Deutscher Ethikrat

Paper Trident/Shutterstock.com

Schutz, Teilhabe und Befähigung von Kindern und Jugendlichen in der digitalen Welt

AD-HOC-STELLUNGNAHME

11. Juni 2026

Herausgegeben vom Deutschen Ethikrat

Jägerstraße 22/23 · D-10117 Berlin
Telefon: +49/30/20370-242 · Telefax: +49/30/20370-252
E-Mail: kontakt@ethikrat.org
www.ethikrat.org

Danksagung

Der Deutsche Ethikrat bedankt sich für den vertrauensvollen und kollegialen Austausch mit der Unabhängigen Expertenkommission „Kinder- und Jugendschutz in der digitalen Welt“ des Bundesministeriums für Bildung, Familie, Senioren, Frauen und Jugend, von deren Sachstandsbericht wir sehr profitiert haben. Besonderer Dank gebührt außerdem Stephan Dreyer, Wouter Lueks und Hannes Federrath für ihre konstruktiven Rückmeldungen zum Entwurf der Stellungnahme und den hilfreichen Austausch zu den juristischen und technischen Aspekten des Themas.

Inhaltsverzeichnis

1 Einleitung und Problembeschreibung

Soziale Medien und andere digitale Technologien spielen eine wichtige und wachsende Rolle im Alltag vieler Kinder und Jugendlicher.[1] Eine aktive und reflektierte Nutzung solcher Angebote in ausgewogenem Umfang kann unter geeigneten Voraussetzungen positiv zur psychosozialen Entwicklung junger Menschen beitragen und ihre Identitätsentwicklung, Informiertheit, Bildung und gesellschaftliche Teilhabe unterstützen.[2] Jedoch zeigt eine steigende Anzahl empirischer Befunde, dass weniger optimale Nutzungsmuster und -erfahrungen das Wohl von Kindern und Jugendlichen negativ beeinflussen können: In Deutschland berichten im Herbst 2025 21,5 Prozent der 10- bis 17-Jährigen eine riskante und 6,6 Prozent eine pathologische Nutzung Sozialer Medien[3], die mit deutlich häufiger berichteten Depressions- und Angstsymptomen, Stress, Schlafproblemen und suizidalen Gedanken einhergeht.[4] Der Gefährdungsatlas der Bundeszentrale für Kinder- und Jugendmedienschutz benennt 43 Medienphänomene, die Minderjährige online gefährden können.[5] Es geht dabei nicht nur um bestimmte Inhalte wie Pornografie, Hass, Gewalt und Extremismus, sondern auch um Vorgänge wie Cybermobbing, Cybergrooming und Anstiftung zu selbstgefährdendem Verhalten sowie um Privatsphäreverletzungen und manipulative Geschäftspraktiken. Diese können nicht nur in Sozialen Medien, sondern auch bei der Nutzung anderer digitaler Angebote auftreten, zum Beispiel bei Onlinespielen, Streamingdiensten, Messenger-Apps oder KI-Anwendungen wie Chatbots.

Die Europäische Kommission teilt Onlinerisiken für Minderjährige in ihren Jugendschutzleitlinien zum Gesetz über digitale Dienste (Digital Services Act)[6] in fünf Kategorien ein:

1. *Inhaltsrisiken (content risks):* „Minderjährige können unerwartet und unbeabsichtigt Inhalten ausgesetzt werden, die ihnen potenziell schaden“, zum Beispiel Inhalte, die Selbstverletzung, Selbstmord, Essstörungen oder extreme Gewalt propagieren.
2. *Verhaltensrisiken (conduct risks):* Sie betreffen „Verhaltensweisen, die Minderjährige im Internet aktiv an den Tag legen können“. Dies beinhaltet beispielsweise das Posten/Versenden von hasserfüllten Inhalten/Nachrichten, gewalttätigen oder pornografischen Inhalten, Darstellungen sexuellen Missbrauchs oder terroristischen Inhalten durch Minderjährige sowie die Teilnahme an gefährlichen Herausforderungen.
3. *Kontaktrisiken (contact risks):* Sie betreffen „Situationen, in denen Minderjährige Opfer der Interaktionen sind und nicht die Täter“. Dazu gehören unter anderem Onlinegrooming, sexuelle Nötigung und Erpressung im Internet, sexueller Missbrauch via Webcam, Cybermobbing, Menschenhandel zum Zweck der sexuellen Ausbeutung sowie auch Online-Betrugspraktiken wie Phishing, Marktplatzbetrug und Identitätsdiebstahl.
4. *Verbraucherrisiken (consumer risks):* Sie beschreiben Risiken, denen Minderjährige „in ihrer Eigenschaft als Verbraucher in der digitalen Wirtschaft“ ausgesetzt sein können. Solche Risiken können beispielsweise von Marketing, Profiling und Werbung ausgehen. Hinzu kommen finanzielle Risiken wie die Ausgabe großer Geldbeträge, Risiken im Zusammenhang mit dem Kauf von Drogen und anderen illegalen oder gefährlichen Produkten sowie Risiken im Zusammenhang mit Verträgen.

---

[1] Vgl. Staksrud et al. (2026).
[2] Vgl. Agyapong-Opoku et al. (2025); Salehi et al. (2025); Brailovskaia et al. (2025) 13 ff.
[3] Vgl. Wiedemann et al. (2026) 14.
[4] Vgl. Brailovskaia et al. (2025) 15 ff.
[5] Vgl. Brüggen et al. (2022) 102 ff.
[6] http://data.europa.eu/eli/C/2025/5519/oj [14.04.2026]; vgl. auch Livingstone und Stoilova (2021).

5. *Querschnittsrisiken (cross-cutting risks):* Sie erstrecken sich über alle Risikokategorien und können „das Leben von Minderjährigen auf vielfältige Weise erheblich beeinträchtigen." Zu ihnen zählen unter anderem Risiken durch KI-Chatbots oder den Einsatz biometrischer Technologien, Risiken durch die übermäßige Nutzung von Onlineplattformen, die etwa Sucht, Depression, Angststörungen, gestörte Schlafmuster und soziale Isolation nach sich ziehen können, und zusätzliche Risiken für die Privatsphäre, den Datenschutz und die Sicherheit von Minderjährigen.

Aufgrund dieser Risiken und Gefahren haben mehrere Länder politische Maßnahmen zum besseren Schutz von Minderjährigen vorgeschlagen oder bereits umgesetzt. In Australien dürfen Kinder und Jugendliche unter 16 Jahren seit dem 10. Dezember 2025 keine Konten bei Sozialen Medien mehr haben[7]; in Großbritannien müssen Websites mit altersbeschränkten Inhalten (wie Pornografie oder Gewalt) seit dem 25. Juli 2025 wirksame Verfahren zur Altersüberprüfung einsetzen[8]. Zahlreiche weitere Länder diskutieren oder arbeiten an Gesetzesinitiativen zu Altersbeschränkungen für Soziale Medien.[9] In Deutschland haben sowohl SPD und CDU im Februar 2026 als auch Bündnis 90/Die Grünen im April 2026 eine gesetzliche Altersgrenze von 14 Jahren für die Nutzung Sozialer Medien gefordert[10]; die Empfehlungen der von der Bundesregierung eingesetzten Unabhängigen Expertenkommission „Kinder- und Jugendschutz in der digitalen Welt" werden im Juni 2026 erwartet[11]. Eine Resolution des Europäischen Parlaments befürwortete im November 2025[12] EU-weite altersgestaffelte Zugangsbeschränkungen zu Sozialen Medien, KI-Chatbots und Videoplattformen und die Europäische Kommission hat im März 2026 ein Gremium eingesetzt[13], das Empfehlungen zur Sicherheit von Kindern im Internet und zu möglichen Altersgrenzen für Soziale Medien und andere Onlinedienste in Europa erarbeiten soll.

