**Deutscher Bundestag**
Ausschuss für Digitales

Ausschussdrucksache
20(23)136

27.02.2023

Der Kinderschutzbund
Bundesverband

**Stellungnahme des Kinderschutzbundes Bundesverband e.V. zur Öffentlichen Anhörung des Ausschusses für Digitales zur "Chatkontrolle"** am Mittwoch, 1. März 2023, 14 bis 16 Uhr.

# Inhalt



## Der Kinderschutzbund Bundesverband e.V.

Der Kinderschutzbund (DKSB) setzt sich für die Rechte aller Kinder und Jugendlichen in Deutschland ein. Er möchte eine kinderfreundliche Gesellschaft, in der die geistige, seelische, soziale und körperliche Entwicklung von Kindern und Jugendlichen gefördert wird. Dabei sollen diese an allen Entscheidungen, Planungen und Maßnahmen, die sie betreffen, beteiligt werden. Der Kinderschutzbund mischt sich zugunsten der Kinder und Jugendlichen ein – in der Bundes- und Landesgesetzgebung, bei Planungen und Beschlüssen in unseren Städten und Gemeinden. Er fordert eine Verbesserung der materiellen Lebensbedingungen der Kinder und Familien, eine kinderfreundliche und gesunde Umwelt und gute Einrichtungen für Kinder und Jugendliche. Dabei nimmt er auch die digitale Lebenswelt in den Blick und folgt dabei vor allem dem General Comment Nr. 25 des Kinderrechteausschusses der VN. Weitere Informationen zu den Zielen des Kinderschutzbundes finden Sie im Leitbild, im ergänzenden Digitalen Leitbild und im Kinderpolitischen Programm**.**

Der Kinderschutzbund bedankt sich für die Möglichkeit, zu den Fragen Stellung zu beziehen. Im Folgenden beantworten wir die Fragen 1-18 aus dem Fragenkatalog.

## Der Verordnungsentwurf und seine Implikationen

1. **Der Vorschlag der EU-Kommission zur CSA-Verordnung, auch bekannt als Chatkontrolle, hat seit seiner Veröffentlichung im Mai 2022 für viele Diskussionen gesorgt. Bitte erläutern Sie die technischen, juristischen, grundrechtlichen, datenschutzrechtlichen, sozialen und/oder gesellschaftlichen Implikationen des Vorschlags.**

Die EU-Initiative sendet ein deutliches Signal an alle Staaten der EU, stärker gegen sexualisierte Gewalt an Kindern vorzugehen. Das begrüßen wir nachdrücklich. Etliche Inhalte des Vorschlags sind Anliegen des Kinderschutzbundes. Der Kern des Regulierungsvorschlags der EU-Kommission zur Festlegung von Vorschriften zur Prävention und Bekämpfung der sexualisierten Gewalt gegen Kinder (CSAR) stellt Kinderschutz im Netz in den Fokus. Das Ziel ist, die Erstellung und digitale Verbreitung von Darstellungen sexualisierter Gewalt gegen Kinder und damit die Gewalt selbst zu bekämpfen. Um dieses unterstützenswerte Ziel umzusetzen, schlägt die Richtlinie notwendige und richtige Maßnahmen vor, geht aber an entscheidenden Punkten zu weit. Vor allem das anlasslose Scannen privater Kommunikation in Messenger-Diensten (wie z.B. WhatsApp oder Signal) oder E-Mails ist weder verhältnismäßig noch zielführend. Dies greift tief in Grundrechte der Kinder und Jugendlichen ein, deren Aufwachsen in einem Umfeld, in dem freie Meinungsäußerung und vertrauliche Kommunikation selbstverständlich sind, ein wesentlicher Pfeiler von Demokratie und Partizipation ist. Wir befürchten zudem, dass beim anlasslosen Scannen Kinder und Jugendliche noch viel häufiger kriminalisiert werden - eine Tendenz, die schon heute in der deutschen Kriminalstatistik sichtbar wird. Das hängt damit zusammen, dass Kinder und Jugendliche häufig selbst Bildmaterial versenden, das als pornografisch eingestuft wird, wodurch sie sich strafbar machen.

In dieser Debatte werden häufig Datenschutz und Kinderschutz gegeneinander ausgespielt - ein der Sache nicht gerecht werdender Ansatz. Die Kinderrechte brauchen beides: das Recht auf körperliche Unversehrtheit, aber auch das Recht auf geschützte Kommunikation. Ein anlassloser Angriff auf verschlüsselte persönliche Nachrichten setzt ein wesentliches Verfassungsrecht außer Kraft und damit gleich mehrere Kinderrechte, die in der EU-Verfassungsrang haben. Sie sind Pfeiler unserer Demokratie – ihre Gewährleistung prägt das Aufwachsen in einer freiheitlich-demokratischen Gesellschaft.

Gerade das Recht auf Privatsphäre, aber auch das Recht auf freie Meinungsäußerung, das Recht auf Information sowie der Schutz vor Gewalt, sind für die Entwicklung von Kindern unerlässlich. Nur wenn sie darauf vertrauen können, nicht konstant überwacht zu werden, können sie das notwendige Vertrauen in ihre Erziehungsberechtigten, Lehrer*innen und Freund*innen entwickeln, das dazu beiträgt, dass sie Hilfe bei Vertrauenspersonen suchen, wenn sie welche benötigen, und sich über gewisse Themen informieren, ohne Konsequenzen befürchten zu müssen. Besonders für Kinder und Jugendliche, die wegen ihrer sexuellen oder geschlechtlichen Identität, ihrer Behinderung, Herkunft oder Hautfarbe oder anderer Merkmale von Diskriminierung betroffen sind, ist dies relevant, denn sie sind online speziellen Risiken ausgesetzt.[1]

### Sinnvolle Maßnahmen für Kinderrechte im Netz

Als sinnvolle Maßnahmen im Vorschlag erachten wir zum Beispiel eine wirksame Altersverifikation

[1] https://home.crin.org/readlistenwatch/stories/encryption-debate

(allerdings ohne Ausweispflicht und Erhebung biometrischer Daten) ebenso wie Sicherheitsauflagen und die Pflicht zu Risikoanalysen für die Anbieter – sowohl von Hosting als auch von Plattformen wie den unter Social Media zusammengefassten. Sie sollen ihre Einrichtungen davor schützen, für Zwecke des Angebots, der Speicherung oder des Tauschs von Darstellungen sexualisierter Gewalt an Kindern genutzt zu werden. Dasselbe gilt auch für Cyber-Grooming – hier plädieren auch wir für Auflagen wie qualitativ hochwertige, sensible Moderation von Chats, Altersverifikation (mit den o.g. Einschränkungen) und so genannte Pattern-Analyse, mit der man Groomer*innen entdecken kann, um sie zu sperren und/oder zu melden. Hinzu kommen leicht erreichbare Meldeverfahren für Kinder und Jugendliche, die Hilfe benötigen. Dort muss es leicht verständliche Beschreibungen der angebotenen Hilfe geben und fachlich qualifizierte Angebote. Wir unterstützen den Plan, das bisher freiwillige Scannen von Bildmaterial auf den Servern der Plattformen und Filehoster verpflichtend zu machen – sowohl die Suche nach bekanntem Material (Hashes) als auch nach neuen Daten (KI-Unterstützung). Unseren Beifall bekommt auch die Einrichtung einer zentralen Behörde, die wie die NCMEC Daten sammelt, Strategien entwickelt, neue technische Verfahren unterstützt und die Unternehmen sowohl kontrolliert als auch bei den Risikoabschätzungen begleitet. Diese Einrichtung muss unserer Meinung nach unabhängig sein (vor allem von Europol) und eng mit Kinderschutzorganisationen zusammenarbeiten.

