

Stellungnahme des Deutschen Kinderhilfswerk zum zweiten Hearing der Expert*innenkommission "Kinder- und Jugendschutz in der digitalen Welt"

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),

Sexualisierte Gewalt ist ein schwerwiegender Eingriff in die körperliche und seelische Integrität. Nicht selten leiden die Betroffenen langfristig unter gesundheitlichen und/oder psychosozialen Folgen. Zugleich ist sexualisierte Gewalt ein komplexes Phänomen. Es bedarf daher unterschiedlicher Zugänge, um diese im analogen wie im digitalen Raum wirksam bekämpfen zu können.

Damit Täter¹ schneller und effektiver ausfindig gemacht werden können und insbesondere kontinuierlicher Missbrauch schnellstmöglich beendet wird, müssen Mitarbeiter*innen der Strafverfolgung für die Themen stärker sensibilisiert werden. Hier braucht es dringend fachliche Qualifizierungsmaßnahmen und Kompetenzbündelung.

Oftmals hat sexualisierte Gewalt zudem eine internationale Dimension. Es bedarf daher zusätzlich verstärkter internationaler Zusammenarbeit der Strafverfolgungsbehörden, wie sie etwa durch das EU-Zentrum in der CSA-Verordnung geplant ist. Eine vertiefte Kooperation über EU-Grenzen hinweg ist insbesondere bei Phänomenen, welche komplett über Online-Kommunikation ausgeführt werden können, wie Sextortion oder die Weiterverbreitung von Missbrauchsdarstellungen, elementar.

Zudem muss der Opferschutz verbessert werden. Verbrechen müssen schnell aufgenommen, betroffene Kinder aus gefährlichen Situationen entfernt und bei verschiedenen Anlaufstellen direkt psychosoziale Unterstützung und Begleitung angebunden werden.

Darüber hinaus müssen Kapazitäten für die Hilfe von Betroffenen ausgebaut werden. Notfall-Hotlines sind oftmals der erste Kontaktpunkt für Opfer sexualisierter Gewalt, geben jedoch hohe Überlastung an. Dass Betroffenen aufgrund einer Überlastung der Hilfestrukturen nicht schnell und kompetent geholfen werden kann, muss unbedingt vermieden werden. Eine weitere wichtige Vorsorgemaßnahme stellt der Ausbau von leicht zugänglichen und verständlichen Reporting-Systemen auf den Plattformen dar. Diese sollten einheitlich gestaltet, gut erkennbar, leicht verständlich und stets leicht erreichbar sein (etwa ein stets

Deutsches Kinderhilfswerk e.V.
Leipziger Straße 116-118
10117 Berlin

Fon: +49 30 308693-0
Fax: +49 30 308693-93
E-Mail: dkhw@dkhw.de
www.dkhw.de

Bankverbindungen:
IBAN:
DE33 3702 0500 0003 3311 00
Spendenkonto:
IBAN:
DE27 3702 0500 0003 3311 11 Bank
für Sozialwirtschaft
BIC: BFSWDE33XXX

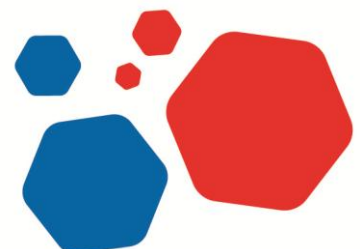
Vereinsregister-Nummer:
AG Charlottenburg 15507 B
USt-ID: DE167064766

Anerkannter Träger der freien
Jugendhilfe (§ 75 KJHG)

Mitglied im PARITÄTISCHEN
Wohlfahrtsverband

Spendensiegel
Deutsches Zentralinstitut
für soziale Fragen (DZI)

¹ Im Kontext sexualisierter Gewalt wird die männliche Form („Täter“) verwendet, da diese Form der Gewalt empirisch überwiegend von Männern ausgeübt wird und die gewählte Formulierung diese strukturelle Geschlechterasymmetrie abbildet.



verfügbarer roter Knopf, der direkt zum Reporting führt). Auch die Prozesse dahinter müssen gut verständlich und altersgerecht formuliert sein. Zudem sollten keine unnötigen Informationen abgefragt werden und Betroffene die Möglichkeit erhalten, die Bedrohung in einem Freifeld selbst beschreiben zu können. Kinder können oftmals die konkrete Gefahrenlage nicht benennen, jedoch eine generelle Bedrohung wahrnehmen. In der Nacharbeit sollte das konkrete Risiko unterstützt nachvollzogen werden. Dabei braucht es auch menschlichen Support, da KI zwar in der Analyse unterstützen kann, in Notlagen jedoch nicht verlässlich empathisch und kindeswohlorientiert handeln würde.

Eine große Herausforderung im Bereich von Missbrauchsdarstellungen und Sextortion entsteht zudem durch KI-generierte Darstellungen. Diese setzen die Hürde für den Zugang zu Missbrauchsdarstellungen herunter, Erschweren die Erkennung realweltlicher Übergriffe und drohen die Fallzahlerkennungen explodieren zu lassen. Abseits von verbesserten Filtersystemen der Plattformen in der Content-Erkennung und seitens der KI-Plattformen, welche zur Erstellung genutzt werden können, zeichnen sich in dieser Frage derzeit noch keine effektiven Lösungen ab. Eine Kennzeichnungspflicht KI-generierter Inhalte greift hier zu kurz, da diese voraussichtlich nur durch Anbieter*innen zulässiger Inhalte umgesetzt werden würde.

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

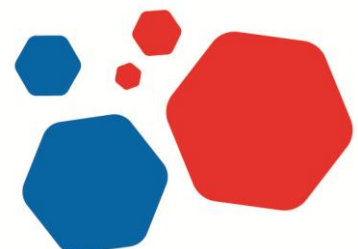
Die möglichen Gestaltungspraktiken für soziale Plattformen sind mannigfaltig und werden kontinuierlich weiterentwickelt. Eine fortlaufende Begleitung und zeitgemäße Regulierung insbesondere jener Designentscheidungen, die sich nachteilig auf die Entwicklung von Kindern auswirken können, bedarf Child Rights by Design² Ansätzen. Das bedeutet, dass Kinder von Beginn an bei solchen Designentscheidungen eingebunden werden müssen, damit sowohl mögliche Risiken frühzeitig hervorgehoben als auch einfache Zugangswege und Nutzungsmöglichkeiten zielgruppengerecht umgesetzt werden können. Da einige der genannten Praktiken erst in der längeren Nutzung deutlich werden, muss die jeweilige Plattform auch Governance-Wege für eine kontinuierliche kinderrechtliche Begleitung vorsehen. Als good practice können hier Jugendbeiräte als Teil der Plattform-Governance-Strukturen genannt werden. Ebenfalls die Bewertung neuer Funktionen durch Eltern-Kind-Konsultationen, wie sie etwa von der USK zur Lesbarkeit ihrer Deskriptoren genutzt wurden, würde relevante Perspektiven vor der Implementation einholen.

