ECPAT Deutschland e.V.
Arbeitsgemeinschaft zum Schutz der Kinder vor sexueller Ausbeutung

Stellungnahme ECPAT Deutschland e.V.

Unabhängige Expertenkommission "Kinder- und Jugendschutz in der digitalen Welt"

Hearing 2 – Technischer Jugendmedienschutz, Plattformgestaltung und Verantwortung digitaler Dienste

– mit der Bitte um verbindliche Rückmeldung bis zum 6. Februar 2026 –

Teilnahme am Hearing 2 – Technischer Jugendmedienschutz, Plattformgestaltung und Verantwortung digitaler Dienste

am Freitag, 13. Februar 2026, 9:00 bis 12:00 Uhr, digital

⊗ **ja** ◯ **nein, nur schriftliche Stellungnahme** ◯ **nein, weder Teilnahme noch Stellungnahme**

Name der/des Teilnehmenden: Lea Peters

Name der Organisation: ECPAT Deutschland e.V.

Die Einwahldaten erhalten Sie in der Woche des Hearings.

LEITFRAGE

Welche Kombination aus technischen, regulatorischen und pädagogischen Maßnahmen ist aus Ihrer fachlichen Sicht am wirksamsten, um Kinder und Jugendliche im digitalen Raum zu schützen und ihre Teilhabechancen zu stärken?

I Risiken, Schutzmaßnahmen und Gestaltung digitaler Dienste

1. Welche Maßnahmen sind aus Ihrer Sicht am wirksamsten, um die folgenden Risiken für Kinder und Jugendliche in digitalen Diensten zu verhindern, zu erschweren oder in ihren Folgen zu begrenzen:

a. digitale sexualisierte Gewalt (z.B. Cybergrooming, Sextortion, Missbrauchsdarstellungen),

Kinder und Jugendliche sind im digitalen Raum einer Vielzahl unterschiedlicher Formen sexualisierter Gewalt ausgesetzt. Dazu zählen unter anderem Cybergrooming, sexuelle Erpressung (sowohl sexuell als auch finanziell motiviert), sexuelle Belästigung und Nötigung, Darstellungen sexualisierter Gewalt an Kindern (CSAM), KI-generiertes CSAM wie Deepnudes oder synthetisches CSAM, sexuelle Ausbeutung durch Livestreaming, sogenannte „Taschengeld-Treffen“ sowie die (ungewollte) Konfrontation mit pornographischen Inhalten. Diese Risiken unterscheiden sich hinsichtlich ihrer Erscheinungsformen, Dynamiken und Folgen, weisen jedoch gemeinsame strukturelle Ursachen auf, etwa asymmetrische Machtverhältnisse, fehlende Schutzmechanismen und kommerzielle Anreizsysteme digitaler Dienste.

Die wirksame Prävention, Aufdeckung und Begrenzung der Folgen digitaler sexualisierter Gewalt erfordert daher einen ganzheitlichen Ansatz, der über isolierte Einzelmaßnahmen hinausgeht. Voraussetzung ist das koordinierte Mitwirken aller relevanten Akteur*innen, darunter zivilgesellschaftliche Organisationen, pädagogische Fachkräfte, Strafverfolgungsbehörden und Justiz, Technologie Unternehmen, Jugendämter, Träger der Kinder- und Jugendhilfe, Meldestellen sowie spezialisierte Fachberatungsstellen. Zentrale

Verantwortung tragen jedoch die Anbieter digitaler Dienste, da sie die strukturellen Rahmenbedingungen schaffen, in denen Risiken entstehen oder begrenzt werden können.

Folgende Maßnahmen sehen wir als essenziell zur Prävention, Aufdeckung und Bekämpfung sexualisierter Gewalt gegen Kinder und Jugendliche in digitalen Räumen:

Gezielte und verpflichtende Risikobewertungen

Zu den wirksamsten Maßnahmen zählt die systematische Durchführung gezielter Risikobewertungen. Gesetzliche Vorgaben und Leitlinien sollten Plattformbetreiber verpflichten, ihre Dienste bereits vor der Markteinführung einer fundierten Risiko- und Folgenabschätzung zu unterziehen, die spezifisch die Risiken sexualisierter Gewalt gegen Kinder und Jugendliche berücksichtigt. Darüber hinaus sind regelmäßige, fortlaufende Risikoanalysen erforderlich, die sowohl bestehende Risiken als auch die Auswirkungen neu eingeführter Funktionen, Features oder algorithmischer Veränderungen erfassen. Diese Analysen sollten nicht nur potenzielle Gefährdungen identifizieren, sondern auch die Wirksamkeit bereits ergriffener Maßnahmen zur Risikominimierung evaluieren und gegebenenfalls Anpassungen erforderlich machen. Besonders relevant ist eine frühzeitige Prüfung neuer Funktionen, bevor diese flächendeckend ausgerollt werden, um risikoverstärkende Effekte von vornherein zu vermeiden.

Child-Rights-by-Design als verbindlicher Gestaltungsansatz

Ein weiterer zentraler Hebel liegt in der konsequenten Umsetzung eines Child-Rights-by-Design-Ansatzes. Verantwortungsvolle digitale Dienste berücksichtigen bei Design, Entwicklung und Weiterentwicklung systematisch alle Kinderrechte, wie sie in der UN-Kinderrechtskonvention verankert sind. Neben dem Schutzrecht umfasst dies auch Befähigungs- und Teilhaberechte. Auf dieser Grundlage hat die britische 5Rights Foundation[1] elf Prinzipien für kindgerechtes Design entwickelt, die unter anderem Gerechtigkeit und Vielfalt, die Berücksichtigung des Kindeswohls, die Einbeziehung von Kindern und Jugendlichen in technische Entwicklungsprozesse, altersgerechte Gestaltung, Datenschutz und Privatsphäre, Sicherheit, Wohlbefinden, Förderung von Entwicklung sowie die Stärkung der Handlungsfähigkeit von Kindern und Jugendlichen umfassen.

Die praktische Umsetzung dieser Prinzipien bedeutet unter anderem, dass Sicherheits- und Schutzmechanismen integraler Bestandteil der Produktgestaltung sein müssen und nicht nachträglich ergänzt werden. Altersgerechte Voreinstellungen, transparente und verständliche Nutzeroberflächen, wirksame Privatsphäre-Einstellungen sowie klare und leicht zugängliche Melde- und Abhilfewege sind dabei ebenso relevant wie die Vermeidung von Designentscheidungen, die Risiken verstärken.

Begrenzung und ggfls. Verbote risikoverstärkender Geschäftsmodelle und Designs

Besondere Bedeutung kommt der Regulierung süchtig machender Designs und manipulativer algorithmischer Systeme zu, die Aufmerksamkeit maximieren, Interaktionen erzwingen oder riskantes Verhalten begünstigen. Solche Mechanismen können die Anbahnung sexualisierter Gewalt erleichtern, indem sie Kontaktaufnahmen fördern, Sichtbarkeiten verzerren oder Hemmschwellen senken. Ein Verbot oder zumindest eine strikte Begrenzung dieser Designs ist daher ein wesentlicher Bestandteil wirksamer Prävention. Voraussetzung hierfür sind umfassende Transparenzpflichten, die es Aufsichtsbehörden und unabhängigen Stellen ermöglichen, Funktionsweisen, Risiken und Auswirkungen algorithmischer Systeme zu prüfen.

b. suchtbegünstigende/hochgradig bindende Gestaltungspraktiken (z.B. Mikrotransaktionen, Lootboxen/Zufallsmechaniken, Dark Patterns),

Diese Mechanismen nutzen gezielt entwicklungsbedingte Vulnerabilitäten von Minderjährigen aus, etwa eine geringere Impulskontrolle, ein ausgeprägtes Bedürfnis nach sozialer Anerkennung oder ein eingeschränktes Verständnis für wirtschaftliche Zusammenhänge.

Mikrotransaktionen sind dabei nicht nur aus jugendschutzrechtlicher Sicht problematisch, sondern stehen häufig in einem direkten Zusammenhang mit weiteren Risiken wie Cybergrooming, sexueller digitaler

Erpressung oder sexueller Ausbeutung. In verschiedenen Konstellationen werden finanzielle Zuwendungen, digitale Geschenke oder In-Game-Käufe gezielt eingesetzt, um Vertrauen aufzubauen, Abhängigkeiten zu erzeugen oder Gegenleistungen zu erwarten.