Der zentrale Punkt im Vorschlag der Kommission, mit dem wir nicht einverstanden sind, ist die landläufig als „Chatkontrolle“ bezeichnete sogenannte „Aufdeckungsanordnung“. Danach ist es möglich, am Ende eines behördlichen und juristischen Verfahrens bei allen Kund*innen eines Providers die Kommunikation über Wochen und Monate hinweg zu scannen. Das gilt für Unternehmen, die ihren Pflichten, das Risiko zu minimieren, nicht nachkommen, und bei denen ein „erhebliches Risiko“ besteht. Diese anlasslose Überwachung von Kommunikation ist ein tiefer Eingriff in das Grundrecht der Kommunikationsfreiheit, eines wesentlichen Bestandteils der Meinungsfreiheit und ein wichtiges Kinderrecht. Wir fürchten Auswirkungen auf das Verhalten von Kindern und Jugendlichen allein dadurch, dass diese Option besteht. Eine „Chatkontrolle“ widerspricht dem Bestreben, Grundrechte in einen Ausgleich zu bringen und eine Güterabwägung vorzunehmen. Auch Ermittler*innen und KI-Expert*innen sehen diese Komponente kritisch.

Unabhängig von diesen Bedenken weisen wir darauf hin, dass hier in einem juristischen Kopfstand die Falschen zur Verantwortung gezogen werden: Wenn Service-Provider den Auflagen nicht folgen, wird das Recht der Kund*innen eingeschränkt (man stelle sich Ähnliches beim Thema Geldwäschegesetz vor – wenn Banken fahrlässig arbeiten, würden dann die Konten aller Kund*innen überwacht).

Eine unserer zentralen Forderungen ist, mehr in Forschung zu investieren. Es braucht Fakten, Daten und Zahlen, um die breite Diskussion auf eine verlässliche Grundlage zu stellen. Beispielsweise sind die bekannten Zahlen der Ermittlungserfolge lediglich aus dem Hellfeld nachvollziehbar. Es gibt aber ein noch viel größeres Dunkelfeld, weshalb wir auch dessen Erforschung fordern:

- Auswirkung digital verfügbarer Darstellungen und Chats auf das Dunkelfeld, auf Täter*innen und Taten im Sozialen Nahbereich (Interaktion)
- Cyber-Grooming – Erforschung der Fälle, Verifikation der daraus resultierenden Taten / realen Begegnungen / Schwächen in Chats und Chatmoderation / Vorgehensweise der Täter*innen
- Die Verbindung und Interaktionen von Online-Material, Chats, Communities zu realen Taten
- Täter*innenprofil: Machtmissbrauch zwischen Pädosexualität und Ersatzhandlungen

- Greift die Theorie des Groomings von David Finkelhor (Vier-Faktoren-Modell)[2] auch im digitalen Raum?
- Die Taten im Nahbereich, in Familien, Nachbarschaften, Freundeskreisen, Vereinen usw. und die daraus resultierenden digitalen Handlungen
- Woher kommt neues Material und wie lässt es sich sicher aufspüren?
- Neue technische Möglichkeiten zur Risikominderung – die neue EU-Behörde in der Pflicht

Die Dringlichkeit des Anliegens dieses Gesetzentwurfs zur Bekämpfung von sexualisierter Gewalt gegen Kinder steht außer Frage. Wie wir hier dargelegt haben, zweifeln wir jedoch die Effektivität der vorgeschlagenen Maßnahmen in der jetzigen Form stark an. Wir weisen an dieser Stelle auch nochmals auf die UN-Kinderrechtskonvention sowie den General Comment 25 (also die Kinderrechte in der digitalen Welt), die einem Bundesgesetz gleichgestellt ist, hin. Denn neben dem Schutz von Kindern müssen auch ihre Teilhabe und Förderung denselben Stellenwert bei der Ausformulierung von gesetzlichen Maßnahmen Berücksichtigung finden.

## Cyber-Grooming

**2. Der Vorschlag der Kommission sieht vor, dass Aufdeckungsanordnungen ergehen sollen, die dazu führen, dass Anbieter*innen von Kommunikationsdiensten oder Geräten verdeckt Informationen ausleiten müssen, sofern der Verdacht besteht, dass über diese Dienste oder Geräte Missbrauchsmaterial ausgetauscht wird oder auf diesen Grooming stattfindet. Welche Dienste und Geräte sind aus Ihrer Sicht davon potenziell und in welcher Reichweite betroffen und welche Auswirkungen hat dies auf deren Nutzer*innen?**

Die aktuelle Studie zu Cyber-Grooming aus dem Jahr 2022 der Landesanstalt für Medien NRW[3] hat gezeigt, dass Cyber-Grooming zunehmend auf Instagram, TikTok, bei WhatsApp und auch auf Gaming Plattformen stattfindet. Es kann im Grunde überall stattfinden, wo Kontaktmöglichkeiten bestehen. Besonders von Kindern und Jugendlichen häufig genutzte Dienste, sind für Täter*innen interessant. Dazu zählen große Online-Plattformen wie YouTube und Twitch, Soziale Netzwerke wie TikTok, Instagram und Facebook, aber auch Online-Spiele und Gaming-Plattformen wie Fortnite, Steam, FIFA22 Online oder Minecraft. Um die Sicherheitsvorkehrungen der Plattformen zu umgehen, versuchen die Täter*innen nach der ersten Kontaktaufnahme oft auf privatere Kommunikationskanäle zu wechseln, etwa auf Messenger wie WhatsApp oder Videochat-Dienste.[4] Dabei handelt es sich also um Plattformen mit sehr großer Reichweite, die täglich von Millionen von Nutzer*innen verwendet werden.

Der Austausch von Missbrauchsmaterial geschieht häufig auf öffentlichen Plattformen – zum einen, um das Material leicht zugänglich zu machen und Interessenten anzulocken, zum anderen sind Angebote von "Neulingen" auf großen Plattformen zu finden. Professioneller gehen Täter*innen vor, die Accounts (z.B. auf TikTok u.a.) anlegen, diese auf privat stellen und mit Missbrauchsmaterial ausstatten und dann die

[2] vgl. Finkelhor 1984
[3] Vgl. https://www.medienanstalt-nrw.de/themen/cybergrooming/ein-viertel-aller-kinder-und-jugendlichen-wurde-bereits-im-netz-von-erwachsenen-zu-einer-verabredung-aufgefordert.html
[4] Vgl. https://www.klicksafe.de/cybergrooming

Zugangsdaten übermitteln. Missbrauchsmaterial, das z.B. in geschlossenen Gruppen, auch im Darknet, angeboten wird, ließe sich am besten entdecken, indem die Ermittler*innen in die Lage versetzt würden, häufiger online "auf Streife" zu gehen. Die rechtlichen Möglichkeiten dazu gibt es (z.B. das Angebot künstlich erzeugten Materials als Eintrittskarte).

Die Auswirkungen_auf die Nutzer*innen sind gravierend. Von digitaler Gewalt (z.B. Cyber-Mobbing, Cyber-Grooming, Hate Speech) betroffene Personen ziehen sich häufig aus dem Netz zurück.[5] Sie sind also in ihren Grundrechten wie Teilhabe, Zugang, Informations- und Meinungsfreiheit sowie auch Privatsphäre eingeschränkt. Darüber hinaus ist mittlerweile bekannt, dass digitale Gewalt genauso verheerende Auswirkungen auf die psychische Gesundheit hat wie alle anderen Formen von Gewalt auch. Häufig suchen sich Betroffene keine Hilfe, etwa weil sie sich schämen oder auch nicht genügend Vertrauen in andere Personen (oder Behörden) haben, sich die angemessene Unterstützung zu suchen.