Darüber hinaus sollten Zugangswege für unabhängige wissenschaftliche Studien erleichtert werden, um explizit Langzeiteffekte nachvollziehbar zu machen. Zudem sollten kinderrechtliche Folgenabschätzungen (Child Rights Impact Assessments)³ verpflichtend als Teil der Risikobewertungen der Plattformen (z.B. im Rahmen des DSA) aufgenommen werden. Dadurch können Langzeitfolgen im Rahmen regelmäßiger Folgenabschätzungen adressiert werden.

Nicht zuletzt bestehen bereits zahlreiche Rechtsmittel, um Problemlagen in diesem Bereich rechtlich zu adressieren. Die Leitlinien zu DSA Art. 28 geben ein Korsett für die kindgerechte Ausgestaltung von Plattformen, d.h. für Plattformen mit sozialen

² <https://childrightsbydesign.5rightsfoundation.com/page/child-rights-by-design/>

³ https://researchonline.lse.ac.uk/id/eprint/128736/3/Policy_Internet_-_2025_-_Livingstone_-_Child_Rights_Impact_Assessment_A_Policy_Tool_for_a_Rights_Respecting_Digital.pdf



Features risikoabgestufte, altersangemessene Voreinstellungen mit differenzierbaren Funktions- und Teilhabeoptionen, z.B. über Parental Controls. In regelmäßigen Aktualisierungen der Leitlinien bietet sich die Chance, neue Trends und Herausforderungen zeitnah aufzugreifen und regulatorisch gegenzusteuern. Die Risiken der persönlichen Integrität in JuSchG und JMStV werden in der Spruchpraxis der Selbstkontrollen berücksichtigt. Diese Praxis könnte ebenfalls auf digitale Inhalte ausgeweitet werden, um neben den Nutzungsbedingungen eine verbindlichere Orientierung über Plattformrisiken zu geben.

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

Diese Phänomene betreffen die gesamte Gesellschaft und müssen daher für den gesamten digitalen Raum reguliert werden. Dafür gibt es zwei Hebel. Erstens braucht es eine bekannte und informierte Gegenöffentlichkeit, die bspw. durch Unterstützungsmaßnahmen für Fact-Checking Programme gefördert werden kann. Hinzu kommt die Verpflichtung der Plattformen zur Nutzung solcher Programme, insbesondere vor dem Hintergrund, dass etwa Meta angekündigt hat, Fact-Checking zu reduzieren, oder X diese Programme gar diskreditiert. Die Anerkennung der Gemeinnützigkeit von Fact-Checking-Organisationen, der Ausbau von Validierungsmaßnahmen durch den DSA Digital Service Coordinator, aber auch staatliche finanzierte (?) Förderprogramme können hier wichtige Lücken schließen.

Zweitens muss die Monetarisierung von Desinformation unterbunden werden. Dies wird gezielte staatliche Desinformation weniger betreffen, allerdings hindert es die Weiterverbreitung und Zweitverwertung von Desinformation durch monetarisierte Kanäle und schränkt zudem Scams und Datensammlungen ein, welche oft auf diese Kampagnen aufspringen.

Wichtig ist dafür das Transparenz-Register für Werbeanzeigen, welches ausgebaut werden muss, um bessere Rückschlüsse auf die Auftraggebenden zuzulassen und Wiederholungstäter vor Anzeigenschaltung zu identifizieren.

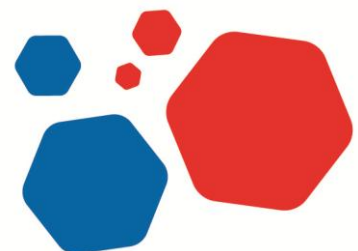
Ein zweiter Schritt besteht in der Demonetisierung von Kanälen, welche sich wiederholt der Verbreitung von Desinformation, Hate Speech, Verschwörungserzählungen oder extremistischen Inhalten schuldig gemacht haben. Wenn diese zudem versuchen, Auflagen zu umgehen, sollte auch nicht vor Deplatforming⁴, dem Komplettausschluss von der respektiven Plattform, zurückgeschreckt werden.

Mit eingeschränkter Verwertbarkeit dieser Inhalte, die durch die Aufmerksamkeitsökonomie begünstigt werden, verlieren diese an Relevanz für Influencer*innen und werden nach und nach eine weniger präasente Rolle im Sozialraum der Plattformen spielen.

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

Dieses Set Risiken greift im Allgemeinen insbesondere stark in die Privatsphäre von Individuen ein. Zu beachten ist dabei, dass Altersgruppen unterschiedlich von den genannten Interaktionsrisiken betroffen sind. Insbesondere beim Stalking kommt zudem eine ausgeprägte Gender-Dimension hinzu.

⁴ <https://www.idz-jena.de/forschung/hate-not-found-das-deplatforming-der-extremen-rechten>



Zunächst ist es wichtig, dass diese Risiken stärker durch die Plattformen unterbunden werden. Proaktives Monitoring anstatt der Verwaltung gemeldeter Beiträge wäre ein Grundsatz, der helfen würde, eine Durchsetzung der Community Guidelines besser umzusetzen. Insbesondere Wiederholungstäter müssen in ihrer Reichweite und in Kontaktmöglichkeiten beschränkt werden und bei schweren Fällen ihre Plattform-Zugänge verlieren. Eine bleibende Herausforderung ist dabei die Abwägung zwischen Redefreiheit und zivil- oder gar strafrechtlichen Übergriffen. Es braucht daher eine adäquate Dokumentation der Vorfälle, um Opfer bei weiteren Schritten zu begleiten.

Auch Kinder und Jugendliche können Opfer von solchen koordinierten Attacken werden. Diese wünschen sich dafür mehr menschliche Unterstützung, schnellere Meldewege, sowie transparente Abhilfe und Reaktionen⁵. Dazu können einheitlich gestaltete Meldesysteme, auch plattformübergreifend, hilfreich sein. Eine Harmonisierung dieser Systeme wäre über Standards und Protokolle umsetzbar. Gleichsam sind ein zentrales Manko die geringen Moderationskapazitäten, welche durch die Plattformen bereitgestellt werden. Während KI bei der Identifikation von Schlagworten, Trends und vernetzten Akteuren unterstützen kann, bedarf es menschlicher Entscheidungen, um Kontextzusammenhänge einzubetten, regionale Besonderheiten zu identifizieren, aber auch folgenreiche Moderationsentscheidungen zu treffen - auch wenn dies bereits oft auf automatisierte Entscheidungen mit Widerspruch ausgelagert wird. Für Kinder, besonders für junge Kinder, ist eine persönliche Begleitung wichtig. Es braucht eine empathische Ansprache und altersgemäße Unterstützung in Notsituationen, die Kinder sonst schnell überwältigen können. Um diese Risiken auszuschließen, bedarf es zusätzlicher Kapazitäten oder klarer Kommunikationsschranken.