Lootboxen und vergleichbare Zufallsmechaniken verstärken diese Risiken zusätzlich, da sie suchtfördernde Elemente enthalten und wiederholte Ausgaben begünstigen. Dark Patterns, etwa voreingestellte Kaufoptionen, irreführende Gestaltung von Abbruchmöglichkeiten oder sozialer Druck durch Ranglisten und Belohnungssysteme, erschweren es Kindern und Jugendlichen, informierte und selbstbestimmte Entscheidungen zu treffen. Gleichzeitig können solche Designs die Bereitschaft erhöhen, auf Forderungen Dritter einzugehen oder riskante Interaktionen einzugehen, um finanzielle Mittel zu generieren.

Zur wirksamen Prävention dieser Risiken sind klare regulatorische Vorgaben erforderlich, die suchtbegünstigende und manipulative Gestaltungspraktiken gegenüber Minderjährigen untersagen oder zumindest erheblich begrenzen. Dazu gehören transparente Kostenstrukturen, strikte Alters- und Ausgabenbeschränkungen, das Verbot irreführender Designpraktiken sowie eine konsequente Berücksichtigung von Child-Rights-by-Design-Prinzipien. Kommerzielle Interessen dürfen nicht zulasten der Handlungsfähigkeit, der finanziellen Sicherheit und des Schutzes von Kindern und Jugendlichen gestellt werden.

c. Hate Speech, Desinformation sowie verschwörungsideologische und extremistische Inhalte,

Hate Speech, Desinformation sowie verschwörungsideologische und extremistische Inhalte stellen eigenständige Risiken für Kinder und Jugendliche im digitalen Raum dar und können zugleich geschlechtsspezifische Gewalt sowie sexualisierte digitale Gewalt begünstigen. Abwertende, entmenschlichende oder sexualisierte Narrative tragen dazu bei, Grenzverletzungen zu normalisieren, Gewalt zu legitimieren oder Betroffene zu diskreditieren. Desinformation und verschwörungsideologische Inhalte können zudem bestehende Stereotype verstärken, Feindbilder aufbauen und Vertrauen in Schutz- und Hilfestrukturen untergraben.

Besonders gefährdet sind Kinder und Jugendliche aus vulnerablen Gruppen, etwa aufgrund ihres Geschlechts, ihrer sexuellen Orientierung, ihrer geschlechtlichen Identität, ihrer ethnischen Zugehörigkeit, einer Behinderung oder ihrer sozialen Situation. Sie werden häufig Ziel von Hassrede, gezielten Anfeindungen oder sexualisierten Angriffen und sind damit einem erhöhten Risiko psychischer Belastungen und sozialer Ausgrenzung ausgesetzt. Extremistische Inhalte können diese Dynamiken weiter verschärfen, indem sie Gewalt legitimieren oder ideologisch aufladen.

Zur Prävention und Begrenzung dieser Risiken sind klare Community-Standards, wirksame Moderation sowie altersgerechte Schutzmechanismen erforderlich. Darüber hinaus ist es notwendig, Kinder und Jugendliche in ihrer Medienkompetenz zu stärken, um sie beim Erkennen von Hass, Desinformation und extremistischen Narrativen zu unterstützen und ihre Resilienz gegenüber solchen Inhalten zu fördern.

d. Belästigung/Cybermobbing und weitere Interaktionsrisiken (z. B. Doxxing, Stalking, koordinierte Angriffe),

Belästigung und Cybermobbing stellen für Kinder und Jugendliche erhebliche Risiken im digitalen Raum dar und treten häufig nicht isoliert auf, sondern in Wechselwirkung mit weiteren Formen digitaler Gewalt. Belästigung weist dabei nicht selten eine sexualisierte Komponente auf. Dazu zählen unter anderem sexualisierende, objektifizierende oder entwürdigende Kommentare unter Beiträgen, Bildern, Videos oder Livestreams von Kindern und Jugendlichen, ebenso wie unerwünschte Direktnachrichten mit sexualisiertem Inhalt. Solche Interaktionen können für Betroffene stark belastend sein, das Sicherheitsgefühl nachhaltig beeinträchtigen und als Einstieg oder Normalisierung weiterer Formen sexualisierter Gewalt wirken.

Darüber hinaus sind Phänomene wie Doxxing, Stalking oder koordinierte Angriffe häufig Teil gezielter Täterstrategien. Das Veröffentlichen oder Androhen der Veröffentlichung persönlicher Daten kann eingesetzt werden, um Druck auszuüben, Kontrolle zu erlangen oder Betroffene einzuschüchtern. Stalking,

sowohl innerhalb einzelner Plattformen als auch plattformübergreifend, ermöglicht eine kontinuierliche Überwachung und Kontaktaufnahme, die Grenzen zwischen Online- und Offline-Raum verwischen kann. Insbesondere im Kontext sexualisierter Gewalt dienen diese Strategien häufig der Machtausübung, der Vorbereitung weiterer Übergriffe oder der Durchsetzung von Schweige- und Abhängigkeitsverhältnissen. Sie können damit eine Vorstufe bilden auch für Straftaten im Bereich Ausbeutung und Menschenhandel.

Koordinierte Angriffe, etwa durch Gruppen oder Netzwerke, verstärken diese Risiken zusätzlich. Sie können dazu führen, dass einzelne Kinder oder Jugendliche massenhaft mit beleidigenden, sexualisierten oder bedrohenden Inhalten konfrontiert werden, was die psychische Belastung erheblich erhöht, und effektive Gegenwehr erschwert. Solche Dynamiken werden durch bestimmte Plattformmechanismen, etwa hohe Sichtbarkeit von Inhalten, algorithmische Verstärkung oder unzureichende Moderation, begünstigt.

Zur wirksamen Prävention und Begrenzung dieser Risiken sind klare Verhaltensregeln, konsequente Moderation und leicht zugängliche Melde- und Abhilfewege erforderlich. Ebenso wichtig ist die frühzeitige Erkennung eskalierender Interaktionsmuster, um Belästigung, Mobbing und sexualisierte Gewalt nicht erst dann zu adressieren, wenn sie bereits erhebliche Schäden verursacht haben. Belästigung und Cybermobbing sind daher nicht als „minderschwere“ Phänomene zu behandeln, sondern als ernstzunehmende Risikofaktoren, die eng mit weiteren Formen digitaler Gewalt gegen Kinder und Jugendliche verknüpft sind.

e. Selbstgefährdungsrisiken (z. B. Selbstschädigung/Suizid, Essstörungen, gefährliche Challenges),

Ausbeutung von und Handel mit Kindern und Jugendlichen werden immer stärker von Digitalisierungsprozessen geprägt und verändern dadurch fortwährend ihre Ausprägungsformen. Sogenannte „Taschengeld-Treffen“ stellen eine neuere Form der sexuellen Ausbeutung von Kindern und Jugendlichen dar und verbinden sexuelle Ausbeutung im digitalen und analogen Raum. „Taschengeld-Treffen“ sind Verabredungen, bei denen sexuelle Handlungen gegen geringe Geldbeträge oder Geschenke angeboten werden – meist über Online-Anzeigenportale oder soziale Medien. Die sexuelle Ausbeutung findet sowohl physisch in Wohnungen, Hotels oder Parks, als auch digital über das Teilen von Fotos, Videos oder in Livestreams statt. In einigen Fällen erfahren Betroffene von Gleichaltrigen von diesen „Taschengeld-Treffen“.[2]

Bei der Umsetzung von mehr Kinderschutz im digitalen Raum stehen Politik und Privatwirtschaft in der Verantwortung. Denn besonders alarmierend ist, dass Anzeigen für diese Form der sexuellen Ausbeutung nicht nur auf Dating-Apps und Erotikportalen geschaltet werden – zu denen Kinder und Jugendliche ohne Probleme Zugang haben – sondern vor allem auch auf allgemeinen Anzeigenportalen geschaltet oder über Social Media Plattformen angebahnt werden.