## Technik allein schützt nicht vor Gewalt

**3. Wieso ist der Kommissionsvorschlag Ihrer Meinung nach geeignet oder nicht geeignet, Kinder effektiv vor (sexuellen) Übergriffen und der Verbreitung von Missbrauchsmaterial zu schützen und wo sehen Sie konkreten Handlungsbedarf?**

Der Vorschlag in seiner jetzigen Form wirft nicht nur verfassungsrechtliche Fragen auf, sondern es hapert auch an der technischen Umsetzung. Der Fokus auf eine technische Lösung ist zu einseitig und bleibt einem gesamtgesellschaftlichen Problem gegenüber blind. Denn beim Kinderschutz vor sexualisierter Gewalt im Netz auf rein technische Lösungen zu setzen, ist ein fataler Fehler mit verheerenden Folgen für demokratische Grundrechte aller Menschen, allen voran der Kinder. Expert*innen aus unterschiedlichen Bereichen (IT, Datenschutz, Menschenrechte, Jurist*innen, usw.) haben mehrfach gezeigt, dass ein solches Vertrauen in Technologie, die das Potential zur Massenüberwachung trägt, naiv ist und die Wahrung der Grundrechte aller Menschen schlichtweg ignoriert.

Die EU-Kommission setzt auf die hohe Trefferquote automatisierter Systeme zur Erkennung sexualisierter Gewalt gegen Kinder, vertraut dabei aber auf Angaben der Hersteller*innen.[6] Das ist ein Fehler, denn es braucht unabhängige Datenerhebungen, damit Hersteller*innen und Anbieter*innen nicht ihre eigenen Interessen bei der Weitergabe der Daten in den Vordergrund stellen können.

Wir teilen außerdem die Kritik, wie sie beispielsweise EDRi[7] formuliert, dass die Verordnung sich ausschließlich auf die Verbreitung im Internet, nicht aber auf die eigentliche Anfertigung von sexualisierten Gewaltdarstellungen von Kindern fokussieren will. Die vorgeschlagenen Maßnahmen seien

[5] Gerade Mädchen und junge Frauen, vor allem diejenigen, die Mehrfachdiskriminierung ausgesetzt sind, sind von digitaler Gewalt betroffen. Die Studie zu digitaler Gewalt an Mädchen und jungen Frauen von Plan International aus dem Jahr 2020 ("Weltmädchenbericht") zeigt auf, dass sich Betroffene aus sozialen Medien zurückziehen und somit von Teilhabe, freier Meinungsäußerung, Informationsfreiheit und anderen Grundrechten ausgeschlossen werden. https://www.plan.de/presse/pressemitteilungen/detail/welt-maedchenbericht-2020-digitale-gewalt-vertreibt-maedchen-und-junge-frauen-aus-den-sozialen-medien.html

[6] https://www.heise.de/news/Chatkontrolle-EU-Kommission-vertraut-bei-Trefferquote-auf-Meta-und-Hollywood-7286503.html

[7] https://edri.org/wp-content/uploads/2022/10/EDRi-Position-Paper-CSAR.pdf

außerdem ungeeignet, um die Verbreitung zu bekämpfen. Zu den sinnvollen Maßnahmen, die der Vorschlag völlig außer Acht lässt, zählen u.a. eine Stärkung der Ermittlungskapazitäten sowie eine angemessene Ausstattung von Institutionen, die sich aktiv für den Schutz von Kindern einsetzen. In seiner jetzigen Ausgestaltung erzeugt der Entwurf sogar Hindernisse für die Ermittler*innen, da die enormen Mengen an Falschmeldungen, die sich aus der Verordnung zwangsläufig ergeben werden, die Ermittlungen gegen die Täter*innen noch schwieriger machen könnten.[8] Des Weiteren ist zu berücksichtigen, dass die Darstellungen sexualisierter Gewalt von organisierten Gruppen kaum über die durch dieses Gesetz kontrollierten Wege verbreitet werden.

**Sinnvolle Maßnahmen**:

- Anbieter*innen in die Pflicht nehmen, das Material aufzuspüren, zu melden und vor allem auch zu löschen sowie Schutzkonzepte[9] transparent zu implementieren
- Prävention und Aufklärung: Wir setzen auf gemeinsame Information von Eltern, Kindern und Lehrer*innen/Betreuenden. Damit meinen wir u.a. Medienkompetenzförderung (z.B. um Kinder angemessen und altersgerecht bei der Internetnutzung zu begleiten, über Risiken bei der Veröffentlichung von Daten informieren), medien- und sexualpädagogische Aufklärung für Kinder, Eltern und Lehrer*innen (z.B. Fortbildungsangebote zu sexualisierter Gewalt), Schutzkonzepte im digitalen Raum[10]
- Stärkung der Ermittlungsbehörden, z.B. wäre es wünschenswert, wenn das Bundesinnenministerium Strukturen schaffen würde, die die Polizei bei ihrer Ermittlungsarbeit und Verfolgung von Straftaten wie Cyber-Grooming flächendeckend unterstützen und dies nicht als Verantwortung der Länder allein wäre. Es fehlt u.a. massiv an geschultem Personal, das auch im Netz unterwegs und ansprechbar ist. Eine Art Wache im Netz, die Kinder und Jugendliche direkt kontaktieren können und bei der Anzeigen niedrigschwellig möglich sind, würde vermutlich die Wahrscheinlichkeit erhöhen, dass Straftaten wie Cyber-Grooming überhaupt zur Anzeige gebracht werden. Außerdem gehört auch Aufklärung der Sicherheitsbehörden dazu: Was zählt als Straftat im Netz? Wie kann ich mich schützen? Wie gehe ich als Betroffene vor, z.B. wenn es um das Sichern von Beweisen geht?[11]
- Herausragend wichtig und nützlich wäre die enge Zusammenarbeit von Polizei und z.B. Kinderschutzorganisationen und Jugendämtern.
- Auch das geplante EU-Zentrum halten wir für sinnvoll, es ist jedoch von besonderer Bedeutung, damit keine von INTERPOL/EUROPOL gesteuerte europäische zentrale Polizeibehörde zu schaffen, das Zentrum muss unabhängig sein:
    - die Schaffung eines EU-Zentrums der zentralen EU-Anlaufstelle zur Bekämpfung sexualisierter Gewalt ist ein wichtiger Schritt. Hier müssen die Bemühungen koordiniert,

[8] https://www.childrenrights.de/special/bibliothek/bibliothek-details/privacy-and-protection-a-childrens-rights-approach-to-encryption
[9] Siehe Reform des JuSchG in 2021: https://www.bmfsfj.de/bmfsfj/aktuelles/alle-meldungen/reform-des-jugendschutzgesetzes-tritt-in-kraft-161184
[10] Informationen dazu z.B. von der Unabhängigen Beauftragten für Fragen des sexuellen Kindesmissbrauchs: https://beauftragte-missbrauch.de/themen/schutz-und-praevention/schutz-im-digitalen-raum
[11] Es gibt beispielsweise die Aufklärungsseite der Polizei, ein solches Angebot müsste ausgebaut werden: https://www.polizeifuerdich.de/

die Maßnahmen der Unternehmen überwacht, das Material begutachtet und katalogisiert und an die nationalen Ermittlungsbehörden weitergeleitet werden - was bisher weit überwiegend in den USA geschieht.
    - Wichtige europäische Institution, analog zum NCMEC (USA), die eine Datenbank mit Bildmaterial verwaltet und Meldungen an INTERPOL/EUROPOL und nationale Strafverfolgungsbehörden weitergibt („Gatekeeperfunktion“ um falsch-positive Meldungen auszusortieren)
    - Wichtige Institution in der Unterstützung von Betroffenen, auch um zirkulierendes Material zu löschen
    - Ggf. Technische und finanzielle Unterstützung von Service-Providern, die sich keine eigenen Kräfte dafür leisten können
- Schulungen der Polizei
- Ermöglichen von „Quick-Freeze“, bzw. Log-In-Fallen um Ermittlungsbehörden Zeit zu geben, einen Anfangsverdacht zu prüfen und gegebenenfalls auf Daten zur Identitätsfeststellung von Täter*innen zugreifen zu können
- mehr sichtbare Präsenz von Polizei im Netz („Streifen“)
- mehr staatliche Meldestellen, auch im Netz
- verstärkter Einsatz für die Prävention von sexualisierter Gewalt, d.h. erhöhte Wachsamkeit/Sensibilisierung im sozialen Umfeld von Kindern, geeignete und in der Breite verfügbare Präventionsangebote für Kinder, Eltern und pädagogisches Personal
- Medienkompetenzförderung
    - Aufklärung bzgl. Identifikation von Grooming und Umgang damit
    - Aufklärung von Kindern und Jugendlichen bzgl. Strafbarkeit von Sexting-Inhalten
- Aufklärung von Kindern und Jugendlichen im Deliktsbereich „Verbreitung, Erwerb und Besitz kinder- und jugendpornografischer Schriften“ (§184b/c StGB), um Kriminalisierung von Kindern und Jugendlichen, sofern keine pädokriminelle Absicht festgestellt werden kann, zu vermeiden