Die Reaktionen auf Initiativen zu Einführung neuer Altersgrenzen für den Zugang zu Sozialen Medien reichen von Enthusiasmus für als dringend notwendig empfundene Maßnahmen bis hin zur Sorge, dass solche Altersgrenzen und die zu deren Umsetzung notwendigen technischen Maßnahmen Minderjährige nicht effektiv schützen, sondern stattdessen sogar zu negativen Konsequenzen wie zum Beispiel reduzierter Teilhabe und Medienkompetenz sowie zu Privatsphäreverletzungen führen. In der Folge hat sich eine intensive öffentliche und politische Debatte darüber entsponnen, welche Art oder Kombination von Maßnahmen am besten geeignet ist, um Risiken und Schäden durch digitale Angebote zu mindern, ohne zugleich unverhältnismäßige, schädliche Nebenwirkungen hervorzurufen.

Leitmaßstab für die Bewertung möglicher Maßnahmen ist das Kindeswohl im Sinne von Art. 3 der UN-Kinderrechtskonvention.[14] Dieses umfasst nicht nur Schutz vor Gefährdungen, sondern ebenso das Recht auf Teilhabe, Berücksichtigung des Kindeswillens und freie Meinungsäußerung (Art. 12, 13), den Zugang zu entwicklungsförderlichen Informationen (Art. 17) sowie die Förderung der Persönlichkeit und der Fähigkeiten des Kindes (Art. 29), einschließlich der Befähigung zu verantwortlicher Mediennutzung. Das Verhältnis zwischen diesen verschiedenen

---

[7] https://www.pm.gov.au/media/albanese-government-protecting-kids-social-media-harms [05.05.2026].
[8] https://www.gov.uk/government/collections/online-safety-act [05.05.2026].
[9] Siehe hierzu Global Social Media Age Restriction Tracker: https://social-media-age-tracker.onrender.com [19.05.2026].
[10] Vgl. SPD-Bundestagsfraktion (2026); CDU Deutschlands (2026) 88 ff.; Bundestagsfraktion Bündnis 90/Die Grünen (2026).
[11] https://www.bmbfsfj.bund.de/bmbfsfj/themen/kinder-und-jugend/expertenkommission-kinder-und-jugendschutz-in-der-digitalen-welt [05.05.2026].
[12] http://data.europa.eu/eli/C/2026/1708/oj [14.04.2026].
[13] https://digital-strategy.ec.europa.eu/en/policies/panel-child-safety-online [05.05.2026].
[14] Die Kinderrechtskonvention gilt für alle Menschen unter 18 Jahren.

Aspekten des Kindeswohls ist nicht frei von Spannungen. Die Priorisierung eines Aspekts kann zu Abstrichen bei der Realisierung der anderen Aspekte führen.

Damit ergibt sich ein ethisch bedeutsames Spannungsfeld aus Schutz-, Teilhabe- und Befähigungsinteressen, das bei der Bestimmung des Kindeswohls zu beachten ist. Wie dieses Spannungsfeld aufzulösen ist, haben in erster Linie die Eltern[15] zu entscheiden, denen sowohl nach der UN-Kinderrechtskonvention (Art. 18 Abs. 1 Satz 2 sowie Art. 5) als auch nach dem Grundgesetz (Art. 6 Abs. 2 Satz 1) die Erziehung ihrer Kinder anvertraut ist. Dessen ungeachtet bleibt durchaus Raum für staatliche Regulierung. Eine solche kann und sollte die Eltern mit vielfältigen Maßnahmen unterstützen und deren Entscheidung auch Grenzen setzen. Sie darf dabei aber nicht aus den Augen verlieren, dass es primär die Aufgabe und Verantwortung der Eltern ist, in einem Spannungsverhältnis stehende Aspekte des Kindeswohls angemessen auszubalancieren.

[15] Damit sind hier und im Folgenden alle Personensorgeberechtigten gemeint.

2 Rechtliche und technische Rahmenbedingungen

Eine ethische Beurteilung von Konzepten für den Kinder- und Jugendschutz in der digitalen Welt erfordert ein Verständnis der relevanten rechtlichen Rahmenbedingungen einerseits sowie der Funktionsweisen und der Rolle digitaler Technologien andererseits.

2.1 Rechtliche Rahmenbedingungen

Hinsichtlich der rechtlichen Rahmenbedingungen für den Schutz von Kindern und Jugendlichen in der digitalen Welt sind für den deutschen Kontext drei Ebenen zu unterscheiden: die Ebene der Europäischen Union, die des Bundes und die der Länder. Aus diesem Zusammenspiel ergibt sich das Bild eines bereits umfangreichen, sich jedoch fortlaufend weiterentwickelnden und teilweise fragmentierten regulatorischen Umfeldes.

Auf EU-Ebene sind verschiedene Rechtsakte in unterschiedlichem Ausmaß relevant, insbesondere der Digital Services Act, die Richtlinie über audiovisuelle Mediendienste, die KI-Verordnung sowie die Datenschutz-Grundverordnung. Ein Gesetz über digitale Fairness (Digital Fairness Act), das eine Reihe von Techniken und kommerziellen Praktiken im Internet verbraucherfreundlicher regeln soll, hat die Europäische Kommission in ihrem Arbeitsprogramm für das vierte Quartal des Jahres 2026 angekündigt.[16]

Auf Bundesebene ist neben der bereits erwähnten UN-Kinderrechtskonvention, die aufgrund des Zustimmungsgesetzes vom 17. Februar 1992 in Deutschland im Range eines einfachen Bundesgesetzes gilt[17], zuvorderst das Jugendschutzgesetz (JuSchG) von Bedeutung, dessen dritter Abschnitt den „Jugendschutz im Bereich der Medien“ regelt. Neben den Vorgaben für die Verwaltungsverfahren zur Freigabe und Alterskennzeichnung von physischen digitalen Medien mit Filmen und Spielen sieht der Abschnitt Vorgaben für Alterskennzeichnungen auf Film- und Spielplattformen vor. Im Bereich der digitalen Dienste verweist § 16 JuSchG hinsichtlich der an die Inhalte von digitalen Diensten zu richtenden besonderen Anforderungen auf den zwischen den Bundesländern geschlossenen Jugendmedienschutz-Staatsvertrag (JMStV). Im Anwendungsbereich des JMStV sind Onlineanbieter, die eigene Inhalte zugänglich machen, zur Vornahme einer Altersbewertung verpflichtet; bei entwicklungsbeeinträchtigenden Inhalten und Funktionen – insbesondere solchen ab 16 und ab 18 Jahren – haben sie dafür Sorge zu tragen, dass Jüngere üblicherweise keinen Zugang zu dem Angebot erhalten.

Die Aufsicht über die Umsetzung der rechtlichen Regelungen des JMStV obliegt den Landesmedienanstalten mit der Kommission für Jugendmedienschutz als zentralem Entscheidungsorgan.[18] Über die Einhaltung der Kennzeichnungspflichten für Film- und Spielplattformen wacht die Bundeszentrale für Kinder- und Jugendmedienschutz, die daneben umfassende Aufgaben zur Weiterentwicklung des Kinder- und Jugendmedienschutzes hat. Der deutsche Ordnungsrahmen im Jugendmedienschutz macht auf beiden Ebenen Gebrauch von Einrichtungen der Freiwilligen Selbstkontrolle. Auf der Grundlage des JuSchG bewerten Selbstkontrolleinrichtungen, die Kooperationsverträge mit den Obersten Landesjugendbehörden haben, ab welcher Altersgruppe Filme und Computerspiele unbedenklich sind. Je nach dem Ergebnis dieser Überprüfung erhalten die betreffenden Angebote eine unbeschränkte Freigabe oder eine Freigabe ab

[16] COM(2025) 870 final, Annex I.
[17] Vgl. Wissenschaftliche Dienste des Deutschen Bundestages (2006).
[18] https://www.kjm-online.de/aufsicht [15.04.2026].

sechs, ab 12, ab 16 oder ab 18 Jahren („Keine Jugendfreigabe“).[19] Die von den Obersten Landesjugendbehörden in der Regel übernommenen Altersbewertungen erfolgen derzeit durch die Freiwillige Selbstkontrolle der Filmwirtschaft (FSK) und die Freiwillige Selbstkontrolle Unterhaltungssoftware (USK).