Daher braucht es mindestens eine verpflichtende und effektive Altersverifikation für digitale Angebote aus dem Bereich Dating und Erotik sowie wirksame Haftungsmechanismen für Plattformbetreibende. Darüber hinaus braucht es mehr Ressourcen für digitale Melde- und Beratungsstellen, als auch den Ausbau und die Förderung von Digital Street Work.

Sexuelle Erpressung, insbesondere finanziell motivierte, stellt weiterhin eine erhebliche Gefahr dar, vor allem für Kinder und Jugendliche. 2023 erhielt das National Center for Missing and Exploited Children (NCMEC) durchschnittlich 812 Meldungen pro Tag, ein Großteil davon mit finanziellem Hintergrund. Täter(*innen) setzen verschiedene Druckmittel ein, zentral ist die Drohung, intime Bilder zu verbreiten. Die Angst vor dieser Veröffentlichung kann schwerwiegende Folgen bis hin zu Suizid haben.

Am häufigsten erfolgt der Kontakt über Instagram und Snapchat, zunehmend aber auch über Ende-zu-Ende-verschlüsselte Messenger, auf die Opfer gezielt verlagert werden. Als Zahlungsmittel werden oft Cash App und Geschenkkarten genutzt. Viele Fälle stehen offenbar im Zusammenhang mit organisierter Kriminalität, insbesondere mit Gruppen aus Nigeria und Côte d’Ivoire. Meldungen zeigen wiederkehrende

Muster wie identische Sprache, Skripte und Profilbilder.

Entscheidend ist unter anderem die Stärkung schneller Interventionsmechanismen. Maßnahmen im Bereich sexualisierter Gewalt sollten nicht allein auf Aufdeckung ausgerichtet sein, sondern insbesondere auf frühzeitige Intervention. Dies ist vor allem bei finanziell motivierter sexueller Erpressung entscheidend, da Eskalationen häufig innerhalb kürzester Zeit erfolgen und bis zu Selbstgefährdung oder Suizid führen können. Dies kann bspw. über den Einsatz technischer Erkennungssysteme umgesetzt werden, die typische Grooming- und Erpressungsskripte erkennen. Ziel muss sein, Betroffenen in akuten Risikosituationen automatisiert und niedrigschwellig Unterstützung, Schutzoptionen und Meldewege anzubieten.

Auch proaktive Schutzmaßnahmen im Präventionsbereich sind essenziell. Die Identifikation und Sperrung potenzieller Fake-Profile sowie von Accounts, die in auffälligem oder überproportionalem Umfang Minderjährige kontaktieren, sollte systematisch ausgebaut werden. Solche Maßnahmen können präventiv dazu beitragen, riskante Kontaktanbahnungen frühzeitig zu unterbinden.

f. **kommerzielle Ausnutzung sowie Daten- und Privatsphäre-Risiken (z. B. Profiling/Tracking, irreführende Werbung, Scams)?**

Kinder und Jugendliche sind im digitalen Raum in besonderem Maße Risiken der kommerziellen Ausnutzung ausgesetzt. Ein zentrales Problem stellt dabei die gezielte oder indirekte Werbung für schädliche und jugendgefährdende Inhalte dar. Hierzu zählen insbesondere pornographische oder erotische Angebote, die über klassische Werbeanzeigen, Empfehlungsmechanismen oder scheinbar harmlose Verlinkungen verbreitet werden. Auch Werbung für Plattformen wie OnlyFans oder sogenannte Sugar-Dating-Webseiten fällt in diesen Bereich, da sie Geschäftsmodelle bewerben, die auf sexualisierten Darstellungen, asymmetrischen Machtverhältnissen oder finanziellen Abhängigkeiten beruhen und für Minderjährige grundsätzlich ungeeignet sind.

Diese Werbeformen sind häufig eng mit datengetriebenem Profiling und Tracking verknüpft. Durch die Auswertung von Nutzungsverhalten, Interessen oder Interaktionsmustern können Kinder und Jugendliche gezielt mit sexualisierten oder grenzüberschreitenden Inhalten konfrontiert werden, ohne dass ihnen die zugrunde liegenden Mechanismen transparent oder verständlich sind. Dies erhöht nicht nur das Risiko einer frühzeitigen oder unfreiwilligen Sexualisierung, sondern kann auch die Anbahnung sexualisierter Gewalt erleichtern, etwa durch die Normalisierung bestimmter Inhalte oder durch Weiterleitungen auf externe, unzureichend regulierte Angebote.

Darüber hinaus weisen solche Werbestrategien häufig irreführende Elemente auf, etwa durch verschleierte Altersangaben, emotionalisierte Ansprache oder Versprechen von Anerkennung, Einkommen oder Zugehörigkeit. In Kombination mit unzureichenden Altersverifikationsmechanismen entsteht so ein erhebliches Risiko, dass Minderjährige in kommerzielle oder ausbeuterische Strukturen hineingezogen werden. Auch Scams und betrügerische Angebote mit sexualisiertem Bezug können auf diese Weise verbreitet werden und zu finanziellen, emotionalen oder sozialen Schäden führen.

Der DSA verbietet, Minderjährigen sexualisierte oder jugendgefährdende Werbung anzuzeigen sowie Profiling zu Werbezwecken bei Minderjährigen. Verstöße gegen diese Vorgaben müssen konsequent überwacht, verfolgt und sanktioniert werden. Dafür ist ein verlässliches Monitoring erforderlich. Plattformbetreiber sollten verpflichtet werden, wirksame Alters- und Zielgruppenschutzmechanismen einzusetzen und transparent offenzulegen, welche Werbeinhalte ausgespielt werden und nach welchen Logiken dies erfolgt. Kommerzielle Interessen dürfen nicht zulasten der Rechte, der Privatsphäre und des Wohlergehens von Kindern und Jugendlichen gehen.

2. **Welche Rolle spielen dabei konkrete Gestaltungsentscheidungen von Diensten (z.B. Default-Einstellungen, Empfehlungs- und Rankingsysteme, Sharing-/Kontaktfunktionen, Interface-Design, Parental-Control-Funktionen)?**

Registrierung und Authentifizierung haben einen erheblichen Einfluss darauf, ob und wie Minderjährige einen Dienst sicher, altersgerecht und unter Wahrung ihrer Rechte nutzen können. Sie können Schutz bieten, dürfen jedoch keine unnötigen Hürden schaffen oder zu zusätzlichen Risiken für Privatsphäre und Teilhabe führen. Eine zentrale Rolle spielen dabei schützende Standardeinstellungen, die das Risiko unerwünschter Kontakte deutlich reduzieren können. So sollten Interaktionen wie Likes, Tags, Kommentare, Direktnachrichten oder Reposts grundsätzlich nur durch zuvor akzeptierte Kontakte möglich sein. Auch Funktionen wie Screenshots oder die Weitergabe von Kontaktinformationen sollten eingeschränkt werden, um Missbrauch vorzubeugen.

Darüber hinaus ist sicherzustellen, dass Minderjährige selbstbestimmt entscheiden können, wie sie einen Dienst nutzen möchten. Das Design digitaler Angebote muss altersgerechte Erfahrungen ermöglichen und darf keine Gestaltungsmechanismen enthalten, die gezielt auf exzessive Nutzung, Abhängigkeit oder andere problematische Verhaltensweisen abzielen. Wirksame Moderation ist ein weiterer zentraler Schutzfaktor, da sie das Risiko verringert, dass Minderjährige mit problematischen oder illegalen Inhalten konfrontiert werden, und zugleich zur Prävention von Straftaten beitragen kann. Kritisch zu betrachten ist dabei, dass viele Dienste ihre Plattformen gezielt auf eine möglichst hohe Nutzungsdauer und Interaktionsdichte ausrichten. Diese Logiken stehen häufig im Widerspruch zu den Rechten und dem Schutz von Kindern und Jugendlichen und müssen entsprechend begrenzt werden.

3. **Wie können Diensteanbieter algorithmisch verstärkte Risiken (z.B. durch KI-basierte Empfehlungen und Profiling) erkennen, bewerten und wirksam mindern?**

Empfehlungssysteme steuern maßgeblich, welche Inhalte priorisiert, verstärkt oder ausgeblendet werden, und können bestehende Risiken für Kinder und Jugendliche erheblich verschärfen. Daher müssen diese Systeme transparent ausgestaltet und regelmäßig im Hinblick auf ihre Auswirkungen auf Minderjährige überprüft, getestet und angepasst werden. Ziel ist es, die Privatsphäre, Sicherheit und den Schutz vor Gefährdungen wirksam zu stärken und risikoverstärkende Dynamiken frühzeitig zu erkennen und zu begrenzen.