Wir weisen auch auf die Vorschriften des DSA hin, die in weiten Teilen ebenfalls geeignet sind, die Verbreitung von Darstellungen sexueller Gewalt zu verhindern und Cyber-Grooming zumindest erheblich zu erschweren. Vor einer Einschränkung von Verfassungsrechten möchten wir dem DSA die Chance geben, seine Wirkung zu entfalten.

## Private Kommunikation im Visier der Behörden

**4. Wie schätzen Sie die Gefahr ein, dass unbescholtene Bürger*innen, durch falsch positive automatisierte Erkennung unter Verdacht geraten und was würden solche Falsch-Positiv-Meldungen für Auswirkungen sowohl auf die Verdächtigen als auch auf die Ermittlungsbehörden haben?**

Die Zahl der falsch-positiven Hinweise ist gerade deshalb so relevant, weil “harmlose Nachrichten, Chats und Fotos von unschuldigen Personen mit expliziten Inhalten auf den Bildschirmen der Ermittler*innen landen und die Betroffenen so in Verdacht geraten könnten”. Die EU-Kommission rechnet damit, dass jede zehnte automatisierte Meldung bei der maschinellen Suche in Chatverläufen nach Cyber-Grooming-Fällen eine völlig legale Kommunikation offenlegen würde. Dies kann schnell dazu führen, dass Millionen

von legalen Nachrichtenaustauschen zu Unrecht ins Visier der Behörden geraten würden.[12]

Die Dateien der Darstellungen sexualisierter Gewalt an Kindern (Fotos, Videos) liegen auf Rechnern (Servern / Filehoster) im Internet. Dass sie entdeckt werden, geht auf freiwillige Vereinbarungen zurück. In den USA scannen vor allem die Unternehmen des Meta-Konzerns (Facebook, Instagram) ihre Bestände. Sie allein melden mehr als 20 Millionen Funde pro Jahr. Auch in Europa scannen Filehoster ihre Server und lösen Hinweise aus – die Erlaubnis dazu bietet eine Ausnahmeregelung einer Datenschutzvorschrift, der EU-Privacy Richtlinie. Sowohl die amerikanischen als auch die europäischen Unternehmen melden ihre Funde an eine amerikanische Nichtregierungsorganisation namens NCMEC (National Center for Missing and Exploited Children). Hier wird das Material gesichtet und eingestuft. Es handelt sich überwiegend um „bekannte" Darstellungen, aber pro Jahr kommen in Europa ca. 500.000 neue Bilder und Videos hinzu – Dokumente aktueller Gewalttaten. Die strafrechtlich relevanten Funde werden von der NCMEC den Strafverfolgungsbehörden der jeweiligen Staaten mitgeteilt – inklusive der IP-Adresse, von der die Dateien geladen wurden – in Deutschland dem BKA. Hier kommen pro Jahr ca. 80.000 solcher Meldungen an. In aller Regel kann das BKA dann über die IP-Adresse nicht nur den Provider ausfindig machen, sondern auch die Person, die zu diesem Zeitpunkt mit der gemeldeten Adresse aktiv war. Da die Provider nicht verpflichtet sind, diese Daten aufzubewahren, werden diese gelöscht, sobald sie aus internen Gründen nicht mehr gebraucht werden – meist innerhalb einer Woche. Danach lässt sich keine Verbindung mehr herstellen zwischen der IP-Adresse und ihrem Nutzer. Obwohl das NCMEC in Kenntnis der deutschen Datenschutzrichtlinien sehr schnell arbeitet, können Verfahren (wenn auch zurzeit eine Minderzahl) aus den o.g. Gründen nicht mehr verfolgt werden.

Die hier geschilderten Scan- und Meldungsabläufe sind die einzige nennenswerte Quelle zur Einleitung von Ermittlungs- und in der Folge Strafverfahren. Hinweise aus der Öffentlichkeit machen nicht einmal zwei Prozent aus. Führen die Online-Meldungen zu Strafverfahren, finden die Ermittler*innen in aller Regel Hinweise auf Mittäter*innen oder ganze Netzwerke. Ein Verzicht auf die automatisierten Scanverfahren würde die Ermittler*innen quasi blind machen.

Wir plädieren deshalb dafür, die Ausnahmeregelung noch einmal zu verlängern, einige aus unserer Sicht unstrittige Vorschläge der EU-Kommission und anderer Beteiligter umzusetzen und zu analysieren, wie sich diese Maßnahmen zusammen mit dem DSA auswirken. Zusammen mit Ergebnissen der von uns erhofften Forschung lassen sich dann ggf. Erkenntnisse gewinnen als Grundlage von weiteren Gesetzen oder neuen Strategien.

Noch vier wichtige Hinweise:

- Die schiere Masse der Meldungen bringt die Ermittlungsbehörden an ihre Grenzen – das BKA, das alles sichtet und die Verfahren einleitet; die Polizeidienststellen, die ausrücken und an Ort und Stelle agieren müssen, und die Justizbehörden.
- In Deutschland sind knapp die Hälfte der ermittelten Täter*innen unter 18 Jahre alt – sie lassen sich in drei Gruppen einteilen: Die einen haben die Aufnahmen mit Kindern einvernehmlich erstellt oder von Kindern geschickt bekommen (Sexting). Die zweite Gruppe hat – zum Beispiel im Gruppenchat – solches Material geschickt bekommen, und es ist durch die oft aktivierte automatische Speicherung auf dem Smartphone gesichert worden. Die mit Abstand kleinste

[12] https://www.heise.de/news/Chatkontrolle-EU-Kommission-vertraut-bei-Trefferquote-auf-Meta-und-Hollywood-7286503.html

Gruppe sind Minderjährige, die aus eigenen pädosexuellen Neigungen oder mit Verkaufsabsichten solche Bilder und Videos erstellen, besitzen und/oder verbreiten.

- Expert*innen nehmen an, dass ein Großteil der Taten nicht aus pädosexuellen Neigungen heraus geschieht, sondern als Ersatzhandlung zur Bedürfnisbefriedigung vor allem männlicher Täter.[13]
- Im sogenannten Darknet sind Pädosexuellengruppen mit fast mafiösen Strukturen aktiv; den Zugang erkauft man sich häufig durch Bilder und Videos.