Schon jetzt gibt es zahlreiche Unterstützungsangebote und Notfallkontakte für Kinder und Jugendliche. Leider sind diese jedoch oft zu wenig bekannt, unterfinanziert und nicht ausreichend sichtbar, wenn Kinder in Notsituationen geraten. Die Plattformen könnten und sollten diese Sichtbarkeit herstellen, ähnlich wie es teilweise schon Praxis für Suizid-Hotlines bei bestimmten Schlagwortsuchen ist.

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

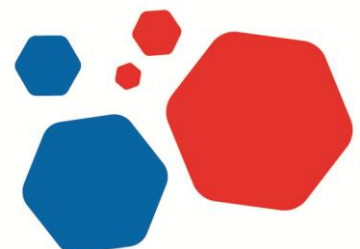
Bei der Selbstgefährdung junger Menschen müssen einerseits die Filtermechanismen der Plattformen greifen, um schädliche Inhalte frühzeitig zu identifizieren. Safety Teams müssen proaktive Moderation zu diesen Inhalten verfolgen, um neue Trends, gefährliche Challenges und sonstige Phänomene frühzeitig zu identifizieren. Dazu gehört auch ein enger Austausch mit Fachverbänden und Forschungsteams.

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

Viele hier passende Punkte wurden bereits unter 1c benannt, da Scams und Desinformation ähnliche Verbreitungslinien haben und teilweise ineinandergreifen.

⁵

https://www.dkhw.de/filestorage/1_Informieren/1.1_Unsere_Themen/Kinder_und_Medien/Kinderrechte_in_der_digitalen_Welt/Dateien/DKHW_Metarecherche_Interaktionsrisiken.pdf



Wichtig ist die konsequente Durchsetzung des DSA sowie das Einfordern einer kindgerechten Plattformgestaltung im Rahmen des DSA Art. 28 und der zugehörigen Leitlinien.

Generell sollten Verstöße gegen die Sorgfaltspflicht der Plattformen konsequenter geahndet werden. Ein neues Instrument dies zu kommerziellen Risiken zu verankern, könnte die geplante EU-Verbraucherschutzrichtlinie in Form des Digital Fairness Acts bieten.

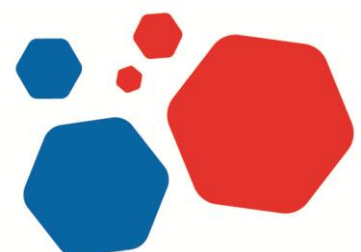
2. Welche Rolle spielen dabei konkrete Gestaltungsentscheidungen von Diensten (z.B. Default-Einstellungen, Empfehlungs- und Rankingsysteme, Sharing-/Kontaktfunktionen, Interface-Design, Parental-Control-Funktionen)?

Das Design von Diensten hat einen umfangreichen Einfluss auf die Nutzungserfahrung. Dabei haben große und kommerzielle Plattformen häufig einen klaren Wettbewerbsvorteil gegenüber gemeinnützigen Alternativangeboten, die in der Regel nicht die Mittel haben, ähnlich attraktive Formate oder ähnlich wirksame Algorithmen zu entwickeln. Es sollte nicht vergessen werden, dass die algorithmische Steuerung eine große Rolle dabei spielt, weshalb diese Plattformen so populär wurden. Gleichsam investieren Unternehmen viel in Forschung, welche explizit darauf abzielt, die Nutzungsdauer zu erhöhen. Um diesem Wissens- und Zugangsvorsprung ein regulatorisches Gegengewicht zu geben, müssen manipulative Praktiken identifiziert und unterbunden werden. Soziale Funktionen haben Milliarden Nutzer*innen auf Facebook gebracht und an den Dienst gebunden. Manipulative Praktiken fanden sich allerdings eher im individuellen Targetting auf der Grundlage der Nutzer*inneninformationen, in der Priorisierung emotionalisierender Inhalte durch den Algorithmus und der Monopolwirkung in Kombination mit Instagram und Whatsapp. Grundlegende Geschäftsinteressen stehen im Konflikt mit den Interessen und Rechten von Kindern, Jugendlichen und anderen Nutzenden. Dies führt zu der Herausforderung, dass manipulative Praktiken kontinuierlich weiterentwickelt und somit Akteur*innen des Kinder- und Jugendmedienschutzes stets auf Trab gehalten werden.

Um diesem vorzubeugen, sollten Kinder und Jugendliche sowohl in der Plattform Governance als auch über Child Rights by Design Ansätze einbezogen werden, wie bereits unter 1b beschrieben.

Die großen Plattformen kopieren bereits grundlegende Funktionen voneinander. Gruppenchats, Kurzvideoformate und Endloses Scrolling finden sich mittlerweile in allen großen Plattformen. Dieses Übernehmen von „good practice“ scheint sich allerdings kaum auf Kinderschutzkonzepte, Meldefunktionen oder das Vermitteln von Unterstützungs- und Guidance Systemen zu übertragen. Wie unter 1d dargestellt, sollten Meldefunktionen plattformübergreifend einheitlich gestaltet, leicht auffindbar und kindgerecht ausgestaltet und beschrieben sein.

Kinderschutz Einstellungen werden zunehmend über Parental Controls abgebildet. Diese sollten daher einheitlich gestaltet sein und derselben Ablauflogik folgen, um Eltern den Zugang zu den Tools zu vereinfachen und die aktive Nutzung der Tools zu erhöhen. Noch nutzen zu wenige Eltern diese Angebote, berichten von zu viel Aufwand, sich in die Tools hineinzuarbeiten. Zudem werden sie oftmals als einmalige Einstellungsmöglichkeiten im Setup Prozess einer App oder eines Geräts genutzt. Da sich die Kompetenzen und Interessen im Heranwachsen wandeln, werden falsch eingestellte Parental Controls zu einer unliebsamen Last, die umgangen wird, anstatt dass sie als Unterstützungsangebot fungieren.



Altersgerechte Voreinstellungen sollten Raum für das Erziehungsprivileg der Eltern lassen, allerdings auch ohne elterliche Intervention dynamische Einstellungsmöglichkeiten für minderjährige Nutzer*innen bieten, mit weiterführenden Funktionen als Opt-In durch eine*n Erziehungsberechtigte*n.