Im Bereich des Rundfunks und der Telemedien erkennt die Kommission für Jugendmedienschutz Einrichtungen der Freiwilligen Selbstkontrolle an. Diese können Angebote auf Antrag eines Anbieters altersbewerten und technische Schutzinstrumente auf ihre Eignung prüfen. Unter der Ägide des JMStV anerkannte Einrichtungen sind die Freiwillige Selbstkontrolle Fernsehen, die Freiwillige Selbstkontrolle Multimedia-Diensteanbieter, die USK.online sowie die FSK.online. Die Befassung einer JMStV-Selbstkontrolle mit einem Angebot führt zu einer Art Schutzschild: Von einer Selbstkontrolle geprüfte bzw. bewertete Angebote können nicht ohne Weiteres von den Landesmedienanstalten beanstandet werden. Online zugänglich gemachte Filme, Serien und Spiele müssen auf ein JuSchG-Alterskennzeichen oder eine JMStV-Altersseinstufung ebenfalls hinweisen. Für Apps gilt das nicht gleichermaßen; hier haben sich in vielen App-Marktplätzen anbietereigene Altersbewertungen auf Basis des IARC-Verfahrens (International Age Rating Coalition) etabliert. Mit den seit Dezember 2025 geltenden Vorgaben zur sogenannten Jugendschutzvorrichtung zielt der JMStV zudem auf von Eltern aktivierbare Kinderschutzfunktionen auf Ebene der Betriebssysteme von Endgeräten (v. a. Smartphones, Computer, Spielekonsolen) ab.

Hinsichtlich des Verhältnisses der unterschiedlichen Rechtsgrundlagen ist der Anwendungsvorrang des EU-Rechts gegenüber dem nationalen Recht zu beachten. Der als EU-Verordnung unmittelbar geltende Digital Services Act (DSA) regelt in Art. 28 bereits, in welcher Weise Onlineplattform-Anbieter, das heißt Angebote, die nutzergenerierte Inhalte öffentlich zugänglich machen, den Schutz Minderjähriger zu gewährleisten haben. Die Regelung enthält keine Öffnungsklausel für nationale Gesetze. Nach dem in Erwägungsgrund 9 des im DSA zum Ausdruck gebrachten Prinzips der Vollharmonisierung sind die Mitgliedstaaten deshalb nach Art. 114 des Vertrags über die Arbeitsweise der Europäischen Union[20] wohl nicht befugt, die Plattformanbieter durch nationale Vorgaben zu einem weitergehenden Schutz von Minderjährigen zu verpflichten.[21] Bei Maßnahmen, die außerhalb des Anwendungsbereichs des DSA liegen oder einen anderen Schutzzweck verfolgen als die Verordnung, tritt diese Schwierigkeit dagegen nicht auf. So könnte etwa ein Verbot privater Handynutzung in Schulen auf nationaler Ebene durch die Länder geregelt werden.

Auf die meisten Angebote generativer KI ist der DSA nicht anwendbar, da diese Anwendungen keine nutzergenerierten Inhalte öffentlich zugänglich machen; eine Ausnahme stellen in Onlineplattformen integrierte KI-Anwendungen dar. Auf KI-Systeme ist grundsätzlich die KI-Verordnung anwendbar; diese enthält aber keine ausdrückliche und einfach handhabbare Vorgabe zur Berücksichtigung von Jugendschutzbelangen.[22] Auch von dem derzeitigen JMStV werden die Anwendungen generativer KI, bei denen der Output regelmäßig ausschließlich auf dem Input durch eine nutzende Person beruht, nicht umfassend erfasst.[23]

---

[19] https://www.bzkj.de/bzkj/wegweiser/spiele [20.05.2026]; https://www.bzkj.de/bzkj/wegweiser/filme [20.05.2026].
[20] Die Vorschrift lässt bei harmonisierenden europäischen Verordnungen in ihren Absatz 5 schutzerhöhende nationale Alleingänge nur zum Schutz der Umwelt und der Arbeitsumwelt zu.
[21] Vgl. Wissenschaftliche Dienste des Deutschen Bundestages (2026).
[22] Vgl. Dreyer (2025).
[23] Vgl. Ukrow (2024).

2.2 Technische Rahmenbedingungen

Digitale Technologien sind im Kontext des Kinder- und Jugendschutzes von doppelter Bedeutung. Einerseits gibt es diverse digitale Technologien, die Kinder und Jugendliche gefährden können, wie zum Beispiel Soziale Medien, aber auch Spiele und zuletzt insbesondere KI-Chatbots. Andererseits gibt es Technologien, welche notwendig wären, um den Schutz von Kindern und Jugendlichen online zu gewährleisten. Hier sind zwei Arten von Verfahren und Technologien von besonderer Relevanz. Zum einen sind dies Altersbestimmungstechnologien, welche Personen, die auf digitale Angebote zugreifen möchten, in relevante Alterskohorten differenzieren, beispielsweise Kinder unter 14 Jahren. Zum anderen sind es jene Technologien, die erforderlich sind, um Angebote oder Inhalte nach ihrer Eignung für bestimmte Altersgruppen zu klassifizieren. Für beide Aspekte bedarf es effektiver, sicherer und robuster technischer Lösungen.

Für die Differenzierung von Inhalten gibt es einerseits die zuvor genannten Institutionen der Freiwilligen Selbstkontrolle für unterschiedliche Medientypen (z. B. die Freiwillige Selbstkontrolle der Filmwirtschaft und die Freiwillige Selbstkontrolle Fernsehen). Diese stützen sich bei der Klassifikation von Inhalten auf etablierte Verfahren unter Beteiligung von Jugendschutzexpertinnen und -experten, wobei auch der Einsatz KI-basierter Verfahren hier auf dem Vormarsch ist. Andererseits klassifizieren Plattformen und Diensteanbieter Inhalte auf freiwilliger Basis. Nicht zuletzt aufgrund der schieren Menge an nutzergenerierten Inhalten verwenden diese jedoch in weitaus größerem Ausmaß KI-basierte Verfahren und delegieren die Moderation oder Löschung von Inhalten an Subunternehmer, vor allem im Globalen Süden.[24] Auch einige von Eltern nutzbare Kindersicherungs-Apps bieten inzwischen eine KI-basierte Klassifizierung von Inhalten an.[25]

Zur Differenzierung von Nutzerinnen und Nutzern nach Altersgruppen gibt es ebenfalls unterschiedliche Verfahren. Hierbei ist es wichtig, sich zu vergegenwärtigen, dass im Falle einer rechtlichen Verpflichtung zur Altersbestimmung alle Personen, die altersbeschränkte Angebote nutzen wollen, von diesen Maßnahmen betroffen sind. Das heißt, auch Erwachsene müssen in diesen Fällen nachweisen, das Mindestalter erreicht zu haben. Entscheidungen für zusätzliche Verpflichtungen zur Altersbestimmung, etwa für Soziale Medien, können also je nach Anzahl und Verbreitung der Dienste, bei denen solche Überprüfungen erforderlich wären, sehr viele Menschen betreffen. Entsprechend müssten technische Lösungen, die für deren Umsetzung nötig wären, nicht nur effektiv und nebenwirkungsarm, sondern auch skalierbar sein.