## KI als Unterstützung, nicht als Ersatz

**5. Anbieter von Hostingdiensten und Anbieter interpersoneller Kommunikationsdienste, die eine Aufdeckungsanordnung erhalten haben, sollen laut Artikel 10 CSAM-E Technologien installieren und betreiben, die die Kontaktaufnahme zu Kindern mit Missbrauchsabsicht ("Grooming") erkennen. Sind Ihnen Technologien bekannt, die verlässlich zwischen unbedenklicher, sexuell oder romantisch aufgeladener, Kommunikation und Grooming unterscheiden können?**

Grundsätzlich stellt sich die Frage, inwiefern rein technisch eine Unterscheidung zwischen unbedenklicher und sexualisierter Kommunikation möglich sein soll. Eine Technologie kann zwar Muster erkennen lernen (machine learning), jedoch bezweifeln wir, dass Täter*innenstrategien auf diese Art allein aufgedeckt werden können. Im Kampf gegen Cyber-Grooming gibt es bereits zahlreiche Ansätze, die KI-basierte Textforensik nutzen. In Großbritannien und Australien wurde eine von Sprachforscher*innen der Swansea University entwickelte KI (“Dragon Spotter”) von der Polizei bereits erfolgreich eingesetzt, um Cyber-Grooming zu entdecken. In Deutschland sowie weltweit in zahlreichen anderen Ländern auch arbeitet die Polizei mit der Microsoft-Software “PhotoDNA”, welche sich allerdings nicht eignet, um neues Material zu finden. Eine weitere weltweit bekannte Software namens Safer wird von der NGO Thorn vermarktet und von Unternehmen wie Microsoft oder Vimeo eingesetzt, um Bild- und Textmaterial, das auf Cyber-Grooming schließen lässt, den Behörden zu melden. Mit welchen Datensätzen diese KIs trainiert werden, ist allerdings nicht weiter bekannt.[14] Technik kann also nicht als Ersatz, sondern unterstützend bei den Ermittlungen eingesetzt werden.

Pattern-Analyse am Beispiel WhatsApp

Auf Plattformen, die zur Kommunikation verwendet werden (also z.B: auch Spiele begleitende Chats), sollte ein ähnliches Verfahren zur Anwendung kommen, wie bei WhatsApp bereits verwendet. Dies geschieht derzeit so: Wenn ein verdächtiges Konto eine Reihe von anderen Konten kontaktiert, von denen einige Missbrauch melden, dann wird genauer hingesehen und nachgeforscht – also anlassbezogen.

Hier ist es besonders wichtig, dass die Meldungen schnell ernst genommen werden, und dass nicht erst nach zahllosen Meldungen ermittelt wird. Dafür sind zum einen geschultes Personal bei den Plattformen nötig, aber auch geschulte Ermittlungsbehörden nötig, um entsprechend auf die Fälle eingehen zu können.

[13] Definition der sexualisierten Gewalt an Kindern siehe Deegener, Prof. Dr. Günther: Kindesmissbrauch. Erkennen – helfen – vorbeugen. Weinheim 2010, S. 22

[14] https://netzpolitik.org/2022/chatkontrolle-was-unternehmen-schon-freiwillig-tun/

Über die Regelungen im DSA hinaus erwarten wir, dass Plattformbetreiber stärker in die Verantwortung genommen werden. Vor allem im Bereich der Überwachung von Interaktionsmöglichkeiten (Chats, Spiele, Lootboxen, usw) müssen strikte Regeln gelten analog der o.g. Pattern-Analyse. Bei Angeboten, die stark von Kindern frequentiert werden, muss auch Verhalten, das auf erwachsene Nutzer deutet, identifiziert und als Warnsignal verstanden werden.

6. **Welche technischen Ansätze halten Sie für effektive und grundrechtlich unbedenkliche Alternativen zu den im Verordnungsentwurf vorgesehenen Maßnahmen?**

Das bereits im Rahmen von Maßnahmen zur Moderation von Inhalten stattfindende Scannen von großen öffentlichen Plattformen (öffentlichen Inhalten) mit Hilfe von unterschiedlichen Werkzeugen (Abgleichen von Hashes, KI) stellt ein geeignetes Werkzeug dar, um öffentlich gepostetes Material aufzufinden, zu prüfen und zu entfernen. Die Verlängerung der Ausnahmeregelung erlaubt dies. Wir können uns auch eine Verpflichtung vorstellen. Das neue Europäische Zentrum müsste unabhängig die nötigen Hashes zur Verfügung stellen und aktualisieren und die Wirkung des Scannens erforschen.

Alle großen Plattformen, die den Werbemarkt bedienen, sind unseres Erachtens in der Lage, recht gut Verhalten vorherzusagen (auch deren Profiling ist eine Pattern-Analyse). Der DSA verpflichtet sie, das Angebot auf kindgerecht zu schalten, sobald die eigenen Systeme davon ausgehen, dass sie es mit einem Kind als Nutzer*in zu tun haben.

Wir plädieren darüber hinaus dafür, dass gewerbliche/institutionelle Angebote online ergänzend zu Impressum/AGB/Datenschutzerklärung eine leicht erreichbare Erläuterung in Einfacher Sprache anbieten, um Kindern den Zweck und die Hintergründe des Auftritts zu erklären und Rat und Hilfe anzubieten.

Überall da, wo Anbieter vergünstigte “Familien-Accounts” offerieren, müssten Eltern mit ihren Kindern die Altersangabe vornehmen – diese sollte (ähnlich wie bei Partnerschaftsvermittlungsangeboten) nicht änderbar sein und ggf. auslesbar zur Altersangabe bei Apps.

## Altersverifikation

7. **Der Vorschlag der Kommission enthält u.a. die Forderung nach einer verpflichtenden Altersverifikation. Wo genau und unter welchen Voraussetzungen müssten Internetnutzer*innen nach diesem Vorschlag ihr Alter verifizieren und welche technischen Ansatzpunkte gibt es oder werden gerade erforscht, um eine Altersverifikation grundrechtskonform unter Wahrung der Anonymität der Nutzer*innen im Internet umzusetzen?**

Wir fordern in Übereinstimmung mit dem General Comment Nr. 25 des Kinderrechte-Ausschusses eine Altersverifikation, die in beiden Richtungen (Inhalte vor Jüngeren verbergen; Zutritt für Ältere bei von Kindern genutzten Angeboten verhindern) funktioniert. Dabei ist es wichtig, diese grundrechtskonform zu gestalten. Rote Linien sind dabei folgende Punkte: Ausweispflicht, eine Erhebung von biometrischen Daten, sowie der Eingriff in verschlüsselte Kommunikation.

Vor allem große, stark nutzer*innenzentrierte und werbefinanzierte Plattformen sind längst in der Lage, Kinder und Jugendliche als Nutzer*innen zu erkennen. Wie im DSA festgehalten, sollten sie in solchen Fällen (Nutzer*in ist Kind/minderjährig) verpflichtet sein, ihr Angebot automatisch in einen angepassten, kindersicheren Modus (jugendsicher) umzuschalten. (Referenz DSA Erwägungsgrund 71 und Artikel 35 j))

Wir plädieren dafür, dass Eltern mit ihren Kindern Smartphone-Accounts anlegen und bei der (freiwilligen) Altersangabe korrekt vorgehen - was in manchen Fällen für sie auch finanzielle Vorteile hat. Wichtig: Diese Altersangabe sollte nicht veränderbar sein und kann als Default-Option (freiwillig) genutzt werden, um das Alter gegenüber anderen Plattformen (und Apps) auszuweisen. Chats und ähnliche Angebote, die Plattformen ergänzen, die stark von Kindern und Jugendlichen genutzt oder gezielt für diese erstellt werden, sollten per Default auf kindgerecht eingestellt sein.

