der Chatkontrolle möglich. Weiterhin werden viele Täter*innen schwer zu ermitteln sein. Das eigentliche Ziel, Kinder und Jugendliche vor Missbrauch und Belästigung zu schützen, wird deshalb mit großer Wahrscheinlichkeit verfehlt.

Es kann bezweifelt werden, dass der durch die Chatkontrolle verfolgte Zweck der Prävention und der Bekämpfung des sexuellen Missbrauchs von Kindern und Jugendlichen durch eine Überwachung erreicht werden kann. Täter*innen könnten die Inhalte über andere Kanäle austauschen und Kinder und Jugendliche weiterhin zu Opfern von sexuellem Missbrauch werden. Auch könnten Kinder und Jugendliche, je nach technischer Ausgestaltung, weiterhin mit Nachrichten oder Inhalten konfrontiert werden, sodass auch dort der gewünschte und erforderliche Schutzzweck ins Leere liefe.

Der Kinderschutzbund hebt hervor, dass auch Kinder in ihrem Recht auf freie Meinungsäußerung und Teilhabe beschnitten würden: Durch die Furcht, ständig überwacht zu werden, könne dies die Entwicklung von Kindern beeinträchtigen, da sie sich nicht mehr über bestimmte Themen informieren oder Hilfe suchen könnten, ohne Konsequenzen befürchten zu müssen[21].

Abkehr von der Unschuldsvermutung

Durch den flächendeckenden Einsatz der Chatkontrolle würden grundsätzlich alle Nutzenden unter Generalverdacht gestellt werden, entsprechendes Bild- oder Videomaterial zu verbreiten oder mittels Textnachrichten Grooming zu betreiben[22]. Art. 48 Abs. 1 GRCh garantiert jedoch die Unschuldsvermutung,

[17] BVerfG (Erster Senat), Urteil v. 15. Dezember 1983, Az. 1 BvR 209/83, Rn. 73
[18] ebd. Rn. 74
[19] https://www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet/cybergrooming, zuletzt abgerufen am 25.09.2024
[20] https://www.bitkom.org/Presse/Presseinformation/Eine-Milliarde-Kurznachrichten-pro-Tag, zuletzt abgerufen am 25.09.2024
[21] https://www.bundestag.de/resource/blob/935798/3c6f75f6c2056130bca757bf7b4d0445/Stellungnahme-Tuerk-data.pdf, zuletzt abgerufen am 25.09.2024
[22] https://www.bundestag.de/resource/blob/935798/3c6f75f6c2056130bca757bf7b4d0445/Stellungnahme-Tuerk-data.pdf, zuletzt abgerufen am 25.09.2024

sodass jede*r als unschuldig anzusehen ist, bis die Schuld in einem rechtskräftigen Gerichtsverfahren nachgewiesen wird. Willkürlich Personen zu verdächtigen, CSA-Material zu besitzen oder Grooming zu betreiben, widerspricht dieser Unschuldsvermutung. Würden nun jedoch die Chats aller Personen ohne Anlass überwacht werden, würde dies den Grundsatz der Unschuldsvermutung erheblich gefährden. Bisher ist eine Überwachung durch Strafverfolgungsbehörden in der Strafprozessordnung nur vorgesehen, wenn diese durch die Staatsanwaltschaft oder ein Gericht angeordnet wird. Auch dies stellt einen Grundrechtseingriff dar, dieser muss jedoch auf die Verhältnismäßigkeit des Eingriffs überprüft werden. Der Eingriff kann beispielsweise unverhältnismäßig sein, wenn alternativ ein milderes Mittel als die Telekommunikationsüberwachung den verfolgten Zweck erfüllen könnte. Ein solches Vorgehen ist in der CSA-Verordnung nicht geplant.

Eingriffe in das Recht auf informationelle Selbstbestimmung gemäß Datenschutz

Die Überwachung und Analyse der Kommunikation der Nutzer durch die Chatkontrolle könnte auch gegen die Datenschutzbestimmungen verstoßen, da sie potenziell personenbezogene Daten der Nutzer betrifft, ohne angemessene Sicherheits- und Datenschutzmaßnahmen zu gewährleisten. Anbieter personeller Kommunikationsdienste ergreifen gemäß Art. 4 Abs. 3 der CSA-Verordnung erforderliche Maßnahmen zur Altersüberprüfung und -beurteilung, sodass minderjährige Nutzende zuverlässig identifiziert werden können. Die gleiche Pflicht trifft gemäß Art. 6 Abs. 1 lit. b und lit. c der CSA-Verordnung auch Anbietende von Stores für Software-Anwendungen. Es besteht die Gefahr, dass verschiedenen Personen(-gruppen) Zugriff auf die zur Identifizierung erforderlichen Daten haben könnten[23]. Es könnte passieren, dass Anbieter der verschiedenen Dienste alle über oder mit ihren Diensten verarbeiteten Daten auf die in Art. 7 Abs. 4 der CSA-Verordnung genannten Inhalte hin überprüfen müssen[24].