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

Generell sollten Diensteanbieter zu kinderrechtlichen Folgeabschätzungen ihrer Dienste verpflichtet werden (Child Right Impact Assessment⁶). Dies sollte einerseits als Teil der Risikoabschätzung geschehen, welche im Rahmen des DSA für VLOPs und VLOSE vorgesehen ist, andererseits ebenfalls als Werkzeug für kleinere Plattformen dienen, um die Angemessenheit ihrer Angebote für Kinder und Jugendliche zu bemessen und ggf. notwendige Vorsorgemaßnahmen einzuleiten.

Die kinderrechtlichen Folgeabschätzungen bauen auf den 5C Risikodimensionen für Kinder in Online-Umgebungen⁷ auf. Diese können als multiperspektivischer Zugang zur Analyse plattformseitiger Risikofaktoren dienen. Darüber hinaus sollte der Gefährdungsatlas der BzKJ⁸ als Referenzwerk für die Erkennung problematischer Praktiken dienen, um aufkommende Phänomene abzubilden. Damit wird der Auslegungsspielraum im Ermessen gefährlicher Praktiken verengt. Dazu muss dieser allerdings auch in kürzeren, regelmäßigen Abständen aktualisiert werden, um aktuelle Praktiken und Risiken sowie deren Bewertung zeitgemäß zu halten.

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

Die unter I.3. benannte kinderrechtliche Folgenabschätzung eignet sich für die Überprüfung der Wirksamkeit von Maßnahmen, da sie nicht nur Risiken und Maßnahmen in den Fokus nimmt, sondern zusätzlich unbeabsichtigte Folgen in der Bewertung heranzieht und die Konsequenzen für Kinder in Bezug auf Schutz, Befähigung und Beteiligung abwägt.

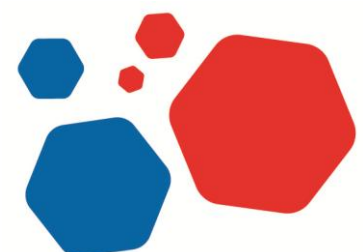
Als weiterer Referenzpunkt sollte eine Prüfung der Sorgfaltspflichten von Plattformen verankert werden. Die bisherigen Risikobewertungen im Rahmen des Digital Services Acts waren detailarm, unambitioniert und rundum unzureichend, um notwendige Anpassungen am Plattformdesign einzuleiten. Bisher wurden nur Verstöße geahndet, wenn, wie durch X/Twitter, keine Risikobewertung vorgenommen wurde. In folgenden Berichten müssen auch Tiefgang und Sorgfalt der Analyse stärker eingefordert werden. Es darf nicht akzeptiert werden, dass Plattformen vor den Risiken mutwillig die Augen verschließen.

Während die Risikobewertungen in den Händen der Plattformen liegen, bedarf es auch unabhängiger Kontrollinstanzen. In einigen Fällen hat die EU-Kommission

⁶ <https://onlinelibrary.wiley.com/doi/10.1002/poi3.70008>

⁷ OECD (2021), "Children in the digital environment: Revised typology of risks", *OECD Digital Economy Papers*, No. 302, OECD Publishing, Paris, <https://doi.org/10.1787/9b8f222e-en>.

⁸ <https://www.bzkg.de/bzkg/service/publikationen/gefaehrungsatlas-digitales-aufwachsen-vom-kind-aus-denken-zukunftssicher-handeln-aktualisierte-und-erweiterte-2-auflage--197812>



bereits eigenständig Untersuchungen eingeleitet. Darüber hinaus sollte allerdings unabhängige Forschung im Bereich möglicher Risiken stärker gefördert werden. Formal sieht der DSA dafür Zugang für eine wissenschaftliche Begleitung vor. Tatsächlich zeigen sich die Plattformen hierfür jedoch unterschiedlich empfänglich, sind unterschiedlich transparent und nicht proaktiv in risikoorientierten Forschungsdesigns. Daher sollten öffentliche Mittel für unabhängige Untersuchungen bereitgestellt werden, wie sie z.B. bereits durch Jugendschutz.net in regelmäßigen Abständen vorgenommen werden, um einzelne Phänomene in den Blick zu rücken. Zudem müssen die Zugangsmöglichkeiten für Forschungen durch die Plattformen abgesichert werden.

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)?

Siehe Punkte I.4. zu Sorgfaltspflichten und kinderrechtlichen Folgeabschätzungen sowie I.1.d. zu kindgerechten Meldewegen.

Erste Transparenzstandards sind durch die Leitlinien zur politischen Werbung umgesetzt. Während die Berichte und Risikobewertungen der Plattformen Ansätze einer transparenten Plattform in sich tragen, sollten hier weitere vergleichbare Kriterien herangezogen werden. Insbesondere in der Moderation gibt es Nachholbedarfe in der Offenlegung: wie viele menschliche Moderator*innen werden pro Nutzer*in eingesetzt, welche Moderationsregeln werden angewandt, welche Sonderregeln bestehen für die Moderation von Meldungen Minderjähriger.

Hinzu kommen Transparenzbedarfe in der Moderationsverwaltung. Kinder und Jugendliche wünschen sich Fortschritts- und Ergebnisberichte ihrer Meldungen mit nachvollziehbaren Prozessupdates und verständlichen Begründungen bei abschlägigen Entscheidungen. Kaum etwas hat das Vertrauen in sichere Plattformumgebungen so beeinträchtigt wie die nachlässigen und intransparenten Moderationsstandards. Wenn Kinder die offiziellen Meldewege meiden, weil diese bewusst unattraktiv und unresponsiv gestaltet sind, dann kommen Plattformen ihrer Schutzverantwortung nicht nach.

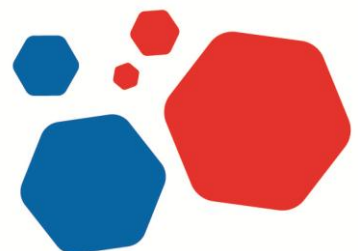
2. Wie lässt sich die Verantwortung der Plattformbetreiber überprüfbar ausgestalten (z.B. Audits, Reporting, unabhängige Aufsicht, Beteiligung von Kindern und Zivilgesellschaft)?

Siehe I.1.b. für Kinder- und Jugendbeteiligung in der Plattform-Governance.

Siehe I.4. für unabhängige Forschungsbeteiligung und Reporting Auflagen im Rahmen des DSA.

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?

Siehe I.4. zu Sorgfaltspflichten und Einforderung qualitativer Risikobewertungen durch die EU-Kommission. Siehe Beteiligung von Kindern und Jugendlichen in Institutionen des Kinder- und Jugendmedienschutzes in I.1.b.