Wir empfehlen einen Blick auf die Anlaufstelle für Kinder- und Jugendschutz ist im Netz in Deutschland, die Kommission Jugendmedienschutz (KJM), welche beispielsweise auch bereits existierende Systeme der Altersverifikation aus Jugendschutzperspektive überprüft und bewertet.[15]

## Privatsphäre ist ein Grundrecht

8. **Der Vorschlag der Kommission würde es ermöglichen, private Kommunikationsdienste zu Aufdeckungsanordnungen zu verpflichten, u.a. um Inhalte aus privaten und verschlüsselten Chats zu erlangen (u.a. Client Side Scanning), um Grooming zu erkennen oder das Alter zu verifizieren; als Folge des technologieneutralen Ansatzes sind potenziell auch Netzsperren denkbar. Welche internationalen Konsequenzen würden solche Möglichkeiten, das Nutzer*innenverhalten zu analysieren, oder den Zugang zu Online-Inhalten und sicheren Räumen zu beschränken, zeitigen – insbesondere im Hinblick auf eine höhere Gefahr rechtswidriger Eingriffe (Hacking) in die Privatsphäre europäischer Bürger*innen aus dem Ausland und im Hinblick darauf, dass autoritäre Staaten die EU-Regeln als Blaupause für illegitime Überwachungsmaßnahmen ohne rechtsstaatliche Einhegung nutzen?**

Eine “Chatkontrolle” würde eine Überwachungsstruktur schaffen, die sich auch für andere Zwecke missbrauchen ließe. Der Vorschlag bedroht dadurch beispielsweise auch bestimmte Berufsgruppen, die zur Verschwiegenheit verpflichtet sind. Technologie, die eine Zensur von bestimmten Inhalten noch vor dem Versenden oder Hochladen ermöglicht, gefährdet vor allem in (teil) autoritär regierten Ländern lebende Menschen, die politisch aktiv sind, Journalist*innen oder Menschen der LGBTIQ+ Communities. Dies betrifft Kinder genauso, vor allem die besonders schutzbedürftigen Kinder. Wir halten es für problematisch, beim Thema Kinder ein solches Pilotprojekt anzusiedeln, und regen eine breite Debatte über die Bekämpfung von Kriminalität und die Durchsetzung von Rechten im Internet (und Metaverse) an.

9. **Zuletzt hat das „Child Rights International Network“ in einer Studie die Bedeutung unterstrichen, „das Framing von Privatsphäre versus Kinderschutz hinter uns [zu] lassen, um**

[15] Siehe Auflistung der geprüften Altersverifikationssysteme: https://www.kjm-online.de/aufsicht/technischer-jugendmedienschutz/unzulaessige-angebote/altersverifikationssysteme/

**die Rechte aller Kinder zu schützen“ (Berichterstattung bei netzpolitik.org vom 02.02.2023). Wie verhält sich der aktuelle EU-Kommissionsvorschlag zu dem Recht von Kindern und Jugendlichen auf Privatsphäre und sichere IT-Systeme und welche kurzfristigen und langfristigen Konsequenzen hätte der Kommissionsvorschlag im Hinblick darauf?**

Die Sicherheit privater Kommunikation und persönlicher Daten sind auch jedes für sich wesentliche Kinderrechte. Aber nicht nur. Die Gewissheit, Meinungen und Haltungen und Vorlieben frei und vertraulich zu äußern, sind Grundlagen der Demokratisierung von Kindern und Jugendlichen. Wer dieses Recht antastet – und da genügt unseres Erachtens schon die Möglichkeit – schwächt die Entwicklung der künftigen Generationen zu Demokrat*innen (siehe Antwort zu Frage 1)

## Potentiale des Digital Services Act

10. **Welches politische Maßnahmenpaket ist aus Ihrer Sicht ganzheitlich erfolgsversprechend, um wirksam, effektiv und grundrechtskonform gegen sexualisierte Gewalt an Kindern vorzugehen – wo besteht Nachsteuerungs- und Verbesserungspotenzial im Bereich der Prävention und bei der Bekämpfung von sexualisierter Gewalt und deren Darstellung im Internet?**

Ein ganzheitlich erfolgsversprechendes Maßnahmenpaket ist uns nicht bekannt. Es gibt allerdings gesetzliche Potentiale, die ausgeschöpft werden können, bevor ein neues Gesetz, das vermutlich vor dem Europäischen Gerichtshof als grundrechtswidrig eingestuft und daher zurückgenommen werden würde, verabschiedet wird, und somit jahrelange Arbeit von vorne beginnen müsste.

Bei der Diskussion um die CSA-Regulierung wird häufig außen vorgelassen, dass die Möglichkeit besteht, die Ausnahme von der ePrivacy Richtlinie, die das neue Gesetz ersetzen soll, vorerst zu verlängern.

Grundlagen:

1. Anlass für den Vorschlag der CSA-Regulierung ist das Ende der Ausnahme von der ePrivacy Richtlinie, die es derzeit Anbieterinnen erlaubt, freiwillig unverschlüsselte interpersonelle Kommunikation zu scannen. Es besteht die Sorge, dass ohne eine dauerhafte Lösung als Nachfolge der Ausnahmeregelung eine große Zahl an Kindesmissbrauchsdarstellungen und damit potenziell Hinweisen auf Täter*innen unentdeckt bleiben.
2. Es gilt seit November 2022 der Digital Services Act, der im Februar 2024 in Kraft treten wird. Dieser enthält bereits eine große Bandbreite an Maßnahmen, die für mehr Kinderschutz online sorgen soll. Die Verlängerung der Ausnahme der ePrivacy Richtlinie in Kombination mit einer strengen Durchsetzung des DSA unter voller Nutzung der darin enthaltenen Schutzmechanismen für Kinder bietet bereits eine Lösung der von der Kommission angesprochenen Probleme.

Es sollte zunächst einmal genau beobachtet werden, ob die Durchsetzung des DSA in Verbindung mit einer Verlängerung der Ausnahmeregelung und in Verbindung mit der Umsetzung einzelner weiterer Vorschläge, darunter unbedingt das europäische Zentrum, um von der NCMEC unabhängig zu werden, den gewünschten Effekt auf die genannten Probleme hat, bevor weitere, sehr tief greifende Maßnahmen in Erwägung gezogen werden.

**Besonders hervor zu hebende Artikel im DSA**

- Art. 7 - Freiwillige Untersuchungen auf Eigeninitiative und Einhaltung der Rechtsvorschriften
- Art. 8 - Keine allgemeine Verpflichtung zur Überwachung oder aktiven Nachforschung
- 23 (Maßnahmen und Schutz vor missbräuchlicher Verwendung)
- Erwägungsgrund 12
- Erwägungsgrund 71
- Artikel 28 Online-Schutz Minderjähriger
- Artikel 34 - Risikobewertung
- Artikel 35 - Risikominderung
- Artikel 44 - Normen

Der Fokus auf Prävention ist aus Kinderschutz-Perspektive enorm wichtig.

Alle mit dem Thema vertrauten Expert*innen sind sich sicher, dass das Dunkelfeld der sexualisierten Gewalt immens groß ist. Wir wissen, dass Täter*innen vor allem dem so genannten sozialen Nahbereich (Familie, Verwandte, Freunde, Nachbarn, Vereine) entstammen. Die Erforschung des Dunkelfeldes der sexualisierten Gewalt (sozialer Nahbereich) muss weiter erfolgen, ohne dabei den Blick für alle Formen der digitalen Gewalt an Kindern zu verlieren, um Prävention und Intervention zu verbessern. Dazu gehören auch Fragen der Täter*innenentwicklung bezüglich bekannter Theorien dazu und möglicher Veränderungen durch die immense digitale Verfügbarkeit von Materialien und Darstellungen sexualisierter Gewalt.

- Welche Rolle spielt das Internet (Bilder und Videos bei der Täter*innenentwicklung, Chats bei der Anmache, Messenger bei der Bindung potenzieller Opfer)? Die Erforschung der Rolle von Online-Komponenten im Umfeld der Taten und der Anbahnung muss ebenfalls aus o.g. Gründen erweitert werden.
- Analyse der Herkunft neuen Materials (sowohl digital als auch seine ursprüngliche Quelle – also der Ort der Tat). Ohne belastbare Zahlen und Strukturkenntnisse laufen selbst weitgreifende politische Maßnahmen ins Leere.