Kinder und Jugendliche sind den beeinflussenden Effekten digitaler Geschäftsmodelle in besonderem Maße ausgesetzt und haben ein Recht darauf, vor wirtschaftlich ausbeuterischen Praktiken geschützt zu werden. Online-Plattformen sind entsprechend so zu gestalten, dass Minderjährige keinen finanziellen Risiken ausgesetzt werden, etwa durch manipulative Kaufanreize, intransparente Kostenstrukturen oder gezieltes Profiling zu kommerziellen Zwecken.

Darüber hinaus sind Kinder und Jugendliche im digitalen Raum auch dem Risiko der Anbahnung von Menschenhandel und sexueller Ausbeutung ausgesetzt. Profiling sowie KI-gestützte Empfehlungssysteme können diese Gefährdungen verstärken, indem sie Kontaktanbahnungen erleichtern, vulnerables Verhalten identifizieren oder Täterstrategien begünstigen. Auch diesem Risiko muss durch klare regulatorische Vorgaben, präventive Systemgestaltung und wirksame Schutzmechanismen begegnet werden.

4. **Benennen Sie nach Möglichkeit Prioritäten (Top-3-Maßnahmen) und Kriterien/Indikatoren, wie die Wirksamkeit von Maßnahmen überprüft wird/werden sollte.**

(1) Verbindliche Risiko- und Kinderrechtsfolgenabschätzungen

Als zentrale Priorität ist die verpflichtende Durchführung von Child Rights Impact Assessments sowie konkreter Risikoanalysen zu nennen, die die unterschiedlichen Risikobereiche – insbesondere sexualisierte Gewalt und Ausbeutung – systematisch erfassen. Diese Analysen müssen vor der Einführung neuer Dienste oder Funktionen sowie regelmäßig im laufenden Betrieb erfolgen. Zwingend erforderlich ist dabei die strukturierte Beteiligung von Kindern und Jugendlichen sowie von Betroffenen, um reale Nutzungserfahrungen, Schutzlücken und unbeabsichtigte Effekte zu identifizieren.

Indikatoren für Wirksamkeit sind unter anderem die Qualität und Nachvollziehbarkeit der Analysen, die dokumentierte Berücksichtigung der Beteiligungsergebnisse sowie die konkrete Ableitung und Umsetzung

von risikominimierenden Maßnahmen.

(2) Rechtlich verbindliche Mindeststandards für den Kinder- und Jugendmedienschutz

Eine weitere zentrale Maßnahme ist die rechtlich verbindliche Festlegung und Durchsetzung von Mindeststandards für den Kinder- und Jugendmedienschutz, die für alle relevanten Anbieter gelten. Diese Standards sollten klare Anforderungen an altersgerechte Gestaltung, Schutzmechanismen, Moderation, Melde- und Abhilfewege sowie risikoreduzierende Designs enthalten.

Die Wirksamkeit lässt sich unter anderem anhand der Umsetzung dieser Standards in Produktdesign und Unternehmensprozessen, der Anzahl und Art festgestellter Verstöße sowie der Durchsetzungs- und Sanktionspraxis der Aufsichtsbehörden überprüfen.

(3) Kontinuierliches Monitoring, Analyse und Transparenz

Als dritte Priorität ist ein kontinuierliches Monitoring der Risiken und der Wirksamkeit ergriffener Maßnahmen zu benennen. Plattformbetreiber sollten verpflichtet werden, regelmäßig strukturierte Berichte zu veröffentlichen, die Risiken, getroffene Maßnahmen und deren Wirkung transparent darstellen. Dieses Monitoring sollte durch die Konsultation externer, unabhängiger Expert*innen ergänzt werden, um eine fachlich fundierte und kritische Bewertung sicherzustellen.

Indikatoren sind hier unter anderem die Regelmäßigkeit und Qualität der Berichte, die Einbindung externer Expertise sowie nachvollziehbare Anpassungen von Maßnahmen auf Grundlage der gewonnenen Erkenntnisse.

II Plattformverantwortung, Regulierung und Durchsetzung

1. Wie sollte die Verantwortung der Plattformbetreiber gegenüber Kindern und Jugendlichen rechtlich und praktisch konkretisiert werden (z.B. Sorgfaltspflichten, Risikoanalysen, Melde- und Abhilfewege, Transparenzpflichten)?

Melde- und Abhilfewege

Plattformbetreiber tragen eine zentrale Verantwortung für die Ausgestaltung wirksamer, niedrigschwelliger und kindgerechter Melde- und Abhilfewege. Unterstützungsangebote und Helplines für (potenzielle) Betroffene oder deren Familien und Freund*innen sind von höchster Bedeutung und müssen systematisch gestärkt und barrierearm gestaltet werden sowie leicht bei der Nutzung von Anwendungen und Plattformen auffindbar sein. Meldeverfahren sollten altersgerecht, verständlich und ohne technische oder soziale Hürden nutzbar sein. Insbesondere für Kinder und Jugendliche müssen klare Informationen darüber bereitgestellt werden, welche Schritte nach einer Meldung erfolgen, welche Unterstützung verfügbar ist und wie ihre Rechte gewahrt werden.

Gleichzeitig fehlt bislang weitgehend an Hilfe- und Orientierungsangeboten für (potenzielle) Täter*(innen) sexualisierter Gewalt. Aktuelle Studien und Statistiken weisen darauf hin, dass die Zahl jugendlicher und junger erwachsener Täter*(innen) in diesem Deliktsbereich zunimmt. Vor diesem Hintergrund ist es aus präventiver Sicht notwendig, auch diese Zielgruppe systematisch in Unterstützungs- und Beratungsstrukturen einzubeziehen. Niedrigschwellige, anonyme und nicht-stigmatisierende Angebote können dazu beitragen, Eskalationen frühzeitig zu verhindern und somit einen wichtigen Beitrag zum Schutz von Kindern und Jugendlichen leisten.

Von zentraler Bedeutung ist dabei die Vertrauenswürdigkeit der empfohlenen Unterstützungsangebote. Plattformbetreiber sollten daher verpflichtet werden, mit etablierten, zertifizierten und unabhängigen Diensten zusammenzuarbeiten, beispielsweise innerhalb des INHOPE-Netzwerks. Auf europäischer Ebene könnten zuständige Institutionen die Entwicklung und Pflege einer regelmäßig aktualisierten Liste vertrauenswürdiger Unterstützungsdienste übernehmen und Plattformen bei deren Integration beraten. Ergänzend sollte – soweit möglich – auch auf Peer-to-Peer-Unterstützungsangebote verwiesen werden, da

diese häufig besonders niedrigschwellig sind und von Kindern und Jugendlichen eher in Anspruch genommen werden.

Darüber hinaus muss sichergestellt sein, dass verlinkte oder empfohlene Unterstützungsangebote über ausreichende personelle und finanzielle Ressourcen verfügen, um Minderjährige im Bedarfsfall wirksam begleiten zu können. Ebenso ist ihre institutionelle Unabhängigkeit von einzelnen Plattformbetreibern zu gewährleisten, um Interessenkonflikte zu vermeiden und Vertrauen nicht zu untergraben. Hier wäre bspw. ein Fond-Modell denkbar, d.h. die Plattformen zahlen abhängig von Größe und Prinzip in einen Fond ein, der dazu dient, Unterstützung- und Hilfsstrukturen zu stärken und auszubauen. Melde- und Beratungsstellen erhalten dann finanzielle Ressourcen aus diesem Fond, so können sie gestärkt werden ohne Kompromisse bei ihrer Unabhängigkeit zu machen.

Sorgfaltspflichten

Die Verantwortung von Plattformbetreibern darf sich nicht auf einzelne spezialisierte Unternehmensabteilungen beschränken. Zwar ist eine fundierte Schulung von Mitarbeitenden in Moderationsteams und im Bereich Kinder- und Jugendschutz unabdingbar, darüber hinaus sollten jedoch sämtliche Beschäftigte zumindest über grundlegende Kenntnisse zu Risiken für Minderjährige, insbesondere im Zusammenhang mit sexualisierter Gewalt, verfügen. Dies umfasst sowohl präventive Aspekte als auch das Wissen um interne Melde- und Eskalationsprozesse.