In Anlehnung an die Klassifizierung des australischen Pilotprojekts[26] können vier Ansätze zur Alterskontrolle unterschieden werden:

1. *Altersverifikation (age verification):* Das Alter wird anhand amtlicher Dokumente überprüft.
2. *Altersschätzung (age estimation):* Das Alter wird anhand biometrischer Merkmale wie Stimme oder Fotos geschätzt.
3. *Altersableitung (age inference):* Das Alter wird anhand von Verhaltensspuren einer Nutzerin oder eines Nutzers abgeleitet, die entweder eine Plattform erhebt oder die (zusätzlich) auf Basis von Daten aus anderen Quellen ermittelt werden.

[24] Vgl. Block und Riesewieck (2018).
[25] Zum Beispiel Helmit, FamiSafe oder Qustodio.
[26] Vgl. Age Check Certification Scheme (2025).

4. *Elterliche Kontrolle* (vorab) *und Zustimmung* (nach Zugriffsversuch) *(parental control and consent):* Eltern nutzen technische Mittel, um den Zugriff auf digitale Inhalte und Dienste gemäß dem Alter und Entwicklungsstand ihres Kindes zu genehmigen. Dies beinhaltet zum einen die Möglichkeit, bei der Einrichtung der Geräte das Alter der Kinder anzugeben, um damit jugendschutzkonforme Grundeinstellungen systemweit zu implementieren. Zum anderen geht es hierbei auch um technische Möglichkeiten, mittels derer Eltern ihren Kindern Zugriff auf bestimmte digitale Angebote wie Apps oder Webseiten gewähren oder verwehren bzw. Nutzungszeiten beschränken können.

Für jeden dieser vier grundsätzlichen Ansätze gibt es unterschiedliche Ausgestaltungen. Von besonderer Relevanz ist hier die Frage, ob die Alterskontrolle auf den Endgeräten der Nutzenden stattfindet, aufseiten der Plattformen selbst oder durch Drittanbieter. Unterschiedliche Formen und Kombinationen der oben genannten Ansätze mit unterschiedlichen Architekturen sind nicht nur technisch zu unterscheiden, sondern haben sehr unterschiedliche Auswirkungen auf die Effektivität, Genauigkeit und Robustheit der Maßnahmen einerseits sowie deren Nebenwirkungen beispielsweise hinsichtlich der Privatsphäre andererseits.[27] Angesichts der potenziell großen Zahl der von den Maßnahmen betroffenen Personen sollten diese Auswirkungen sorgfältig geprüft werden.

[27] Vgl. Lueks et al. (2026).

3 Ethische Analyse

Eine ethische Analyse von Schutzkonzepten für Kinder und Jugendliche in der digitalen Welt muss sich am Leitziel des Kindeswohls orientieren. Ethische Herausforderungen stellen sich hier in mindestens dreifacher Form. Erstens eröffnet ein mehrdimensionales Verständnis des Kindeswohls selbst bereits ein ethisches Spannungsfeld aufgrund der unterschiedlichen und nicht einfach auszubalancierenden Erfordernisse, die aus Teilhabe-, Schutz- und Befähigungsinteressen resultieren. Zweitens ergeben sich weitere ethische Herausforderungen mit Blick auf die Komplexität der digitalen Welt, die unterschiedliche Betroffenheit von Akteuren und die Verteilung von Verantwortung. Drittens müssen auch problematische Nebenwirkungen der Schutzmaßnahmen zur Alterskontrolle einer ethischen Analyse unterzogen werden, insbesondere hinsichtlich der Gewährleistung der Privatsphäre, Anonymität und Sicherheit aller Menschen, die digitale Dienste nutzen.

3.1 Schutz, Teilhabe und Befähigung in der digitalen Welt

Das Spannungsfeld von Schutz, Teilhabe und Befähigung ist grundlegend für die ethische Analyse des Kinder- und Jugendschutzes in der digitalen Welt. Jedwede vorgeschlagene Maßnahme muss sich vor dem Hintergrund dieses Spannungsfelds normativ rechtfertigen lassen. Sie darf die zum Teil gegenläufigen Aspekte nicht ohne Rücksicht auf die jeweils anderen optimieren und muss Grenzen so ziehen, dass den Eltern noch der notwendige Raum verbleibt, um die Schutz-, Teilhabe- und Befähigungsinteressen ihres Kindes individuell auszubalancieren. Letzteres ist nicht nur zur Wahrung des Elternrechts wichtig, sondern auch, weil eine allgemeine Regulierung weder die Persönlichkeit und Bedürfnisse der Kinder und Jugendlichen noch ihre konkrete Lebenssituation berücksichtigen kann.

3.1.1 Schutz

Wie eingangs dargestellt, herrscht Einigkeit darüber, dass Minderjährige aktuell in vielen Bereichen des Internets mit vielfältigen Risiken und nicht altersgerechten Inhalten konfrontiert werden, die sich nach den fünf Risikokategorien der Europäischen Kommission klassifizieren lassen. Insbesondere algorithmisch gestützte Plattformangebote mit einem auf Datensammlung und Werbung basierenden Geschäftsmodell wie Soziale Medien, aber beispielsweise auch Onlinespiele, Streamingdienste[28] und KI-Chatbots sind so gestaltet, dass die Aufmerksamkeit, das emotionale Engagement und letztlich die Verweildauer der Nutzenden maximiert werden (Stichwort: Aufmerksamkeitsökonomie).[29] Dabei kommen häufig Gestaltungselemente zum Einsatz, die eine exzessive Nutzung begünstigen können (z. B. personalisierte Empfehlungen, automatisches Abspielen von Inhalten, Endlos-Feeds, die zum Dauerscrollen verleiten, und psychologische Belohnungsmechanismen wie Likes, Streaks und zufällig ausgegebene virtuelle Gewinne, etwa aus digitalen „Schatzkisten“). Ebenso fördern viele Algorithmen die Verbreitung von Fehlinformationen und extremen oder aufwühlenden Inhalten, da diese aufgrund

[28] Insbesondere die problematische Nutzung von Onlinevideos hat zuletzt bei Kindern und Jugendlichen zugenommen. Laut der DAK-Mediensuchtstudie nutzte 2025 erstmals mehr als ein Viertel der 10- bis 17-Jährigen Streamingdienste, Reels und ähnliche Angebote auf riskante oder pathologische Weise. Das ist ein Anstieg von 60 Prozent im Vergleich zum Vorjahr. Die problematische Nutzung Sozialer Medien liegt schon seit 2022 auf ähnlich hohem Niveau. Ebenfalls mehr als ein Viertel dieser Altersgruppe nutzt inzwischen generative KI-Chatbots mehrmals pro Woche bis täglich. Vgl. Wiedemann et al. (2026).
[29] Vgl. Deutscher Ethikrat (2023) Kap. 7.

ihrer überraschenden oder emotionalisierenden Wirkung besonders aufmerksamkeitsbindend sind.