Die Kinderschutz-Verbände fordern seit Jahren diese präventiven Maßnahmen:

- Einbinden von Kinderschutzthemen mit digitaler Komponente in die Ausbildung aller relevanten Berufsgruppen
- Einbeziehen von Onlineverhalten in Diagnosegesprächen, etwa bei Essstörungen und Identitätsproblemen.
- Präventionsmaßnahmen in Kitas und Schulen unter aktiver Einbindung der Eltern und Kinder
- Schutzkonzepte in allen Vereinen und Schulen verpflichtend – ständiges Monitoring und Weiterentwicklung
- Prävention zu Cyber-Grooming
- Jugendmedienschutz als Querschnittsanliegen in allen Schulfächern – insbesondere im Sachunterricht – der Grundschulen.
- Technischer Schutz - Bilder, die nicht weiterverbreitet werden können, sperren von Screenshots, verhindern das Bilder heruntergeladen werden => Weiterverbreitung verhindern

Wir weisen hier ausdrücklich darauf hin, dass die BIK-Initiative (Better Internet for Kids) der EU-

Kommission viele solcher Ansätze enthält.[16]

**11. Erfasst der Vorschlag der EU-Kommission alle Plattformen im Internet, auf denen kinderpornographisches Material verbreitet werden kann, zielgerecht oder in welcher Form besteht möglicherweise Nachbesserungsbedarf mit Blick auf den Geltungsbereich?**

Die Verbreitungswege sind sehr wahrscheinlich vielfältiger und werden flexibler genutzt, als wir es uns vorstellen können. Als Beispiel: Wir gehen davon aus, dass es eine enge Interaktion und viel Austausch zwischen Darknet und offenem Internet gibt, der durch Polizeiarbeit (international) und konsequentes Löschen durchbrochen werden kann. Das wäre auch politisch in den Blick zu nehmen.

## Das EU-Zentrum

**12. Sind Instrumente zur besseren Strafverfolgung und Rechtsdurchsetzung hinreichend im Vorschlag der EU-Kommission gewürdigt worden, wo besteht möglicherweise Verbesserungsbedarf und welche Instrumente wären dazu notwendig?**

Dies bedarf einer juristischen Einschätzung, die sowohl die EU-Ebene wie auch die staatlichen und länderspezifischen strafrechtlichen Regeln in diesem Zusammenhang ganzheitlich einschätzen kann. Grundsätzlich sind Instrumente notwendig, die die Ermittlungsbehörden sowohl personell, psychologisch als auch technisch bei der Bearbeitung derartiger Materialien im Bereich der sexualisierten Gewalt ausreichend aufstellt, um mit der schieren Masse an Materialien, Täter*innennetzwerke usw. effektiv arbeiten können.

Bei aller Distanz zu Europol wäre das neue Zentrum gut geeignet, Erfolg und Misserfolg unterschiedlicher Ermittlungsansätze zu messen und zu kommunizieren und daraus internationale Strategien abzuleiten.

Redundanzen sind zu vermeiden.

**13. Wird das neue EU-Zentrum die nationalen Strafverfolgungsbehörden und Europol, laut der aktuellen Planungen, angemessen unterstützen können und welche Ausstattung würde es dazu benötigen?**

Solange nicht geklärt ist, welche abschließenden Befugnisse dieses Zentrum hat, ist diese Frage nicht zu beantworten.

Grundsätzlich ist das Schaffen einer europäischen Version des "National Center of Missing and exploited Children" begrüßenswert. Eine enge Kopplung, jeglicher Art, an Europol ist jedoch abzulehnen.

Ein EU-Center sollte vollständig unabhängig sowohl finanziell als auch örtlich von Europol sein. Es muss eine enge Zusammenarbeit mit Kinderschutzorganisationen und Hotlines gewährleisten.

Weitere Verantwortungen sollte die Verwaltung der Hash Datenbank mit bereits bekanntem Material

[16] Siehe “A European strategy for a better internet for kids (BIK+)” https://digital-strategy.ec.europa.eu/en/policies/strategy-better-internet-kids

sowie die Forschung von Trends im Bereich Verbreitung o.Ä. sein.

Allerdings ist auch eine Zusammenarbeit mit nationalen Ermittler*innen zwingend notwendig. Das Zentrum betrachten wir nicht als Teil der Polizeiarbeit, aber es bewertet und vermittelt Erfahrungen – durchaus auch mit technischen Unterstützungswerkzeugen und Methoden nationaler Zusammenarbeit und Gesetzgebung.

Hilfreich wäre zudem, kleine und mittlere Anbieter sowohl finanziell als auch mit KnowHow und konkreten (Software-)Lösungen zu unterstützen, um deren Angebote und Dienste kindersicher zu machen und verdächtiges Material zu entdecken.

Darüber hinaus: Siehe Antwort zu Frage 3

## Kinderfreundliche Technologien by default

### 14. Umfasst der Vorschlag der EU-Kommission aus Ihrer Sicht alle technischen Ansätze, mit denen das Ziel, dem Schutz von Kindern gerecht zu werden, erreicht werden kann und welche weiteren technischen Ansätze wären aus Ihrer Sicht erforderlich?

Die derzeitigen technischen Ansätze im Entwurf sind nicht ausreichend. Um einen besseren Einblick in datenschutzkonforme und grundrechtewahrende technische Möglichkeiten zu erhalten, bedarf es an der Stelle Forschung und Aufklärung.

Bereits effektive und vielversprechende Ansätze sind zum einen das Server-Side-Scanning von öffentlichen Plattformen. Das bereits im Rahmen von Maßnahmen zur Moderation von Inhalten stattfindende Scannen von großen öffentlichen Plattformen (öffentlichen Inhalten) mit Hilfe von unterschiedlichen Werkzeugen (Abgleichen von Hashes, KI) stellt ein geeignetes Werkzeug dar, um öffentlich gepostetes Material aufzufinden, zu prüfen und zu entfernen. Zum anderen die so genannte Log-In-Falle[17] sowie das Quickfreeze[18], um extremes Material, das seinen Ursprung häufig im Darknet hat, nach Auffinden den Kreislauf von Kopie und Vorbereitung derartigen Materials zu stoppen, konsequent zu löschen. Wir plädieren zur Ermittlung von Täter*innen u.a. für den Einsatz der so genannten Log-In-Falle, bei der anlassbezogen die Identität von Nutzenden festgehalten wird. Alternativ befürworten wir eine anlassbezogen sowohl zeitlich als auch vom Umfang her eng umgrenzte Speicherung von Adressdaten (Quickfreeze), um Ermittler*innen eine verlässliche Chance zu geben. Dafür sind eine entsprechende Rechtsgrundlage sowie auch deutlich verbesserte personelle Ressourcen bei Strafverfolgungsbehörden unabdingbar. Ebenso müssen passende Technologien zur digitalen Beweissicherung zur Verfügung gestellt werden. Der Grundsatz für die technischen Maßnahmen zur Beweissicherung muss sein, nicht über die Kommunikation zu gehen.

**Patternanalyse am Beispiel Whatsapp** (siehe Antwort zu Frage 5)

**Kinderfreundliches Design und Pflichthinweise an Kinder inklusive Beratungs- und Hilfsangeboten**

[17] Vertiefende Informationen zur Loginfalle- https://d-64.org/login-falle/
[18] Vertiefende Informationen zum Thema Quickfreeze:- https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2010/22_QuickFreezeStattVorratsdatenspeicherung.html- Quickfreeze

Neben den technischen Möglichkeiten, Video- und Bildmaterial, das sexualisierte Gewalt an Kindern darstellt, zu löschen und die Täter*innen zu ermitteln, ist grundsätzlich (im Einklang mit dem General Comment 25 der UN-KRK) eine kinderfreundliche Gestaltung von Webseiten und Apps wünschenswert.