Wie unter 1.3. bereits angemerkt, sollte der Gefährdungsatlas der BzKJ eine stärkere Referenzrolle für die Risikobewertungen der Diensteanbieter einnehmen. Dies kann sowohl in der praktischen Anwendung, in Kontrollen durch die Medienanstalten und den DSC geschehen aber auch über Referenzen, z.B. als Ergänzung in den Leitlinien des DSA Art. 28. Ebenfalls unter 1.3. wurde eine regelmäßige Aktualisierung des Gefährdungsatlas angemerkt. Dies sollte unter aktiver Beteiligung von Kindern- und Jugendlichen geschehen, damit diese möglichst aktuell ihre lebensweltlichen Perspektiven einbringen können.

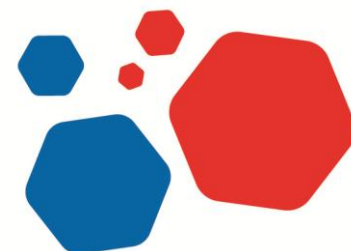
Zusätzlich wurden im Rahmen der JuSchG-Novelle viele neue Aufgaben an die BzKJ übertragen. Dazu gehört auch die Förderung kindgerechter Angebote. Allerdings wurde daran keine ausreichende Budgetierung gekoppelt. Seit dem Wegfall der Förderprogramme durch das Familienministerium sind starke Einbrüche in der Kinderangebotslandschaft zu verzeichnen. Qualitative Kinderangebote bedürfen nachhaltiger Finanzierung und struktureller Förderung, damit sie attraktive Angebote und notwendige Informationsvielfalt anbieten können. Der Wegfall von Kinderangeboten reduziert nicht nur die Vielfalt qualitativer Informationsangebote für Kinder, er verengt auch ihre Wahlmöglichkeiten, was sie schneller in Richtung kommerzieller Plattformen drängt. Die BzKJ sollte also mit zureichenden Mitteln ausgestattet werden, um ihrem Arbeitsauftrag der Förderung kindgerechter Angebote nachzukommen.

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

Der starke regulatorische Fokus auf Altersfeststellungsverfahren steht in einem Widerspruch dem Anliegen gegenüber Plattformen zu einer kindgerechten Gestaltung ihrer Angebote zu bewegen. Altersfeststellungsverfahren sollen dazu geeignet sein geschlossene Nutzer*innengruppen abzubilden. In der Regel dienen sie daher dem Ausschluss (fast ausschließlich) jüngerer Zielgruppen. Regulierungen, wie der DSA, welche den Ausschluss aufgrund von Risiko als eine gleichberechtigte Option neben der kindgerechten Gestaltung verstehen, verkennen die ökonomische Motivation der Plattformen. Verbunden mit dem Verbot personalisierter Werbung für minderjährige und notwendiger Einschränkungen in den Anreizen Geld auszugeben insbesondere in den jüngsten Altersstufen, fehlen Anreize für die Plattformen die Kosten für ein kindgerechtes Design zu übernehmen. Die Implementation eines akkreditierten Altersfeststellungsverfahrens (insbesondere wenn die Kosten aus öffentlichen Geldern gedeckt werden) ist für Plattformen somit eine deutlich wirtschaftlichere Maßnahme als umfassende Anpassungen ihres Plattformdesigns.

Primär ist die fehlende und unzureichende Durchsetzung von Regulierung problematisch. In seinen Regulierungsbereichen ist der Kinder- und Jugendmedienschutz gut aufgestellt und etabliert.

Leider ist die Jugendbeteiligung, welche ebenfalls im JuSchG vorgesehen ist, noch immer im Aufbau begriffen. Mit unserer Publikation „Beteiligung von Heranwachsenden im Kinder- und Jugendmedienschutz: Altersspezifische Formate und Qualitätskriterien“⁹, haben wir verschiedene Angebote und



Entwicklungspotentiale beleuchtet und im letzten Jahr durch ein Jugendpanel unter Beteiligung der Selbstkontrollen, BzKJ und mabb weiterentwickelt. Die Ergebnisse des Panels werden im Sommer veröffentlicht werden.

Ein weiteres Manko sind die unzureichend durchgesetzten Nutzungsbedingungen der sozialen Netzwerke. Dort sind Mindestalter zwischen 13 und 18 Jahren vorgesehen, obwohl diese nachweislich auch von jüngeren Nutzer*innen besucht werden. Hier fehlen Regelungen zur Sorgfaltspflicht bzw. werden diese Regelungen nicht umgesetzt. Beschwerdemöglichkeiten beim DSC bei systematischen Nicht-Interventionen der Plattformen, wenn minderjährige Accounts nicht entfernt werden, sind nur unzureichend bekannt. Mehr Informationen über Eingriffs- und Beschwerdemöglichkeiten für Kinder, Jugendliche aber auch Erziehungsberechtigte müssen besser bekannt gemacht werden, z.B. im Rahmen einer breiten Informationskampagne zur Medienkompetenz.

Neu hinzu kommen KI-Phänomene, welche bisher kaum reguliert werden und teilweise über andere Rahmenwerke abgedeckt werden sollen (z.B. DSGVO für Datenverarbeitungszusammenhänge, DSA für algorithmisches Targetting). Viele Phänomene brauchen jedoch eine Einzelbetrachtung und ggf. maßgeschneiderte Regulierung. Z.B. haben Nudifier-Apps bereits erheblich in die Lebenswelten, insbesondere junger Mädchen, eingegriffen. Hier eine schwerwiegende Jugendgefährdung festzustellen und sie auf dieser Grundlage aus den App-Stores zu entfernen, wäre ein nachvollziehbarer Schritt. Andere Phänomene bedürfen einer stärkeren Einzelfallabwägung, etwa Chatbots, insbesondere personalisierte „Charakterbots“, welche menschliche Beziehungen nachahmen, die als mögliches Risikophänomen eruiert werden sollten. Eine weitere Herausforderung sind allg. generative KI-Tools, da Inhaltsregulierung auf diese durch ihren hohen Grad an Personalisierung und die Nicht-Wiederholbarkeit ihrer Outputs nur schwer anzuwenden sein wird.

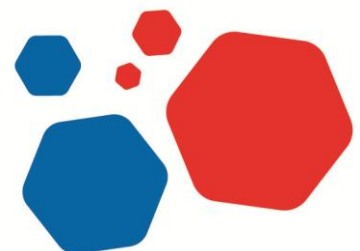
5. Welche Rolle spielen starke Verschlüsselungslösungen (z.B. Ende-zu-Ende-Verschlüsselung) für den Schutz von Kindern – und welche Spannungsfelder ergeben sich mit Überwachungs- und Interventionsmöglichkeiten?