Diese Gestaltungsmerkmale bergen erhebliche Risiken für die individuelle Selbstbestimmung, die Gesundheit und die Persönlichkeitsrechte des Einzelnen. Mechanismen, die gezielt das Belohnungssystem stimulieren und Aufmerksamkeit binden, verstärken die Gefahr, dass die Nutzung dieser Technologien auf Kosten anderer wichtiger Aktivitäten ausgedehnt wird. Die algorithmische Bevorzugung emotional aufwühlender und extremer Inhalte wiederum erhöht deren Verbreitung und damit die mit solchen Inhalten verbundenen Risiken. Zu den beobachteten Folgen gehören beispielsweise die Entwicklung von Suchtverhalten, Erfahrungen digitaler Gewalt und eine Zunahme psychischer Leiden insgesamt. Aufgrund ihrer noch unausgereiften Identitätsentwicklung und Emotionsregulation sind Minderjährige gegenüber diesen Risiken weniger resilient und daher besonders gefährdet.[30]

Mit Blick auf die immer allgegenwärtiger werdenden KI-Chatbots, die ebenfalls überwiegend von großen Technologiekonzernen betrieben werden und auf das Sammeln möglichst vieler Daten sowie eine möglichst hohe Verweildauer ausgerichtet sind, kommen weitere Risiken hinzu, die unter anderem Lern- und Entwicklungsprozesse beeinträchtigen können (vgl. Abschnitt 3.1.3). Außerdem kann insbesondere der Aufbau einer emotionalen Bindung zu Chatbots Abhängigkeiten erzeugen[31] und die Vulnerabilität für schädliche Ratschläge, etwa zu selbstgefährdendem Verhalten, erhöhen, die solche Werkzeuge trotz Eindämmungsversuchen seitens der Anbieter nach wie vor abgeben.[32]

Die beschriebenen Gestaltungsmerkmale algorithmisch gestützter Plattformangebote bergen nicht nur Risiken für Minderjährige, sondern auch für die gesamtgesellschaftliche Entwicklung. Sie ermöglichen es beispielsweise, strategisch Narrative zu platzieren und zu verstärken, um Vertrauen zu erodieren, Gruppen gegeneinander auszuspielen und Urteils- sowie Entscheidungsprozesse zu verzerren. Diese Missbrauchsmöglichkeiten werden bereits von unterschiedlichen Akteuren in erheblichem Maße genutzt, um den demokratischen Willensbildungsprozess in der Gesellschaft manipulativ zu beeinflussen.[33] In Bezug auf Minderjährige sind diese Formen der Manipulation schon deshalb besonders aussichtsreich, weil algorithmisch gestützte Plattformangebote vor allem für jüngere Menschen zur wichtigsten Quelle für Informationen und Nachrichten sowie zu bedeutenden Kommunikationsräumen geworden sind.[34] Hinzu kommt, dass Heranwachsende gegenüber solchen Manipulationsversuchen anfälliger sein können.[35]

Angesichts dieser Ausgangslage besteht weitgehend Einigkeit darüber, dass die Konfrontation von Minderjährigen mit sie gefährdenden Inhalten, Akteuren und Mechanismen deutlich umfassender als bislang verhindert werden sollte. Allerdings gibt es unterschiedliche Auffassungen, welche Schutzkonzepte und Ansätze den Belangen des Kinder- und Jugendschutzes in der digitalen Welt am besten gerecht werden.

---

[30] Vgl. Orben et al. (2024).
[31] Laut der DAK-Mediensuchtstudie zeigen Kinder und Jugendliche mit hohen psychosozialen Belastungen ein stärker ausgeprägtes Bindungsverhalten bei der Nutzung von generativen KI-Chatbots. Sie geben deutlich häufiger an, dass sie Chatbots nutzen, um weniger einsam zu sein oder sich von negativen Gefühlen abzulenken, dass der Chatbot sie besser versteht als ein Mensch und dass sie ihm Dinge erzählen, die sie sonst niemandem oder nur engen Freundinnen oder Freunden sagen würden. Vgl. Wiedemann et al. (2026).
[32] Vgl. Common Sense Media (2025).
[33] Vgl. Deutscher Ethikrat (2023) 273 ff.
[34] Vgl. Behre et al. (2025); Rohleder (2023); Gesellschaft für Innovative Marktforschung (2022).
[35] Vgl. Kops et al. (2025); Ma et al. (2026).

Einführung eines pauschalen gesetzlichen Mindestalters für den Zugang zu bestimmten Diensten, insbesondere zu Sozialen Medien

Wie in der Einleitung näher dargestellt, steht in der gesellschaftlichen und politischen Diskussion derzeit der Gedanke im Vordergrund, der Konfrontation von Minderjährigen mit schädlichen Inhalten, Akteuren und Mechanismen durch die Einführung eines gesetzlichen Mindestalters für den Zugang zu Sozialen Medien entgegenzuwirken.

Von der Einführung einer solchen pauschalen Zugangsbeschränkung erhofft man sich, ein höheres Schutzniveau rascher oder effektiver zu erreichen als auf anderen Wegen. Angesichts der beschriebenen Geschäftsmodelle, die einer jugend- bzw. generell menschenfreundlicheren Gestaltung von Sozialen Medien und anderen digitalen Angeboten entgegenstehen, und der großen Marktmacht der beteiligten Konzerne gäbe es wenig Aussicht auf hinreichend rasche freiwillige Verbesserungen.[36] Der bestehende Rechtsrahmen sieht auf EU-Ebene zwar Eingriffsmöglichkeiten vor, um Veränderungen durchzusetzen. Hier steht allerdings die Befürchtung im Raum, dass diese Prozesse auch mit Blick auf die sich dynamisch entwickelnden Nutzungsmuster und die hohen Risiken für Minderjährige zu lange dauern, zumal es erheblichen politischen Widerstand gegen Regulierungsversuche, zum Beispiel seitens der USA, gibt.

Als weiteres Argument für ein gesetzliches Mindestalter wird angeführt, dass dieses Instrument beim Schutz vor Risiken in der analogen Welt effektiv dazu beigetragen hat, dass Minderjährige nicht oder zumindest weniger mit problematischen Situationen konfrontiert werden. Außerdem besteht die Hoffnung, dass ein Ausschluss Minderjähriger von bestimmten Diensten langfristig auch als Anreiz für Anbieter wirken könnte, sichere und jugendfreundliche digitale Räume zu gestalten. Denn erst mit der Bereitstellung von Angeboten, die den Anforderungen des Jugendschutzes genügen, würde die begehrte Zielgruppe „Kinder und Jugendliche“[37] wieder erreichbar werden.

Konsequente Umsetzung und Ausbau eines risikobasierten differenzierten Schutzkonzepts

Alternativ kommt ein risikobasiertes Schutzkonzept infrage, das statt pauschaler Altersgrenzen für bestimmte Dienste Risiken in den Vordergrund stellt, welche sich aus spezifischen Mechanismen, Funktionen und Inhalten dieser Dienste ergeben und an diese Risiken angepasste Schutzmaßnahmen vorsieht. Das entspricht im Wesentlichen dem risikobasierten Ansatz, der in Art. 28 Abs. 1 DSA angelegt ist und den die Europäische Kommission in ihren Leitlinien zu dieser Vorschrift näher ausformuliert. Die Leitlinien umfassen Maßnahmen wie standardmäßige private Kontoeinstellungen für Minderjährige, effektive Moderations- und Meldewerkzeuge, die jugendgerechte Anpassung algorithmischer Empfehlungssysteme, Download- und Screenshotsperren für von Minderjährigen gepostete Inhalte, Sicherheitsfunktionen gegen Cybermobbing oder die Deaktivierung suchterzeugender Designfunktionen. Auch bereits existierende Optionen für Minderjährigenkonten mit eingeschränkter Funktionalität, inhaltlichen Filtern und elterlichen Kontrollmöglichkeiten bei Diensten wie Instagram, TikTok und ChatGPT entsprechen prinzipiell diesem Ansatz.

Die bisherige Umsetzung solcher Schutzmaßnahmen durch die Plattformanbieter wird zwar bislang vielfach als unzureichend betrachtet. Dies wird insbesondere damit begründet, dass die

[36] Siehe hierzu paradigmatisch die Diskussion um die sogenannten „Facebook Files“: https://www.wsj.com/articles/the-facebook-files-11631713039 [21.05.2026].