Eine besondere Verantwortung kommt Entwickler*innen, technischen Designer*innen und Software-Programmierer*innen zu, da sie maßgeblich die Strukturen, Funktionen und Anreizsysteme von Plattformen gestalten. Sie sollten verpflichtend in interdisziplinäre Prozesse eingebunden sein und eng mit Fachstellen für Kinderrechte, Prävention und Opferschutz zusammenarbeiten. Ziel muss es sein, Risiken systematisch bereits in der Konzeption neuer Produkte und Funktionen zu identifizieren und zu minimieren. Sicherheits- und Schutzmechanismen für Kinder und Jugendliche sind als integraler Bestandteil eines „Safety- und Child-Rights-by-Design“-Ansatzes zu verstehen und nicht als nachträgliche Korrektur.

Transparenzanforderungen & Risikoanalyse

Transparenz ist von größter Bedeutung, um festzustellen, ob präventive und interventive Maßnahmen gegen sexualisierte Gewalt wirksam sind und um Schutzlücken in den Diensten zu identifizieren. Daher ist es empfehlenswert, Transparenzanforderungen weiter auszuführen und zu verstärken – auch unter Berücksichtigung der erweiterten Anforderungen an sehr große Online-Plattformen im Digital Services Act (DSA).

Plattformbetreiber sollten regelmäßig strukturierte Risikoanalysen durchführen, die alters- und nutzungsspezifische Gefährdungen erfassen und dokumentieren. Die Ergebnisse dieser Analysen sollten in geeigneter Form veröffentlicht und von unabhängigen Stellen überprüfbar sein. Darüber hinaus sollte nicht nur dargelegt werden, welche Maßnahmen und Tools zur Risikominimierung und zur Erhöhung der Sicherheit implementiert wurden, sondern auch einen Überblick über deren beobachtete Wirkung geben. Weiterhin sind Details zu Beteiligungsprozessen von Kindern sowie weiteren Konsultationsprozessen, etwa mit Betroffenen oder Kinderrechtsexperten, sind sowohl für Fachleute als auch für die breite Öffentlichkeit von Interesse.

Nur wenn Prävention, Intervention und Transparenz konsequent zusammengedacht werden, kann die rechtliche und praktische Verantwortung von Plattformbetreibern gegenüber Kindern und Jugendlichen wirksam konkretisiert werden.

2. **Wie lässt sich die Verantwortung der Plattformbetreiber überprüfbar ausgestalten (z.B. Audits, Reporting, unabhängige Aufsicht, Beteiligung von Kindern und Zivilgesellschaft)?**

Damit die Verantwortung von Plattformbetreibern gegenüber Kindern und Jugendlichen nicht auf freiwilligen Selbstverpflichtungen beruht, sondern tatsächlich wirksam und überprüfbar ausgestaltet ist, bedarf es verbindlicher Strukturen zur Evaluation, Kontrolle und Weiterentwicklung der ergriffenen Maßnahmen.

Zentrale Elemente sind hierbei transparente Prüfmechanismen, eine unabhängige Aufsicht sowie die systematische Beteiligung von Kindern, Jugendlichen, Betroffenen und der Zivilgesellschaft.

Beteiligung von Kindern und Jugendlichen

Kinder und Jugendliche sind keine homogene Gruppe und sollten nicht lediglich als Schutzobjekte betrachtet werden, sondern als zentrale Akteur*innen, deren Perspektiven für die Bewertung von Risiken und Schutzmaßnahmen unverzichtbar sind. Plattformbetreiber sollten verpflichtet werden, altersgerechte und kontinuierliche Beteiligungsformate zu etablieren, etwa in Form von Jugendbeiräten, partizipativen Nutzendenbefragungen oder Co-Design-Prozessen bei der Entwicklung neuer Funktionen. Diese Beteiligung muss freiwillig, sicher und angemessen begleitet erfolgen und darf nicht auf symbolische Konsultationen reduziert werden. Die Ergebnisse solcher Beteiligungsprozesse sollten dokumentiert und nachvollziehbar in Risikoanalysen, Produktentscheidungen und Schutzkonzepte einfließen.

Beteiligung von Betroffenen

Ergänzend zur Perspektive von Kindern und Jugendlichen ist die Einbindung von Betroffenen sexualisierter Gewalt von besonderer Bedeutung. Ihre Erfahrungen liefern wertvolle Erkenntnisse darüber, wie Risiken konkret entstehen, welche Schutzmechanismen versagen und welche Unterstützungsangebote tatsächlich wirksam sind. Plattformbetreiber sollten daher in Zusammenarbeit mit spezialisierten Fachstellen sichere und freiwillige Beteiligungsmöglichkeiten für Betroffene schaffen. Dabei ist zwingend sicherzustellen, dass diese Beteiligung nicht retraumatisierend wirkt, angemessen vergütet wird und auf klaren ethischen Standards basiert. Die Einbindung von Betroffenen sollte insbesondere bei der Evaluation bestehender Maßnahmen und der Entwicklung neuer Schutzmechanismen erfolgen.

Zusammenarbeit mit Kinderrechtsexpert*innen

Eine regelmäßige, strukturierte Zusammenarbeit mit unabhängigen Kinderrechts- und Präventionsexpert*innen ist ein weiterer zentraler Baustein überprüfbarer Verantwortung. Diese Expert*innen sollten nicht nur beratend tätig sein, sondern – sofern geeignet – auch in Audits, Monitoringprozesse und Wirkungsanalysen eingebunden werden. Ziel ist es, die Angemessenheit und Wirksamkeit der Maßnahmen zur Risikominimierung fachlich fundiert zu bewerten und Weiterentwicklungsbedarfe frühzeitig zu identifizieren. Entsprechende Gutachten, Empfehlungen und Evaluationsergebnisse sollten in geeigneter Form veröffentlicht werden, um Transparenz und Rechenschaftspflicht zu stärken.

Unabhängige Aufsicht und Audits

Schließlich ist eine wirksame unabhängige Aufsicht unerlässlich, um die Einhaltung gesetzlicher Vorgaben sowie die Qualität der Schutzmaßnahmen zu überprüfen. Plattformbetreiber sollten verpflichtet werden, regelmäßige unabhängige Audits durchzuführen, die sowohl technische als auch organisatorische Aspekte des Kinder- und Jugendschutzes umfassen. Die zuständigen Aufsichtsstellen müssen über ausreichende Ressourcen, Fachkompetenz und Durchsetzungsbefugnisse verfügen, um Prüfungen effektiv durchführen und bei Verstößen angemessen reagieren zu können. Dazu zählen unter anderem verbindliche Reportingpflichten, transparente Prüfberichte sowie abgestufte Sanktionsmöglichkeiten.

Insgesamt lässt sich die Verantwortung von Plattformbetreibern nur dann glaubwürdig und nachhaltig überprüfen, wenn Kontrollmechanismen, unabhängige Expertise und die systematische Beteiligung derjenigen, die von Risiken unmittelbar betroffen sind, verbindlich miteinander verknüpft werden. Nur so kann sichergestellt werden, dass Schutzmaßnahmen nicht nur formal existieren, sondern im digitalen Alltag von Kindern und Jugendlichen tatsächlich wirksam sind.

3. **Wie kann die Umsetzung bestehender Vorschriften – insbesondere der Vorgaben zum Schutz Minderjähriger nach Artikel 28 DSA samt Leitlinien der Kommission – sowie des JMStV und JuSchG verbessert werden?**

Die rechtlichen Vorgaben zum Schutz von Kindern und Jugendlichen im digitalen Raum sind auf europäischer wie nationaler Ebene grundsätzlich vorhanden. Insbesondere Artikel 28 des Digital Services Act (DSA) sowie die hierzu erlassenen Leitlinien der Europäischen Kommission formulieren klare Erwartungen an Online-Plattformen. Ergänzend regeln der Jugendmedienschutz-Staatsvertrag (JMStV) und das Jugendschutzgesetz (JuSchG) zentrale Anforderungen im nationalen Kontext. Defizite zeigen sich jedoch weniger auf der normativen Ebene als vielmehr in der konsequenten und einheitlichen Umsetzung dieser Vorschriften. Um ihre Wirksamkeit zu erhöhen, bedarf es gezielter Maßnahmen zur Stärkung der rechtlichen Verbindlichkeit, zur Konkretisierung unternehmensinterner Pflichten sowie zur Schaffung positiver Anreize für Anbieter.