Verschlüsselungstechnologien gelten als zweischneidiges Schwert im Kinder- und Jugendmedienschutz. Sie bieten unüberwachte Rückzugsräume für Kinder- und Jugendliche, können Schutzräume für benachteiligte Gruppen gewährleisten und einen anonymen oder pseudonymen Erprobungsraum zur Identitätsbildung junger Menschen bieten. Gleichzeitig sind sie, aufgrund ihrer Intransparenz, Orte für Übergriffe abseits von elterlicher oder staatlicher Kontrolle und zumeist ohne externe Unterstützungsmöglichkeiten. Kontaktrisiken können durch Verschlüsselung daher verstärkt werden.

Es erfordert ein hohes Maß an Medienkompetenz und Medienerfahrungen, selbstbewusst mit diesen Kontaktrisiken umzugehen und durch Blockieren und Melden unliebsame Nutzer*innenanfragen abzuweisen. Gerade frühes Ausprobieren mit sozialen Medien birgt das Risiko, unbewusst Daten preiszugeben, welche auch langfristig zu neuen Online-Risiken führen können.

Gleichzeitig sollte nicht ausgeblendet werden, dass Verschlüsselung auch die Privatsphäre minderjähriger Nutzer*innen schützt und ein Umgehen von Verschlüsselung nachhaltig die Sicherheitsinfrastruktur des Internets schädigen kann.

Allerdings gibt es hier weniger invasive Alternativen, welche Kinder und Jugendliche ermächtigen, Risiken begegnen zu können. Die bereits unter I.1.d.



angemerkten zusätzlichen Moderationsaufwände und Reportingmechanismen sowie die dort angemerkten harmonisierten Standards, können und sollten mit Ausleitungsmechanismen unterfüttert werden. Kinder und Jugendliche sollten riskante Kommunikationen auch ohne Benennung eines konkreten Risikos melden können und daraufhin Unterstützung erfahren. Ausleitung dient hier dazu, durch die meldenden Nutzer*innen automatisch entschlüsselte Chatinhalte zu dokumentieren und dann unverschlüsselt als Teil einer Meldung weiterzuleiten. Damit können die Meldenden freiwillig unilateral die Verschlüsselung aussetzen. In Verbindung mit den Metadaten der Konversation sollten Plattformen dann ausreichend Informationen haben, um Grooming, Scams oder Mobbing identifizieren 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?

Bei dieser Frage stehen ambitionierte Ziele im Konflikt mit der technischen Umsetzung. Während grundlegende Schutzeinstellungen auf unterster Geräteebene wünschenswert sind, unter dem Vorsatz, möglichst ganzheitliche Vorsorgemaßnahmen anzubieten, steht diesen aus technischer Sicht eine relativ fragmentierte Gerätelandschaft entgegen. Neben mannigfaltigen Gerätetypen (Mobiltelefon, Tablet, Spielkonsole, Laptop, Handheld) sind diese teilweise mit verschiedenen Betriebssystemen und untergeordnet mit verschiedenen Versionen oder Modifikationen ausgestaltet. Insbesondere bei älteren Geräten, welche häufig an jüngere Geschwister weitergegeben werden, wird ein nachträglicher Patch zur Einführung solcher Vorsorgemaßnahmen nur schwierig umzusetzen sein, insbesondere wenn die Betriebssysteme nicht mehr durch die Anbieter gewartet werden.

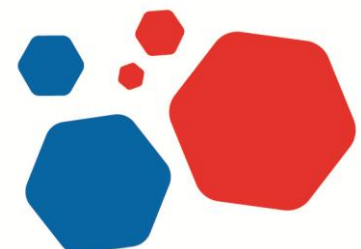
Ein zweiter Punkt ist die Rolle der sich entwickelnden Kompetenzen von Kindern, welche aus kinderrechtlicher Sicht Berücksichtigung finden müssen. Zumeist geschieht dies über Parental Controls, allerdings auch nicht mehrheitlich. Auch hier bietet sich ein niedrigschwelliger Zugang an, um möglichst wenig Einstellungen an den Geräten vornehmen zu müssen. Leider führt dies allerdings auch häufig dazu, dass Parental Controls nicht regelmäßig mit den Interessen und Bedürfnissen der Kinder abgeglichen werden.

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

Viel zu lange wurde an menschlichem Moderationsaufwand gespart. „Das skaliert nicht“ darf kein Argument sein, um Jugendschutz nicht durchzusetzen, insbesondere seitens der global erfolgreichsten Firmen. Moderationsschlüssel müssen deutlich erhöht werden. Trust and Safety Teams ausgebaut werden.

Qualitativ hochwertiger Jugendschutz braucht auch Jugendbeteiligung. Eingebundene Kinder und Jugendliche müssen altersgerecht informiert und unterstützt werden. Eine Scheinbeteiligung erhöht das Schutzniveau nicht. Plattformen sollten daher in eigene (nationale) Jugendpanels investieren, mit klar formulierten Rollen und Kompetenzen in der Plattform-Governance und der Möglichkeit, eigenständig Themen zu setzen und Design-Entscheidungen der Plattform vor Markteintritt zu bewerten.

Eine Herausforderung für die Einforderung kindgerechter Anpassungen ist das Verbot personalisierter Werbung im DSA. Wenn Kinder keine werberelevante



Zielgruppe sind, gleichsam Investments nötig sind, um sie auf den Plattformen zu halten, gibt es wenig Anreize für die Plattformen, eigenständig kindgerechte Anpassungen vorzunehmen. Dies ist besonders unwahrscheinlich, da durch geschlossene Nutzer*innengruppen, die mit den Altersfeststellungsverfahren erzeugt werden sollen, eine kostengünstige Alternative gegeben wird. Die Installation einer Altersfeststellung, die Minderjährige formal ausschließt (egal wie umgehbar), gilt als zureichende Schutzmaßnahme, um an risikobehafteten Praktiken festzuhalten. Es bedarf daher Lösungen, welche Plattformen Anreize geben, kindgerechte Anpassungen vorzunehmen, statt einfache Ausflüchte über Ausschlüsse umzusetzen.

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?

Verbindliche Altersgrenzen sind nicht erforderlich, wenn kindgerechte Vorsorgemaßnahmen by default eingestellt sind. Wenn eine kinderrechtliche Folgenabschätzung kein Sicherheitsrisiko ergibt oder zureichende Vorsorgemaßnahmen umgesetzt wurden, die in der Lage sind, Kinder vor Gefahren zu bewahren, können Angebote auch ohne Altersfeststellungsverfahren funktionieren, analog zu Altersfreigaben ohne Altersbeschränkung der Alterskennzeichen. Ein Beispiel dafür ist die vom Deutschen Kinderhilfswerk betriebene Seite Kindersache.de. Diese sieht neben von Kindern selbstgestalteten Inhalten auch Interaktionsfunktionen wie Kommentare vor. Aktive Moderation aller Kommentare, bevor diese live gehen, in Kombination mit pädagogischer Begleitung, falls ein Kommentar oder Inhalt ein Risiko umfassen könnte, führt zu einem umfassenden Schutz und Befähigungskonzept, welches auch für junge Kinder Raum zur Beteiligung lässt.