[37] Laut Schätzungen betrugen die Werbeeinnahmen im Zusammenhang mit Minderjährigen auf sechs großen Social-Media-Plattformen im Jahr 2022 fast 11 Milliarden US-Dollar und waren über ein Viertel der Werbeeinnahmen von Snapchat, TikTok und YouTube auf junge Menschen zurückzuführen. Vgl. Raffoul et al. (2023).

DSA-Leitlinien nur empfehlenden Charakter hätten und es keine klaren Vorgaben zur Zuständigkeit und zu den jeweils einzusetzenden Technologien gäbe. Die Spielräume für eine bessere Implementierung inhalts- und mechanismenbezogener Schutzmaßnahmen sind allerdings aus Sicht derjenigen, die ein risikobasiertes differenziertes Schutzkonzept befürworten, noch nicht ausgeschöpft. Aktuell entwickeln sich die Bemühungen und Auseinandersetzungen zur besseren Durchsetzung bestehender Regulierungsinstrumente ebenso wie der politische Druck auf Anbieter sehr dynamisch, sodass eine zügige Verbesserung des Schutzniveaus auf diesem Weg realisierbar erscheint. So geht die Europäische Kommission etwa unter dem DSA zunehmend gegen Geschäftspraktiken großer Onlineplattformen vor, darunter TikTok, Instagram und Facebook sowie Snapchat, welche das Wohl von Minderjährigen beeinträchtigen.[38] In den USA wurden sowohl Meta als auch Google im März 2026 in zwei unterschiedlichen, auf verschiedenen Rechtsgrundlagen beruhenden Verfahren aufgrund von Mängeln beim Jugendschutz zu Schadensersatzzahlungen verurteilt.[39] Die gezielte Weiterführung und Intensivierung der Bemühungen, den DSA durchzusetzen unter konsequenter Ausschöpfung der darin vorgesehenen Ermittlungs- und Sanktionsmaßnahmen, hat also das Potenzial, das risikobasierte Schutzkonzept effektiver umzusetzen.

Bei der Beurteilung dieser beiden alternativen Schutzkonzepte ist im Blick zu behalten, dass kein Maßnahmenpaket alle Risiken vollständig ausschalten kann und es daher möglich sein sollte, problematische Vorgänge und Fehlentwicklungen rechtzeitig zu erkennen und einzudämmen. Dafür brauchen diejenigen, die für den Jugendschutz Verantwortung tragen, realistische Einblicke in die digitalen Räume, in denen Minderjährige sich bewegen, Raum für vertrauensvollen Austausch mit Kindern und Jugendlichen über ihre Erfahrungen in der digitalen Welt sowie Möglichkeiten, Anbieter und Personen bei Vorgängen zur Rechenschaft zu ziehen, die das Wohl Minderjähriger beeinträchtigen.

Erste Erfahrungen nach der Implementierung des Verbots Sozialer Medien für unter 16-Jährige in Australien („social media delay“) zeigen, dass viele Jugendliche Wege finden, um Zugangsbeschränkungen zu umgehen.[40] Wenn Minderjährige aber trotz Altersgrenzen über Mechanismen wie VPN (Virtual Private Network) oder mithilfe von älteren Geschwistern, Bekannten oder der Eltern doch Zugang zu altersbeschränkten Angeboten erhalten oder gar auf noch problematischere, zum Beispiel unregulierte oder illegale Alternativen ausweichen, wären solche Nutzungen und die damit verbundenen problematischen Folgen nicht mehr gut messbar und Gegenmaßnahmen schwieriger umzusetzen. Betroffene, die sich nur unerlaubt in bestimmten digitalen Sphären bewegen, könnten außerdem weniger offen über negative Erlebnisse sprechen. Gleichzeitig könnte das Schutzniveau auf Plattformen insgesamt sinken, wenn es aufgrund von Nutzungsverboten für Minderjährige keinen Anreiz mehr für Anbieter gäbe, ihre Inhalte jugendfreundlich zu gestalten, und man auch keine Handhabe hätte, Änderungen gesetzlich einzufordern.

3.1.2 Teilhabe

Eine ethische Beurteilung von Konzepten für den Kinder- und Jugendschutz in der digitalen Welt muss auch berücksichtigen, wie sich Schutzmaßnahmen auf die Teilhabemöglichkeiten von Minderjährigen auswirken. Digitale Technologien sind sowohl für Erwachsene als auch für

[38] https://ec.europa.eu/commission/presscorner/detail/en/ip_26_312 [05.05.2026]; https://ec.europa.eu/commission/presscorner/detail/en/ip_26_920 [05.05.2026]; https://ec.europa.eu/commission/presscorner/detail/en/ip_26_723 [05.05.2026].
[39] Vgl. Kang und Tan (2026); Kang et al. (2026).
[40] Vgl. Molly Rose Foundation (2026).

Kinder und Jugendliche so stark in das heutige Leben eingebunden, dass sie eine wichtige Rolle bei der Erfüllung grundlegender Informations-, Kommunikations- und weiterer sozialer Bedürfnisse spielen. Das gilt vor allem für die 12- bis 19-Jährigen.[41] Für sie sind Dienste wie WhatsApp, TikTok, Instagram und YouTube mittlerweile nicht nur Kommunikationsmedien, sondern auch wichtige Quellen für Nachrichten und Informationen. 93 Prozent nutzen ihr Smartphone täglich für durchschnittlich fast vier Stunden und vor allem für Messengerdienste und Soziale Medien. Auch KI-Tools wie ChatGPT werden zunehmend genutzt: 2025 bereits von 84 Prozent der Jugendlichen (2023: 38 Prozent), vor allem für Schulaufgaben und zur Informationssuche. Bei jüngeren Kindern spielt die digitale Welt ebenfalls eine große Rolle.[42] 63 Prozent der 10- bis 11-Jährigen verfügen inzwischen über ein eigenes Smartphone, 81 Prozent nutzen regelmäßig WhatsApp, 46 Prozent TikTok und 26 Prozent Instagram. Bei den 8- bis 9-Jährigen besitzen immerhin 33 Prozent ein Smartphone, 64 Prozent nutzen regelmäßig WhatsApp und 17 Prozent TikTok. Gleichzeitig sind angesichts der gesellschaftlich insgesamt zunehmenden Dominanz von digitalen Angeboten wie Sozialen Medien und Messengerdiensten manche Informationen und Angebote über „klassischere“ Medien nicht mehr im gleichen Ausmaß oder in der gleichen Qualität verfügbar. Viele Organisationen, Unternehmen und Personen des öffentlichen Lebens erstellen beispielsweise zahlreiche Inhalte exklusiv für Soziale Medien. Austausch und Absprachen in sozialen Gruppen laufen inzwischen häufig vorwiegend über Chatgruppen wie zum Beispiel Klassen- oder Familienchats.

Maßnahmen für besseren Jugendschutz im Internet müssen vor dem Hintergrund dieser starken und steigenden digitalen Durchdringung berücksichtigen, wie die Informations-, Kommunikations- und sozialen Bedürfnisse von Kindern und Jugendlichen erfüllt und wie ihre Rechte auf Wohlergehen, Information, Bildung und freie Meinungsäußerung gewahrt werden können. Auch mit Blick auf diese Teilhabeinteressen sind mehrere Ziele relevant, die teils in Spannung zueinander stehen.