Stärkung der rechtlichen Verbindlichkeit

Zentrale Anforderungen aus Artikel 28 DSA sowie aus JMStV und JuSchG sollten stärker operationalisiert und mit klar überprüfbaren Mindeststandards hinterlegt werden. Insbesondere Leitlinien und Empfehlungen der Europäischen Kommission entfalten bislang häufig nur orientierenden Charakter. Ihre Wirksamkeit könnte deutlich gesteigert werden, wenn sie in Teilen verbindlich ausgestaltet oder zumindest systematisch in Aufsichts- und Sanktionspraxis einbezogen würden. Eine engere Verzahnung europäischer und nationaler Durchsetzungsmechanismen sowie klarere Zuständigkeitsregelungen könnten zudem dazu beitragen, Rechtsunsicherheiten für Anbieter zu reduzieren und ein einheitlicheres Schutzniveau für Minderjährige sicherzustellen.

Unternehmensinterne Kinderschutzrichtlinien als verbindlicher Standard

Zur praktischen Umsetzung der bestehenden Vorgaben sollten Online-Anbieter ausdrücklich dazu angehalten werden, unternehmensinterne Kinderschutzrichtlinien zu entwickeln, umzusetzen und regelmäßig zu evaluieren. Diese Richtlinien sollten sich explizit an Kinderrechten orientieren und insbesondere Aspekte der Privatsphäre, Sicherheit und des Schutzes vor sexualisierter Gewalt adressieren. Konkret könnten sie unter anderem vorsehen, dass alle Mitarbeitenden verpflichtend zu Kinderrechten und relevanten Schutzmaßnahmen geschult werden, dass klare interne Melde- und Eskalationsprozesse bei Sicherheitsbedenken existieren und dass eine kontinuierliche Zusammenarbeit mit unabhängigen Kinderrechtsexpert*innen erfolgt.

Ein mögliches Vorbild für eine solche strukturierte Selbstverpflichtung bietet der Tourismussektor mit dem „Code of Conduct for the Protection of Children from Sexual Exploitation in Travel and Tourism“. Ein vergleichbarer Ansatz im digitalen Bereich könnte dazu beitragen, abstrakte gesetzliche Vorgaben in konkrete, organisationsinterne Handlungsstandards zu übersetzen und deren Umsetzung überprüfbar zu machen.

Anreizsysteme durch Zertifizierung oder Prüfsiegel

Zur zusätzlichen Motivation von Anbietern könnte ein Zertifizierungs- oder Prüfsiegelmodell eingeführt werden, das die wirksame Umsetzung von Maßnahmen zum sicheren Gebrauch von Online-Diensten durch Minderjährige bestätigt. Voraussetzung hierfür wäre die Entwicklung transparenter, anspruchsvoller und regelmäßig überprüfter Kriterien, die sowohl technische als auch organisatorische Schutzmaßnahmen berücksichtigen. Ein solches Gütesiegel könnte Anbietern einen reputativen Vorteil verschaffen und zugleich Eltern, Kindern und Jugendlichen eine bessere Orientierung bieten. Wichtig ist dabei, dass eine Zertifizierung nicht als Ersatz für behördliche Kontrolle verstanden wird, sondern diese sinnvoll ergänzt

Insgesamt kann die Umsetzung bestehender Vorschriften zum Schutz Minderjähriger nur dann nachhaltig verbessert werden, wenn rechtliche Verbindlichkeit, interne Organisationsstrukturen und positive Anreize zusammengedacht werden. Die Kombination aus klaren gesetzlichen Erwartungen, verbindlichen unternehmensinternen Standards und sichtbarer Anerkennung wirksamer Schutzmaßnahmen bietet die Chance, den bestehenden Rechtsrahmen mit tatsächlicher Wirkung im digitalen Alltag von Kindern und Jugendlichen zu füllen.

4. Gibt es aus Ihrer Sicht Regelungslücken im Bereich des technischen Kinder- und Jugendmedienschutzes, und welche Instrumente wären geeignet, diese wirksam zu schließen?

Ein bislang unzureichend reguliertes Teilphänomen im Bereich des technischen Kinder- und Jugendmedienschutzes sind KI-gestützte Deepfakes, insbesondere sogenannte Deepnudes. Mithilfe von „Nudify"-Apps oder Gesichtstausch-Tools werden dabei harmlose Bilder realer Minderjähriger – unabhängig von ihrer Geschlechtsidentität –, etwa Schulfotos oder Bilder aus sozialen Medien, in synthetische sexualisierte Darstellungen oder explizite sexuelle Handlungen umgewandelt. Diese Inhalte stellen eine Form digitaler sexualisierter Gewalt dar, auch wenn kein physischer Übergriff stattgefunden hat.

Deepfake-Inhalte werden dabei nicht ausschließlich von erwachsenen Täter(*innen) erstellt, sondern zunehmend auch von Gleichaltrigen, etwa Klassenkamerad*innen oder Freund*innen, unter Nutzung niedrigschwelliger mobiler Anwendungen. Sowohl erwachsene Täter(*innen) als auch Minderjährige mit grenzverletzendem sexuellem Verhalten nutzen solche Inhalte für sexuelle Erpressung, Finanzkriminalität, Mobbing, Belästigung oder zur Machtausübung. Sexualisierte Deepfakes von Minderjährigen stellen ein schnell wachsendes Risiko dar und haben gravierende rufschädigende und psychische Folgen für die Betroffenen, bis hin zu schweren Formen der Selbstverletzung und Suizidalität.

Hier zeigt sich eine deutliche Regelungslücke: Zwar erfassen bestehende Straf- und Jugendschutzvorschriften Teile dieser Phänomene, jedoch fehlt es bislang an klaren, spezifischen Regelungen, die bereits die Bereitstellung und Nutzung entsprechender KI-gestützter Anwendungen wirksam adressieren. Geeignet wäre daher ein ausdrückliches gesetzliches Verbot von KI-Anwendungen zur sogenannten Nudifizierung von Personen, insbesondere von Nudifier- oder Nudification-Apps. Darüber hinaus sollte sichergestellt werden, dass auch allgemeine generative KI-Systeme durch verbindliche Schutzmechanismen, Trainingsvorgaben und Nutzungseinschränkungen nicht missbräuchlich zur Herstellung von Darstellungen sexualisierter Gewalt eingesetzt werden können. Dazu zählen unter anderem klare Ausschlusskriterien im Training, technische Filter, Missbrauchserkennung sowie konsequente Durchsetzungs- und Meldepflichten.

Weitere Regelungslücken bestehen im Umgang mit Chatbots und großen Sprachmodellen. Diese Systeme werden bereits heute missbräuchlich genutzt, um Grooming und sexuelle Erpressung zu erleichtern. Sie können gezielt Grooming-Skripte oder Nachrichten zur sexuellen Erpressung generieren, missbräuchliche Inhalte übersetzen oder umformulieren, menschenverachtende, frauenfeindliche oder sexualisierte Ideologien verstärken oder sexuell explizite „Rollenspiel"-Szenarien mit Minderjährigen simulieren. Die bestehenden rechtlichen Vorgaben adressieren diese Formen der mittelbaren Ermöglichung sexualisierter Gewalt bislang nur unzureichend.

Geeignete Instrumente zur Schließung dieser Regelungslücken sind daher klare rechtliche Vorgaben für Anbieter KI-gestützter Systeme, die den Schutz von Kindern und Jugendlichen verbindlich verankern. Dazu gehören risikobasierte Einsatzbeschränkungen, verpflichtende Missbrauchsprävention, Transparenz über Schutzmaßnahmen sowie effektive Aufsichts- und Sanktionsmechanismen. Ziel muss es sein, nicht nur einzelne Inhalte zu regulieren, sondern die strukturellen Voraussetzungen zu schaffen, um digitale sexualisierte Gewalt durch KI-Technologien zu unterbinden.