Wo geschlossene Nutzer*innengruppen notwendig sind und Altersgrenzen als Schutzinstrument unabdingbar sind, sollten sie so implementiert werden, dass sie nicht zu Ausschlüssen von anderen Rechtsbereichen führen, wie dem Recht auf Information, Kommunikation, Bildung, etc. Dies kann beispielsweise über Risikofreie Alternativangebote abgesichert werden.

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

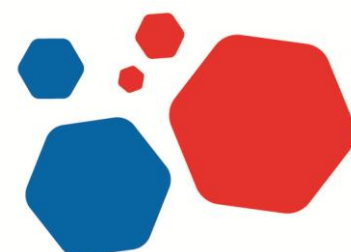
In unserem „Grundsatzpapier zivilgesellschaftlicher Organisationen zum Thema Altersverifikation/Altersfeststellung (Age Assurance)“¹⁰ haben wir umfassend die Rahmenbedingung einer kinderrechtlich ausgewogenen Altersfeststellung skizziert und auch die rechtlichen und technischen Bedingungen berücksichtigt.

Im Kern der kindgerechten Umsetzung stehen 4 Grundsätze:

- Datenschutz/Schutz der Privatsphäre
- Safety by Design/Sichere Umsetzung
- Transparency by Design/informierte Einwilligung zur Nutzung
- Access(ibility) by Design/niedrigschwellige Zugangsmöglichkeiten

Daraus leiten sich Privatsphäre-schonende, minimalinvasive Verfahren ab, die öffentlich kontrolliert (im Sinne von Open Source) auch unabhängig von

¹⁰ <https://kinderschutzbund.de/wp-content/uploads/2025/06/AltersfeststellungPaper.pdf>



Personaldokumenten genutzt werden können und die verschiedenen Altersstufen, sowie das Erziehungsprivileg der Eltern berücksichtigen.

Eine Altersverifikation sollte eingesetzt werden, um kindgerechte Angebote bestimmten Altersgruppen zuzuweisen, nicht um jüngere Altersgruppen von Diensten auszuschließen.

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

Generell sollte, wo möglich, auf Altersabsicherung verzichtet werden, da Datenverarbeitung persönlicher Daten immer Risiken von Datenlecks bietet, aber durch Scammer und Desinformation auch genutzt werden kann, um Nutzer*innen irrtümlich ihre Daten unbekannten Dritten preiszugeben.

Der Einsatz von Altersfeststellungsverfahren sollte nur nach einer kinderrechtlichen Folgenabschätzung erfolgen, wenn diese Feststellung auch einen Mehrwert im Interesse des Kindes bietet.

Eine detaillierte Analyse der verschiedenen Feststellungsverfahren und der mit ihnen verbundenen Herausforderungen findet sich in unserem „Grundsatzpapier zivilgesellschaftlicher Organisationen zum Thema Altersverifikation/Altersfeststellung (Age Assurance)“¹¹.

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?

Für jüngere Altersgruppen müssen im Sinne der UN Kinderrechtskonvention Erprobungsräume ermöglicht werden, insbesondere für Kinder in Grundschule und Kita. Dabei kann es zielführend sein, auch Erwachsene auszugliedern bzw. nur verifizierte Fachkräfte zuzulassen. Diese Räume sollten stets pädagogisch begleitet und umfassend moderiert sein, um frühzeitig Nutzungsregeln und gegenseitige Achtung zu vermitteln.

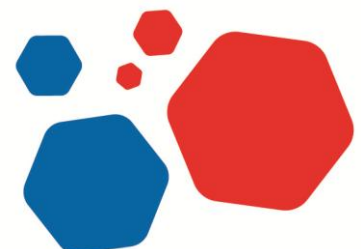
Zumeist bieten sich solche Räume in lokalen Kontext mit persönlich bekanntem Mitgliederkreis an, z.B. verwaltet über Schule oder Jugendklub, was die Verifizierung der Teilnehmenden vereinfacht.

Ziel dieser Räume ist eine stufenweise Vorbereitung auf das offene Netz und Kindern erste digitale Erfahrungen und Kommunikationsregeln zu vermitteln. Ein Beispiel für die Umsetzung könnten etwa von Jugendclubs betreute Server oder Kommunikationskanäle sein oder das Mein Bildungsraum¹² Konzept, welches digitale Schulangebote für lokale Träger anbieten sollte.

Es ist wichtig die digitalen Bedarfe von Kindern mit altersgerechten Angeboten abzudecken, damit sie nicht auf unangemessene Angebote ausweichen. Die Verantwortungsübertragung vom Familienministerium auf die BzKJ für kindgerechte Angebote im Rahmen der JuSchG Novelle ging nicht mit den notwendigen finanziellen Mitteln einher, um in eine attraktive Kinderangebotslandschaft zu investieren. Der Wegfall früherer Förderungen hat bereits die Einstellung zahlreicher Kinderangebote nach sich geführt, während viele weitere um ihren Bestand bangen müssen. Während die Ansprüche von Kindern an ihre digitalen Umgebungen sich mit der vielfältigen Medienlandschaft

¹¹ <https://kinderschutzbund.de/wp-content/uploads/2025/06/AlterfeststellungPaper.pdf>

¹² <https://www.meinbildungsraum.de/>



wandeln, fehlen Förderprogramme, welche den Kinderangeboten ein Mitwachsen ermöglichen würden. Es bedarf offener, kindeswohlorientierter Medienangebote, die altersabgestuft Kindern erlauben Erfahrungen mit den vielfältigen Spielarten digitaler Medien zu sammeln. Diese Angebote sollten pädagogisch begleitet sein und einen Schutzraum zum Experimentieren bieten. Dazu gehören ebenfalls soziale Medien, generative KI und Videoplattformen. Diese Angebote sind bereits in ihren nicht-jugendgerechten Formen tief in den Nutzungsgewohnheiten vieler Kinder verankert, was zu einem großen Akzeptanzproblem führen wird, sollte rigide Altersgrenzen für ihren Medienzugang eingeführt werden.

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?

„By Design“-Ansätze tragen zu einer Harmonisierung bei. Ein vergleichbares Sicherheitsniveau und vergleichbare, möglichst übertragbare Schutzkonzepte. Eine optimale Umsetzung würde ebenfalls gemeinsame Protokolle, Standards und Abläufe mit sich führen und somit den kognitiven Aufwand der sicheren Plattformnutzung reduzieren. Eine solche Standardisierung erleichtert z.B. die Befähigung zur eigenständigen Nutzung.