Positive digitale Teilhabemöglichkeiten bewahren und ausbauen

Digitale Räume und Werkzeuge bringen nicht nur die erwähnten Risiken für Kinder und Jugendliche mit sich, sondern eröffnen auch zahlreiche Chancen. Informationen können unabhängig von lokal zugänglichen Bibliotheken auch zu speziellen Themen und aus unterschiedlichen Perspektiven beschafft werden. Es gibt vielfältige Möglichkeiten, mit anderen Menschen unabhängig von geografischer Nähe zu spezifischen Interessen und Anliegen in den Austausch zu treten. Soziale Medien und Messengerdienste werden von Kindern und Jugendlichen aktiv zur Pflege von Freundschaften genutzt und können somit Werkzeuge sein, um emotionale Unterstützung und Zugehörigkeit zu erleben. Sie bieten zudem Raum für freie und öffentlichkeitswirksame Meinungsäußerung sowie für kreative Selbstentfaltung. KI-Werkzeuge ermöglichen die Gestaltung und Umsetzung personalisierter Lernstrategien und eröffnen ebenfalls erweiterte Möglichkeiten zur kreativen Selbstentfaltung. Insbesondere für junge Menschen, denen lokal weniger Kontaktmöglichkeiten, Informationsangebote und sonstige soziale Infrastrukturen zur Verfügung stehen, weil sie beispielsweise in Gebieten mit geringer Bevölkerungsdichte leben oder chronisch erkrankt sind, können digitale Teilhabemöglichkeiten sehr wertvoll sein. Gleiches gilt für Minderjährige mit besonderen Interessen oder Bedürfnissen, die sich vor Ort nicht immer ohne Weiteres mit Gleichgesinnten oder ähnlich Betroffenen vernetzen können (z. B. zu queeren Themen, Neurodiversität oder Behinderungen). Auch wenn es an Unterstützung oder

[41] Vgl. Feierabend et al. (2025a).
[42] Vgl. Feierabend et al. (2025b); Kieninger et al. (2024).

Verständnis durch Erwachsene im persönlichen Umfeld mangelt, können digitale Teilhaberäume einen Ausgleich bieten.

Viele der genannten Chancen könnten in jugendgerechter gestalteten, digitalen Räumen besser verwirklicht werden als unter den aktuellen Bedingungen mit ihren zahlreichen problematischen Gestaltungsmerkmalen. Doch solange es keine besseren Alternativen gibt, würde ein Ausschluss von digitalen Diensten, die aktuell eine große Rolle für die Teilhabe Minderjähriger spielen, die Rechte von Kindern und Jugendlichen auf Wohlergehen, Information, Bildung und freie Meinungsäußerung insgesamt beeinträchtigen. Diese Effekte könnten zudem ohnehin marginalisierte Gruppen noch stärker treffen.

Analoge Teilhabemöglichkeiten wieder stärken

Die Teilhabeinteressen von Kindern und Jugendlichen können nicht rein digital verwirklicht werden. Zeit, die Kinder und Jugendliche mit der Nutzung digitaler Angebote und Aktivitäten verbringen, fehlt womöglich für andere Aktivitäten, bei denen sie in der realen Welt Teilhabe erleben und praktizieren können. Längsschnittstudien zeigen tatsächlich, dass Umverteilungen zwischen analogen und digitalen Aktivitäten stattfinden. Der Anteil der 12- bis 19-Jährigen, die sich mindestens mehrmals pro Woche mit Freunden treffen, ist beispielsweise zwischen 2005 und 2025 von 88 Prozent auf 64 Prozent gesunken, während die häufige Internetnutzung in dieser Zeit von 60 Prozent auf 96 Prozent gestiegen ist. Andere analoge Aktivitäten wie zum Beispiel Sport und kreative Hobbies sind hingegen stabil geblieben.[43] Gerade bei problematischer Nutzung digitaler Medien ergeben sich durch Interventionen, die die Bildschirmzeit zugunsten anderer Aktivitäten beschränken, schnell Verbesserungen des Wohlbefindens.[44] Mit Initiativen, die analoge Angebote fördern oder überhaupt erst verfügbar machen, wird daher die Hoffnung verbunden, dass eine solche Stärkung von Offlineaktivitäten insgesamt zu mehr Wohlbefinden und Ausdrucksmöglichkeiten für Kinder und Jugendliche beiträgt. Bessere Angebote zur Information, Bildung und freien Meinungsäußerung im analogen Raum könnten auch etwaige altersabhängige Nutzungsbeschränkungen für bestimmte digitale Angebote zumindest teilweise ausgleichen.

Beteiligung von Jugendlichen an Entscheidungen über die Nutzung digitaler Technologien

Entscheidungen über den Zugang und die Möglichkeit der Nutzung digitaler Technologien sind für die Lebenswirklichkeit von Kindern und Jugendlichen von großer und unmittelbarer Bedeutung. Daher haben Kinder und Jugendliche das Bedürfnis, bei solchen Entscheidungen ihre eigene Perspektive einbringen zu können. Um diesem berechtigten Teilhabebedürfnis gerecht zu werden, sind sie an den Entscheidungen über den Zugang und die Möglichkeiten zur Nutzung digitaler Technologie altersadäquat zu beteiligen. Dies gilt vor allem für Gespräche innerhalb der Familie (vgl. Abschnitt 3.2.3), sollte aber bei Jugendlichen auch eine angemessene Beteiligung an politischen Entscheidungen beinhalten. Ansätze in diese Richtung gibt es bereits. So hat die Unabhängige Expertenkommission „Kinder- und Jugendschutz in der digitalen Welt“ Workshops mit Jugendlichen durchgeführt, um deren Erfahrungen und Wünsche in ihre Beratungen und Empfehlungen einfließen zu lassen.[45] Auch beim Special Panel on Child Safety

[43] Vgl. Feierabend und Rathgeb (2005); Feierabend et al. (2025a).
[44] Vgl. Hunt et al. (2018); Davis und Goldfield (2025).
[45] https://www.bmbfsfj.bund.de/bmbfsfj/themen/kinder-und-jugend/kinder-und-jugendschutz/junge-menschen-beteiligen-wenn-es-um-digitalen-kinder-und-jugendschutz-geht--280504 [21.05.2026].

Online der Europäischen Kommission sind junge Menschen über das Youth Advisory Board der Kommissionspräsidentin eingebunden.[46]

3.1.3 Befähigung

In der Kindheit und Jugend werden wichtige Fähigkeiten für das gesamte Leben erworben und weiterentwickelt. Daher haben Bedingungen und Maßnahmen, die diese Prozesse fördern oder behindern, besondere ethische Relevanz. Befähigung ist eng mit Teilhabe verbunden, da sich Lern- und Entwicklungsprozesse nicht nur in formellen Bildungssituationen, sondern im gesamten Handeln und Erleben junger Menschen vollziehen. Im Zusammenhang mit Sozialen Medien und weiteren digitalen Technologien ist vor diesem Hintergrund zum einen bedeutsam, wie sich die Nutzung solcher Angebote insgesamt auf Lern- und Entwicklungsprozesse auswirkt. Zum anderen stellt sich die Frage, wie die Fähigkeiten junger Menschen zur sinnvollen Nutzung digitaler Medien und im Umgang mit deren Herausforderungen, Risiken und Gefahren am besten entwickelt und gestärkt werden können. Zu beiden Aspekten lassen sich Befähigungsinteressen identifizieren.