5. Welche Rolle spielen starke Verschlüsselungslösungen (z.B. Ende-zu-Ende-Verschlüsselung) für den Schutz von Kindern – und welche Spannungsfelder ergeben sich mit Überwachungs- und Interventionsmöglichkeiten?

Starke Verschlüsselung, insbesondere Ende-zu-Ende-Verschlüsselung, ist ein zentraler Baustein für Privatsphäre und digitale Sicherheit, auch für Kinder und Jugendliche. Gleichzeitig kann sie von Täter*innen genutzt werden, um Grooming, sexuelle Erpressung oder den Austausch von Darstellungen sexualisierter Gewalt zu erleichtern und Interventionen zu erschweren. Daraus ergibt sich ein Spannungsverhältnis zwischen Privatsphäre und effektivem Kinderschutz.

Dieses Spannungsverhältnis sollte nicht durch pauschale Aufweichungen von Verschlüsselung gelöst werden,

sondern durch verhältnismäßige, differenzierte Schutzmaßnahmen, die starke Verschlüsselung mit wirksamer Prävention und Intervention verbinden.

Ein zentraler Ansatz kann dabei die Verhinderung des Uploads bereits bekannter Darstellungen sexualisierter Gewalt in Ende-zu-Ende-verschlüsselten Umgebungen sein. Diese Methode gilt als technisch umsetzbar und datenschutzwahrend und wird von Unternehmen bereits bei anderen Inhaltskategorien eingesetzt. Sie sollte konsequent auch auf CSAM ausgeweitet werden. Regierungen sollten Unternehmen verpflichten, entsprechende Upload-Präventionsmechanismen in E2EE-Diensten zu implementieren, um die Verbreitung bekannter Missbrauchsdarstellungen wirksam einzudämmen. Die Internet Watch Foundation hat hier eine ausführliche Erklärung zu erarbeitet.[3]

Darüber hinaus sollten Regierungen und Unternehmen Forschung und Entwicklung zu weiteren technischen und präventiven Maßnahmen fördern, um alle Formen sexualisierter Gewalt gegen Kinder und Jugendliche auch in verschlüsselten Kommunikationsräumen wirksam bekämpfen zu können.

6. **Welche Rolle sollen Betriebssysteme und App-Stores für den technischen Jugendmedienschutz übernehmen (z.B. geräteweite Jugendschutzeinstellungen, einheitliche Altersstufen-/Label-Standards, Default- und Kaufbeschränkungen) und welche regulatorischen Instrumente wären dafür geeignet?**

   Betriebssysteme und App-Stores übernehmen als Gatekeeper eine zentrale Rolle im technischen Kinder- und Jugendmedienschutz. Durch geräteweite Jugendschutzeinstellungen können Schutzmechanismen plattformübergreifend wirksam umgesetzt werden, etwa durch altersabhängige Zugriffsbeschränkungen, kindgerechte Default-Einstellungen und Einschränkungen bei Installationen oder In-App-Käufen.

   Ergänzend sind verbindliche Altersstufen- oder Labeling-Systeme für digitale Angebote sinnvoll, auch über den Bereich von Games hinaus. Alterskennzeichnungen können als Grundlage für automatische Schutzmaßnahmen dienen und sollten bei risikoreichen Anwendungen mit einer Freigabe durch erziehungsberechtigte Personen verknüpft sein.

   Voraussetzung hierfür sind einheitliche, idealerweise europaweite Standards sowie eine unabhängige Monitoring- und Aufsichtsstelle, um Verlässlichkeit und Durchsetzung sicherzustellen. Entsprechende regulatorische Vorgaben für App-Store-Betreiber können so einen wirksamen, strukturellen Beitrag zum Jugendmedienschutz leisten.

7. Welche wirtschaftlichen und betrieblichen Implikationen gehen mit einem umfassenden Jugendmedienschutz einher?

III Altersgrenzen, Altersverifikation und spezifische Schutzräume

1. **Halten Sie verbindliche Altersgrenzen für bestimmte digitale Angebote für erforderlich, und wenn ja: Nach welchen Kriterien sollten diese festgelegt werden?**

   Aus unserer Sicht besteht die Gefahr, dass pauschale gesetzliche Verbote oder starre Altersgrenzen für digitale Angebote die tatsächlichen Risiken digitaler sexualisierter Gewalt verzerren, weil sie unterschiedliche Gefährdungslagen, Nutzungsweisen und Schutzbedarfe von Kindern und Jugendlichen nicht ausreichend berücksichtigen. Sie können dazu führen, dass Kinder und Jugendliche von wichtigen zwischenmenschlichen Beziehungen zu Gleichaltrigen sowie von digitalen Unterstützungs- und Schutzräumen ausgeschlossen werden. Gleichzeitig besteht das Risiko, dass Verantwortung von denjenigen Akteur*innen wegverlagert wird, die strukturelle Veränderungen am wirksamsten vorantreiben können – insbesondere von Regierungen und Technologieunternehmen, die für die Gestaltung sicherer digitaler Umgebungen verantwortlich sind.

   Unbestritten ist jedoch, dass es digitale Angebote gibt, für die klare Altersgrenzen sinnvoll und notwendig

sind. Dies betrifft insbesondere Plattformen oder Angebotsbereiche, die Inhalte bereitstellen, die als schädlich oder gefährdend für Kinder und Jugendliche gelten. Hierzu zählen vor allem Angebote aus dem Bereich Erotik und Pornographie, für die bereits heute eine Altersgrenze ab 18 Jahren besteht. In diesem Bereich besteht jedoch erheblicher Verbesserungsbedarf bei der tatsächlichen Durchsetzung. Nach deutschem Strafrecht sind das Zeigen und Zugänglichmachen pornographischer Inhalte gegenüber Minderjährigen strafbar und als sexualisierte Gewalt einzuordnen. Bestehende Altersgrenzen entfalten daher nur dann Schutzwirkung, wenn sie konsequent und wirksam umgesetzt werden.

Für andere digitale Angebote, etwa soziale Netzwerke oder Kommunikationsplattformen, greifen pauschale Altersgrenzen hingegen zu kurz. Sie können zwar kurzfristig politische oder elterliche Beruhigungseffekte erzeugen, stellen jedoch einfache Antworten auf komplexe Problemlagen dar. Kinder und Jugendliche haben nach der UN-Kinderrechtskonvention ein Recht auf Teilhabe, das in der Allgemeinen Bemerkung Nr. 25 ausdrücklich auch für die digitale Teilhabe konkretisiert wird. Dieses Recht umfasst den Zugang zu digitalen Räumen, in denen soziale Beziehungen, Meinungsäußerung und gesellschaftliche Teilhabe stattfinden.

Starre Altersgrenzen und Zugangsverbote können zudem ein trügerisches Sicherheitsgefühl erzeugen, während sie tatsächliche Risiken und Schäden nicht wirksam reduzieren. Rechtskonforme Altersverifikationsmaßnahmen sind zwar ein wichtiges Instrument des Kinder- und Jugendschutzes, sie beschränken jedoch primär den Zugang zu Angeboten und ersetzen keine altersgerechte Gestaltung digitaler Umgebungen. Entscheidend ist vielmehr, dass Plattformen sichere, kind- und jugendgerechte Nutzungserfahrungen ermöglichen und Schutzmechanismen systematisch in Design, Moderation und Geschäftsmodelle integrieren.

Darüber hinaus ist zu berücksichtigen, dass Kinder und Jugendliche schrittweise Kompetenzen zur sicheren Nutzung digitaler Dienste entwickeln müssen. Dazu gehört auch zu lernen, wie Risiken erkannt und verantwortungsvolle Entscheidungen getroffen werden können. Digitale Schutzkonzepte sollten daher nicht auf Ausschluss setzen, sondern auf Befähigung, altersangemessene Begleitung und schrittweise wachsende Selbstständigkeit. Verbindliche Altersgrenzen sind dort erforderlich, wo Inhalte eindeutig schädlich sind; für andere Angebote sollten differenzierte, risikobasierte und kinderrechtsorientierte Ansätze im Vordergrund stehen.