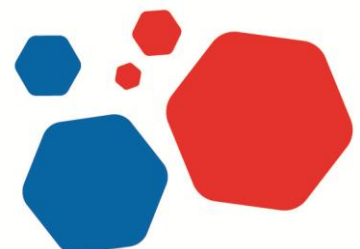
„By Design“ umfasst auch sichere Voreinstellungen und hohe Sicherheitsstandards ab erster Nutzung der Dienste, aber auch eine Berücksichtigung der Jugendschutzinteressen bei neuen Designentscheidungen. Als Querschnittsanliegen in den Designentscheidungen sollten also potenziellen Risiken bereits durch proaktive Gegensteuerung begegnet werden, etwa Nudges oder präsente Selbstregulierungs-Tools für Bildschirmzeit.

Gleichzeitig muss eine gute Umsetzung von „Kinder- und Jugendmedienschutz by Design“ auch Vorkehrungen treffen, um Overblocking von Inhalten zu vermeiden, wie es etwa beim weitverbreiteten Tool jusprog geschehen ist¹³. By Design darf nicht in ein rigoroses Korsett überspringen, sondern muss flexibel genug bleiben, um den sich entwickelnden Kompetenzen von Kindern und Jugendlichen Raum zu geben. Zudem sollte ein kinderrechtlich abgesichertes Konzept auch Maßnahmen berücksichtigen, mit denen Kinder- und Jugendliche weitere Funktionen oder Inhalte erschließen können, etwa durch Einverständnis eines*r Erziehungsberechtigten. Zudem sollten Beteiligung und Befähigung auch abgesichert werden, falls Kinder ohne die Unterstützung von Familienmitgliedern aufwachsen.

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)?

Nach einem sprunghaften Anstieg der digitalen Nutzung während der Corona-Maßnahmen, ging die Nutzung wieder auf ein Vor-Pandemie-Niveau zurück. Kinder und Jugendliche zeigten sich selbstreflektiert und suchten nicht-digitale Angebote. Zentrales Motiv on- und offline ist der Kontakt mit Freund*innen. Grade

¹³ <https://netzpolitik.org/2024/verhuetung-erst-ab-18-deutschlands-wichtigster-jugendschutz-filter-blockiert-hilfsangebote/>



jüngere Kinder drücken explizit den Wunsch aus, auch draußen zusammen zu spielen und Freund*innen in Person zu treffen. Selbst unter Jugendlichen bevorzugt nur ca. ¼ den digitalen Kontakt vor persönlichem Austausch¹⁴.

Daher ist eine zentrale Herausforderung attraktive, in der Breite verfügbare nicht-digitale Angebote zu unterbreiten. Grade im ländlichen Raum fehlen abseits der Schule oft Beteiligungsräume für Kinder. Es braucht einen quantitativen und qualitativen Ausbau von Kinder- und Jugendfreizeitangeboten, anstatt in immer weiteren Einsparungen die Beteiligungsmöglichkeiten kontinuierlich einzuschränken.

Im digitalen Raum haben sich Nudges und Transparenz als gute Werkzeuge erwiesen, um exzessive Nutzung zu veranschaulichen. Immer frequentere Hinweise bei langanhaltender Nutzung, rücken die lange Verweildauer ins Bewusstsein. Eine wöchentliche oder tägliche Zusammenfassung der App-Nutzung mit Zeitangaben hilft auch der Selbstreflexion.

Bei jüngeren Kindern haben Eltern über Parental Controls die Möglichkeit, Beschränkungen für die Nutzungsdauer zu setzen. Wichtig ist hier das Verständnis zu verankern, dass diese Entscheidungen nicht im Alleingang getroffen werden sollten, sondern im Einvernehmen mit den Kindern getroffen werden sollten, um ein Verständnis für eine gesunde Mediennutzung zu entwickeln und die Selbstregulierungskompetenz zu schulen.

Insbesondere im Grundschulalter haben sich verpflichtende Ruhepausen, etwa während der Schulzeit und ein Ruhemodus in den Abend- und Nachtstunden bewährt.

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?

Mit unserem Rechtsgutachten „Kindeswohlgefährdung durch kommerzielle Veröffentlichung von Kinderfotos und -videos im Internet“¹⁵ haben wir die Herausforderungen, welche durch kommerzielles Family-Influencing entstehen, prüfen und bewerten lassen.

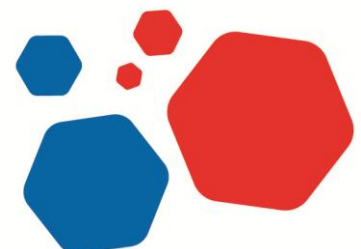
Innerhalb des bestehenden Rechtsrahmens wäre eine Prüfung einer möglichen Jugendgefährdung über die Jugendämter umsetzbar, allerdings unwahrscheinlich. Es fehlt sowohl an Kapazitäten als auch Expertisen in der Prüfung solcher Influencing-Verhältnisse.

Eine Klarstellung des Anwendungsfeldes des JArbSchG auf digitale Arbeitsformen sollte aufgenommen werden, um sichere Rahmenbedingungen für die Kinder im Family-Influencing zu schaffen. Eine Handhabe analog der Ausnahmegewilligungspraxis, wie sie für schauspielerische Aufführungen gilt, müsste auch für digitale Tätigkeiten adaptiert werden. Zudem sind Einwilligungsregelungen für die Kinder notwendig, um den Rollenkonflikt der Eltern als Bezugs- und Erziehungsperson aber auch Auftraggeber aufzulösen.

Ein weiterer Ort, wo Family-Influencing aufgegriffen werden könnte, wäre in den Leitlinien des DSA Art. 28. Dort werden unter Commercial Practices risikobehaftete Influencer-Angebote aufgegriffen. Hier könnte der Sachverhalt ebenfalls abgebildet werden. Damit müssten die Plattformen eigene Maßnahmen als

¹⁴ <https://newsroom.vodafone.de/jugendliche-wuenschen-sich-mehr-bildschirmfreie-zeit>

¹⁵ <https://www.dkhw.de/informieren/im-ueberblick/aktuelles/nachricht/rechtsgutachten-familien-influencing/>



Vorsorgemaßnahmen aufnehmen z.B. Informationskampagnen innerhalb ihrer Influencer-Programme.

Zudem sollte auch in der frühkindlichen Medienbildung ein Bewusstsein für das Recht am eigenen Bild geschaffen werden und die Entscheidungskompetenzen der Kinder geschult werden. Kinder müssen dazu befähigt werden, ihrem Unbehagen Ausdruck zu verleihen, auch wenn sie durch ihre Eltern Druck erfahren.