[23] https://www.dr-datenschutz.de/die-chatkontrolle-eu-kommission-auf-abwegen, zuletzt abgerufen am 25.09.2024

[24] https://www.datenschutzkonferenz-online.de/media/en/20231017DSKEntschliessungChatkontrolle.pdf, zuletzt abgerufen am 25.09.2024

4 Die Chatkontrolle verfehlt das eigentliche Ziel

Die Einführung der Chatkontrolle zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern setzt nicht an den eigentlichen Ursachen des Problems an und suggeriert eine technische Lösung. Bei einer Umsetzung der aktuell im Entwurf vorgeschlagenen Chatkontrolle wird somit das eigentliche Ziel verfehlt und stattdessen ein tiefgreifender Einschnitt in das Grundrecht auf Sicherheit und Vertraulichkeit der Kommunikation vorgenommen.

Denn wie die Analyse zeigt:

- Die Vertraulichkeit von Chatnachrichten und die Ende-zu-Ende-Verschlüsselung sichern zentrale Grundrechte von 450 Millionen Einwohner*innen der EU.[25]
- Der Schutz von Kindern und Jugendlichen im Internet durch die geplanten Maßnahmen wird bestenfalls temporär und nur grob lückenhaft erreicht, wahrscheinlicher jedoch vollständig verfehlt. [26]

Um Kinder und Jugendlichen zu schützen, erfordert es geeignete technische[27], rechtliche, pädagogische und gesundheitliche Maßnahmen. Cyber-Grooming ist nach §176 StGB bereits seit dem Jahr 2020 verboten. Technische Maßnahmen werden beispielsweise im Rahmen einer Kooperation zwischen der Onlineplattform Knuddelz und dem BKA erprobt.[28] Wie der Lagebericht 2024 des BKA mit den weiter ansteigenden Fallzahlen verdeutlichen, sind die aktuellen Maßnahmen jedoch nicht ausreichend.

Entscheidend sind zum Beispiel die frühzeitige Aufklärung und Schulung von Kindern und Eltern, innerhalb wie außerhalb der Schulen.[29] Eine Massenüberwachung dagegen würde auch die Freiheit von Kindern beschneiden, wie der Kinderschutzbund in seiner Stellungnahme im Deutschen Bundestag betonte[30].

Über das FZI

Das FZI Forschungszentrum Informatik mit Hauptsitz in Karlsruhe und Außenstelle in Berlin ist eine gemeinnützige Einrichtung für Informatik-Anwendungsforschung und Technologietransfer. Es bringt die neuesten wissenschaftlichen Erkenntnisse der Informationstechnologie in Unternehmen und öffentliche Einrichtungen und qualifiziert für eine akademische und wirtschaftliche Karriere oder den Sprung in die Selbstständigkeit. Betreut von Professoren verschiedener Hochschulen entwickeln die Forschungsgruppen am FZI interdisziplinär für ihre Auftraggeber Konzepte, Software-, Hardware- und Systemlösungen und setzen die gefundenen Lösungen prototypisch um. Mit dem FZI House of Living Labs steht eine einzigartige Forschungsumgebung für die Anwendungsforschung bereit. Das FZI ist Innovationspartner des Karlsruher Instituts für Technologie (KIT) und strategischer Partner der Gesellschaft für Informatik (GI).

---

[25] https://www.datenschutzkonferenz-online.de/media/en/20231017DSKEntschliessungChatkontrolle.pdf, zuletzt abgerufen am 25.09.2024
[26] Zurawksi in ZD-Aktuell 2022, 01240
[27] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Kinderschutz-im-Internet/kinderschutz-im-internet_node.html, zuletzt abgerufen am 25.09.2024
[28] https://hilfe.knuddels.de/de/articles/7983486-knuddels-und-das-bka-starten-kooperation, zuletzt abgerufen am 25.09.2024
[29] https://link.springer.com/article/10.1007/s00787-024-02566-9, zuletzt abgerufen am 25.09.2024
[30] https://www.bundestag.de/resource/blob/935798/3c6f75f6c2056130bca757bf7b4d0445/Stellungnahme-Tuerk-data.pdf, zuletzt abgerufen am 25.09.2024

Weitere Informationen und Kontakt

Jérôme Nguyen, Communications
FZI Forschungszentrum Informatik
Haid-und-Neu-Str. 10-14, 76131 Karlsruhe
Telefon: +49 721 9654-924
E-Mail: presse@fzi.de
Internet: www.fzi.de

Maria Rill, Forschungsbereich Cybersecurity and Law
Abteilung Law
FZI Forschungszentrum Informatik
Haid-und-Neu-Str. 10-14, 76131 Karlsruhe
E-Mail: m.rill@fzi.de

Samuel Kalbfleisch, Forschungsbereich Cybersecurity and Law
Abteilung Security Engineering
FZI Forschungszentrum Informatik
Haid-und-Neu-Str. 10-14, 76131 Karlsruhe
E-Mail: Kalbfleisch@fzi.de