Zum einen könnten Webseiten dazu verpflichtet werden, zusätzlich zu AGBs, Datenschutz und Impressum, kindgerechte Informationen (in leichter Sprache) darüber vorzuhalten und kindgerecht anzubieten, was auf der Webseite abgebildet wird und wozu die Website da ist. Diese Informationen können auch Eltern dabei helfen, besser einschätzen zu können, womit ihre Kinder konfrontiert werden. Zum anderen sollten Plattformen, die primär von Minderjährigen verwendet werden, niedrigschwellige Melde-, Abhilfe- und Beschwerdemechanismen anbieten (vgl. Erwägungsgrund 89 DSA). Dazu gehört, dass für Minderjährige klar ersichtlich ist, an wen sie sich wenden können, sollten sie sich verunsichert fühlen. Dies kann z.B. ein Chat sein, der 24 Stunden durch Fachpersonal besetzt ist. Dessen Verfügbarkeit und Kompetenz könnte durch Kinderschutzorganisationen abgesichert werden.

Weiter sollte zusätzlich gut verständlich deutlich gemacht werden, welches passende Hilfsangebote für die jeweilige Situation sind (situation based services) (zentrale nationale Stelle, die Zuweisung zu Hilfsorganisationen sicherstellt).[19]

**15. Der Verordnungsentwurf sieht auch die Möglichkeit von Netzsperren einzelner URLs vor, die im Zuge der bisherigen Entwurfsänderungen während der tschechischen Ratspräsidentschaft sogar noch ausgeweitet werden sollen. Halten Sie es angesichts der weit verbreiteten https-Verschlüsselung von URL-Abrufen für technisch möglich, einzelne URLs gezielt zu sperren, ohne auf die Sperrung ganzer Domains zurückzugreifen, wenn ja, auf welche Weise soll dies möglich sein und wenn nein, können Netzsperren auf diese Weise den Anforderungen des europäischen Gerichtshofs an die Zielgerichtetheit von Netzsperren genügen?**

Netzsperren sind allenfalls ein allerletztes Mittel – wir glauben, dass technisch bewanderte Nutzer*innen sie umgehen können. Besser wäre es, das Material zu löschen. Wir würden darüber reden, Einrichtungen für den Internet-Access grundsätzlich in einer kindersicheren Version ausliefern zu lassen und dies an Alterskennzeichnungen der Inhalte und Interaktionsmöglichkeiten zu binden. Das würde den Eltern die Beschäftigung mit Kinderschutzsoftware und deren Installation auf verschiedenen Geräten ersparen.

## Das EU-Zentrum II

**16. Wie bewerten Sie die Rolle und den Charakter des laut EU-Verordnungsentwurf geplanten EU-Zentrums einerseits mit Blick auf die Wahrnehmung primär präventiver Aufgaben und andererseits mit Blick auf Aufgaben, die die Entwicklung und den Einsatz technischer Überwachungswerkzeuge betreffen?**

Die Rahmung für Prävention sehen wir eher nicht beim EU-Zentrum; aber die Bereitstellung von Informationen, Forschungsergebnissen und Erkenntnissen für die Erarbeitung von Präventionsangeboten

[19] Vertiefende Gedanken und Hintergründe dazu finden Sie auch in diesem Papier (siehe vor allem Seite 7): https://www.cl.cam.ac.uk/~rja14/Papers/chatcontrol.pdf

sind willkommen. Es muss ohnehin eine enge Koordination der verschiedenen Aspekte des Kampfes gegen sexualisierte Gewalt (und nicht nur auf den Kampf gegen die Verbreitung von Darstellungen sexualisierter Gewalt fokussiert werden) geben. Das EU-Zentrum sehen wir stark fokussiert auf

- die Aufdeckung und Löschung des Materials,
- den Kampf gegen die Verbreitung,
- Mithilfe (Erkenntnisse, Technik, Finanzierung) bei der Ermittlung der Täter*innen und der Beweisführung und -sicherung,
- den Kampf gegen die damit und mit Cyber-Grooming verbundenen Versuche, digital neue Taten vorzubereiten
- Mithilfe bei der Verbesserung präventiver Angebote, aber auch bei besserer Unterstützung Betroffener
- Mithilfe bei rechtlichen Rahmungen

**17. Wenn nicht die Endgeräte, sondern die mit ihnen mögliche Kommunikationen („Chats“) durchsucht würden, gälte das auch für eine Ende-zu-Ende-Verschlüsselung etwa von Messenger-Diensten. Auch hier gerieten ungezählte gesetzestreue Bürger ins Visier der Behörden, nur weil sie einen bestimmten Dienst mit entsprechender Software nutzen. Sind Ihnen Software-Lösungen bekannt, die das Echtzeit-Mitlesen oder zumindest das Knacken Ende-zu-Ende-verschlüsselter Kommunikation erlauben? Halten Sie es für vertretbar, die grundgesetzlich garantierte vertrauliche private Kommunikation durch Algorithmen aufzuheben?**

Derzeit sind uns derartige Technologien nicht bekannt.

Wie bereits mehrfach festgehalten: Wir halten es nicht für vertretbar, die Ende-zu-Ende-verschlüsselte Kommunikation in garantiert vertraulicher privater Kommunikation durch Algorithmen aufzuheben. Anlasslose Scans von verschlüsselter Kommunikation sind unverhältnismäßig und nicht zielführend. Das Recht auf Privatsphäre ist ein Grundrecht aller Menschen, auch von Kindern. Siehe zum Thema Privatsphäre die Antwort auf Frage 1.

Die sog. „Chatkontrolle“ ist aus Sicht des Kinderschutzbundes nicht zielführend. Der Kinderschutzbund hält den Scan von Kommunikation für einen unverhältnismäßig großen Eingriff in die Privatsphäre der Bürgerinnen und Bürger – und vor allem der Kinder –, der nicht der gebotenen Abwägung unterschiedlicher Grundrechte entspricht.

**18. Im Verordnungsentwurf heißt es, das zu gründende Zentrum für Fragen des sexuellen Kindesmissbrauchs in Den Haag solle verbindliche Indikatoren für Abbildungen sexuellen Missbrauchs liefern, die von den scannenden Unternehmen anzuwenden seien. Nun wissen erfahrene Ermittler*innen, dass es keineswegs eindeutig zu definieren und im Einzelfall zu belegen ist, aufgrund welcher Kriterien was als Familienfoto, als selbstdokumentiertes Spiel unter Kindern und Jugendlichen, als Zufallsschnappschuss einer Sportveranstaltung oder eben als Kinderpornografie zu gelten hat. Gibt es bereits Erkenntnisse über das methodische**

**Vorgehen des genannten EU-Zentrums? Und falls ja, kann dieses Vorgehen gegebenenfalls als verlässlich und geeignet eingeschätzt werden?**

Bevor das EU-Zentrum überhaupt eingerichtet ist, können wir kaum über das methodische Vorgehen urteilen.

Wir können an dieser Stelle noch einmal mit Nachdruck darauf verweisen, dass eine rein technische Lösung, die auf die Zuverlässigkeit einer KI baut, nicht zielführend ist, denn die Fehleranfälligkeit ist zu hoch und gerade bei derartigen Unterscheidungen bedarf es stets eine fachlich kompetente Einschätzung trainierten Personals. Siehe dazu auch die Antwort auf Frage 5. Ermittler*innen sagen uns aber, dass in der Regel neues Material da zu finden ist, wo man auch altes entdeckt hat. KI kann dahingehend trainiert werden im bisherigen Umfang zu scannen und somit dazu beitragen, verdächtiges neues Material zu finden. Das EU-Zentrum kann zudem helfen, die jeweils besten Methoden (und Programme) HERSTELLERUNABHÄNGIG zu ermitteln.

---

**Berlin, 27.02.2023**

**Der Kinderschutzbund Bundesverband e.V.**
Schöneberger Str. 15
10963 Berlin
Tel (030) 21 48 09-0
Fax (030) 21 48 09-99
E-Mail info@kinderschutzbund.de
www.kinderschutzbund.de

---