2. Wie sollte eine altersangemessene Altersverifikation rechtlich und praktisch ausgestaltet werden?

Altersverifikation gilt grundsätzlich als sinnvolle Maßnahme, um Kinder und Jugendliche besser vor sexualisierter Gewalt und Ausbeutung im digitalen Raum zu schützen und altersgerechte Angebote zu ermöglichen. Sie soll Plattformen befähigen, Inhalte, Funktionen und Schutzmechanismen altersangemessen zu gestalten und zugleich den Zugang potenzieller Täter*innen zu Minderjährigen zu erschweren, etwa bei gezielter Kontaktanbahnung durch Fremde oder Erwachsene, die sich als Gleichaltrige ausgeben.

Gleichzeitig ist zu berücksichtigen, dass ein erheblicher Teil digitaler sexualisierter Gewalt im sozialen oder familiären Umfeld stattfindet. Altersverifikation kann daher keinen umfassenden Schutz gewährleisten und darf nur als ergänzende Maßnahme innerhalb eines ganzheitlichen Schutzkonzepts verstanden werden.

Der DSA sowie die Leitlinien der Europäischen Kommission zu Artikel 28 begründen bislang keine generelle Pflicht zur Altersverifikation, empfehlen ihren Einsatz jedoch ausdrücklich in risikoorientierter Kombination mit weiteren Schutzmaßnahmen. Zugleich wird klargestellt, dass reine Selbstauskünfte („self-declaration“) im Kinder- und Jugendschutz nicht ausreichen. Aus fachlicher Sicht empfehlen wir, den Leitlinien künftig einen verbindlicheren Charakter zu verleihen, um ein einheitlicheres und wirksameres Schutzniveau zu gewährleisten.

Für die rechtliche und praktische Ausgestaltung ist entscheidend, dass Altersverifikationssysteme datenschutzkonform und verhältnismäßig umgesetzt werden. Zentrale Prinzipien sind Datenminimierung

sowie der Einsatz datenschutzfreundlicher Technologien, etwa Zero-Knowledge-Proofs. Altersverifikation darf weder unverhältnismäßig in die Privatsphäre eingreifen noch neue Risiken schaffen.

Wesentliche Anforderungen sind daher:

- diskriminierungsfreier Zugang für alle, einschließlich marginalisierter Gruppen;
- kind- und jugendgerechte, verständliche Kommunikation über Zweck und Einsatz sowie niedrigschwellige Widerspruchs- und Beschwerdemöglichkeiten;
- Transparenz hinsichtlich Funktionsweise, Datenverarbeitung und Zweckbindung.

Altersverifikation kann somit ein wirksamer Baustein des Kinder- und Jugendschutzes sein, wenn sie verhältnismäßig, datenschutzfreundlich und eingebettet in umfassende Schutzmaßnahmen umgesetzt wird. Sie ersetzt jedoch weder altersgerechtes Plattformdesign noch Moderation oder weitere Präventionsinstrumente.

3. **Welche Formen der Altersabsicherung (Age-Assurance wie Schätzung, Verifikation, Token-, Wallet-basierte Nachweise) halten Sie für geeignet und wie können Over-Collection, Diskriminierung und Umgehbarkeit vermieden werden?**

Welche Form der Altersabsicherung geeignet ist, muss abhängig vom jeweiligen Dienst, seinem Risikoprofil und den angebotenen Funktionen entschieden werden. Eine pauschale Festlegung auf einzelne Verfahren ist weder sachgerecht noch mit den Leitlinien zu Artikel 28 DSA vereinbar. Altersabsicherungssysteme müssen stets den Anforderungen an Privatsphäre, Schutz und Sicherheit entsprechen und in ein umfassendes Schutzkonzept eingebettet sein.

Grundsätzlich sollten Plattformen verpflichtet werden, mehrere Formen der Altersabsicherung anzubieten, etwa altersbasierte Schätzverfahren, verifikationsbasierte Lösungen oder token- beziehungsweise walletbasierte Nachweise. Dies dient zum einen der Niedrigschwelligkeit des Zugangs und reduziert Ausschlüsse, zum anderen stärkt es das Mitbestimmungsrecht der Nutzer*innen, indem sie die für sie sicherste und vertrauenswürdigste Methode wählen können. Ein „One-size-fits-all“-Ansatz birgt hingegen die Gefahr unnötiger Datenerhebung, erhöhter Umgehungsanreize und sozialer Ausgrenzung.

Zur Vermeidung von Over-Collection sollten Altersabsicherungssysteme konsequent nach dem Prinzip der Datenminimierung ausgestaltet werden. Ziel muss es sein, ausschließlich altersbezogene Informationen zu verarbeiten, ohne Identität oder weitere personenbezogene Daten offenzulegen. Datenschutzfreundliche Technologien wie Zero-Knowledge-Proofs oder anonyme Altersnachweise können hierzu einen wichtigen Beitrag leisten. Gleichzeitig sollten Systeme so gestaltet sein, dass Umgehbarkeit nicht durch übermäßige Datenerhebung, sondern durch risikoadäquate Kombinationen technischer und organisatorischer Maßnahmen begrenzt wird.

Insgesamt sind Altersabsicherungssysteme dann geeignet, wenn sie verhältnismäßig, diskriminierungsfrei, datenschutzfreundlich und kontextabhängig eingesetzt werden. Sie dürfen nicht als isolierte Maßnahme verstanden werden, sondern müssen Teil eines umfassenden, kinderrechtsorientierten Schutzkonzepts sein.

4. Braucht es aus Ihrer Sicht speziell gestaltete digitale Räume für Kinder und Jugendliche mit begrenztem oder ausgeschlossenem Zugang für Erwachsene, und wie ließen sich solche Räume technisch, rechtlich und organisatorisch realisieren?

IV Chancen, Teilhabe und spezielle Problemfelder

1. Welche Chancen für Information, Bildung, Beteiligung und Freizeit ergeben sich durch technischen Kinder- und Jugendmedienschutz, wenn er beispielsweise „by design“ in digitale Dienste integriert wird?

2. Wie kann ein übermäßiger Medienkonsum von Kindern und Jugendlichen wirksam begrenzt werden, und welche Verantwortung tragen Anbieter hinsichtlich der Designentscheidungen, der Nutzungsdauer und des digitalen Engagements (Interaktionen)?

Übermäßiger Medienkonsum bei Kindern und Jugendlichen lässt sich nicht allein durch zeitliche Begrenzungen oder App-Sperren wirksam reduzieren, sondern erfordert eine verantwortungsvolle Gestaltung digitaler Dienste. Anbieter tragen hierbei eine zentrale Verantwortung für Designentscheidungen, die Nutzungsdauer und das digitale Engagement maßgeblich beeinflussen.

Ein wirksamer Ansatz besteht im gezielten Einsatz von Elementen und Funktionen, die zu einer aktiven statt überwiegend passiven Mediennutzung anregen. Dazu zählen interaktive, kreative und partizipative Formate, die Kinder und Jugendliche zum eigenständigen Gestalten, Reflektieren und bewussten Interagieren befähigen, anstatt sie in endlose Konsum- und Scrollmechaniken zu ziehen. Solche Gestaltungsprinzipien können dazu beitragen, Nutzungszeiten sinnvoller zu strukturieren und die Selbstregulation zu stärken.

Darüber hinaus sollten altersgerechte Social-Media-Elemente und Funktionen in alterskonformen, geschützten digitalen Angeboten bereitgestellt werden, um Medien- und Handlungskompetenzen frühzeitig aufzubauen. In diesen altersgerechten Kontexten können Kinder schrittweise lernen, mit Interaktionen, Sichtbarkeit, Feedbackmechanismen und digitalen Beziehungen umzugehen. Dies schafft eine wichtige Grundlage für eine spätere, verantwortungsvolle Nutzung nicht altersgerechter Angebote und reduziert das Risiko von Überforderung, Abhängigkeit und schädlichem Nutzungsverhalten.

3. Wie kann in Fällen von Sharenting und Family-/Kinder-Influencing einem Missbrauch von Bildern und personenbezogenen Daten technisch, regulatorisch und durch Medienbildung vorgebeugt werden?

---

[1] https://5rightsfoundation.com/resource/child-rights-by-design/
[2] Weitere Informationen: https://ecpat.de/publikationen/#tgtreffen
[3] www.iwf.org.uk/media/21rpo2o4/iwf-preventing-the-upload-of-child-sexual-abuse-material-in-end-to-end-encrypted-e2ee-environments-v1.pdf