Lernen, Wissens- und Kompetenzerwerb schützen und fördern

Metaanalysen zeigen ein differenziertes Bild zur Wirkung digitaler Werkzeuge auf die Lernleistung von Schülerinnen und Schülern. Insbesondere deren außerschulische Nutzung wirkt sich hinderlich auf Lernerfolge aus, vor allem bei jüngeren Kindern sowie Minderjährigen aus bildungsferneren Haushalten. Faktoren mit negativen Effekten auf die schulische Leistung sind hierbei unter anderem die jeweilige Bildschirmzeit, die Bildschirmzeit der Eltern, Cyberbullying, Smartphone-Sucht und auch Soziale Medien. Im schulischen Kontext ergeben sich durch das Ablenkungspotenzial von Smartphones oder das Lesen an digitalen Geräten ebenfalls negative Auswirkungen. Mit dem gezielten Einsatz von Lerntechnologien wie zum Beispiel technikunterstütztes Feedback, intelligente Tutorsysteme oder interaktive Lernvideos sind hingegen positive Effekte verbunden.[47]

Die Wahrnehmung, dass die Nutzung von Smartphones in der Schule zu Aufmerksamkeits- und Konzentrationsproblemen führt, hat bereits mehrere Bundesländer dazu veranlasst, die Nutzung solcher Geräte in Schulen insgesamt oder für bestimmte Schultypen oder Altersklassen zu verbieten oder stark einzuschränken.[48] Auch weitere Risiken wie zum Beispiel die unzulässige Anfertigung und Nutzung von Aufnahmen für Cybermobbing können als Argument angeführt werden, Schulen als besonders geschützte Räume des Lernens und der persönlichen Entwicklung von Kindern und Jugendlichen weitgehend[49] frei von der privaten Nutzung mobiler Endgeräte zu halten. Regelungen, bei denen private Geräte während des Aufenthalts in der Schule abgegeben werden, hätten den Vorteil, Lehrkräfte überwiegend von der Aufgabe zu entlasten, potenzielle Verstöße festzustellen und zu ahnden. Soweit die Nutzung digitaler Technologien im Unterricht nicht auf schulischen Endgeräten erfolgen kann, könnten die privaten Geräte für diese Zwecke wieder ausgehändigt werden.

---

[46] https://commission.europa.eu/topics/digital-economy-and-society/protect-our-children-also-online_en [21.05.2026].
[47] Hattie 2008; 2023 (zitiert nach Unabhängige Expertenkommission „Kinder- und Jugendschutz in der digitalen Welt“ (2026) 33 ff.).
[48] Vgl. Brand (2026) Abschn. 3.
[49] Ausnahmen können beispielsweise Schülerinnen und Schüler betreffen, bei denen die private Gerätenutzung einen medizinischen Zweck verfolgt oder der Gleichstellung dient.

Mit Blick auf die stark zunehmende Verwendung generativer KI-Tools durch Minderjährige[50] gibt es zum einen die begründete Sorge, dass eine unsachgemäße, in erster Linie auf die Vermeidung mentaler Anstrengungen gerichtete Nutzung Lernprozesse negativ beeinflussen oder sogar zum Abbau von Fähigkeiten führen kann (Deskilling).[51] Minderjährige laufen hier im Gegensatz zu Erwachsenen Gefahr, grundlegende Kompetenzen gar nicht erst zu erwerben, wenn Aufgaben vor allem in entscheidenden Entwicklungsphasen übermäßig an KI abgegeben werden.[52] Der Einsatz von KI kann jedoch bei einer Fokussierung beispielsweise auf Coaching- und Reflexionsprozesse auch lernförderlich ausfallen, sodass die Wirkung entscheidend von den tatsächlichen Nutzungsmustern abhängen dürfte.[53] Angesichts der hohen Komplexität und Dynamik der Entwicklungen spricht viel dafür, Ressourcen und Strukturen bereitzustellen, die es Bildungseinrichtungen ermöglichen, flexibel auf Entwicklungen zu reagieren, um Bildungsprozesse und Lernerfolge im digitalen Wandel mit einer Mischung aus digitalen und analogen Ansätzen und Werkzeugen möglichst optimal zu gestalten.

Soziale Kompetenzbildung schützen und fördern

Mechanismen und Bedingungen, die die Teilhabe von Minderjährigen in digitalen und analogen Situationen fördern oder behindern, wirken sich auch auf die Entwicklung sozialer Kompetenzen aus, da diese durch Interaktion mit anderen Menschen eingeübt werden. Insofern sind die im Abschnitt zur Teilhabe genannten Ziele auch für die soziale Befähigung von Kindern und Jugendlichen relevant.

Zusätzlich gewinnen weitere Aspekte an ethischer Relevanz, die insbesondere die direkten Wechselwirkungen zwischen der digitalen Mediennutzung und persönlichen Interaktionen betreffen. Hier sind zum einen Situationen zu nennen, in denen Menschen ihre Aufmerksamkeit auf digitale Geräte statt auf ihre Mitmenschen richten. Dieses, auch als Phubbing bezeichnete Phänomen hat negative Auswirkungen auf das Wohlbefinden von Minderjährigen, sowohl wenn sie es selbst ausüben als auch wenn es ihnen widerfährt.[54] Zum anderen steht im Zusammenhang mit der steigenden Nutzung von Messengerdiensten, Sozialen Medien und neuerdings vor allem auch generativer KI die Sorge im Raum, dass eine exzessive Nutzung die Entwicklung sozialer Kompetenzen und die Bildung stabiler Sozialkontakte beeinträchtigen kann. So gibt es Hinweise, dass junge Menschen sich zunehmend weniger trauen, ohne digitale Unterstützung wie visuelle Filter und KI-Formulierungshilfen zu kommunizieren und sich zu präsentieren.[55] Insbesondere mit Blick auf KI-Chatbots, die eine persönliche Beziehung simulieren, kommt hinzu, dass diese zunehmend anstelle von Menschen als persönliche Ratgeber oder als emotionale Ansprechpartner genutzt werden.[56] Die gezielte Schaffung und Förderung von Räumen und Situationen, in denen junge Menschen ohne Rückgriff auf digitale Technologien mit anderen interagieren, könnte daher dazu beitragen, negative Konsequenzen für die Entwicklung sozialer Fähigkeiten zu mindern oder auszugleichen.

Digitale Medienkompetenz stärken

Digitale Medienkompetenz von Kindern und Jugendlichen sowie von Erwachsenen, die sie in ihrem Heranwachsen begleiten, ist nicht nur wichtig, um digitale Werkzeuge so zu nutzen, dass

[50] Vgl. Feierabend et al. (2025a).
[51] Vgl. Stadler et al. (2024); Kosmyna et al. (2025).
[52] Vgl. Burns et al. (2026).
[53] Vgl. OECD (2026); Scheiter et al. (2025).
[54] Vgl. Nuñez und Radtke (2024); Wiedemann et al. (2025).
[55] Vgl. Institut für Jugendkulturforschung und Kulturvermittlung (2024); (2026).
[56] Vgl. Yu et al. (2025); Wiedemann et al. (2026).

sie Lern- und Entwicklungspotenziale möglichst unterstützen statt zu behindern. Sie ist auch essenziell, um alle Beteiligten, insbesondere junge Menschen selbst, zu befähigen, mit den vielfältigen beschriebenen Risiken und Gefahren umzugehen. Minderjährige müssen lernen, problematische Inhalte, Mechanismen und Verhaltensweisen bei sich selbst und bei anderen nicht nur möglichst frühzeitig zu erkennen, sondern auch angemessen auf problematische Situationen zu reagieren, selbst Abhilfe zu schaffen oder sich von geeigneten Stellen Hilfe zu holen. Bislang sind sowohl die Ausprägung solcher Fähigkeiten als auch die Unterstützung, die junge Menschen bei der Entwicklung dieser Kompetenzen erfahren, unzureichend. So wissen viele Jugendliche zwar, dass Algorithmen existieren und sie bei der Nutzung von Sozialen Medien wie auch KI-Tools beeinflussen, reflektieren darüber aber kaum und erleben dementsprechend auch wenig kompetente Handlungssteuerung und Selbstwirksamkeit in diesem Bereich.[57] In der achten Klasse erreichen mehr als 40 Prozent der Schülerinnen und Schüler in Deutschland nur rudimentäre digitale Kompetenzen. Trotz verstärkter Digitalisierung in Schulen sind diese Kompetenzen seit 2018 sogar gesunken.[58] Darüber hinaus gibt es Hinweise, dass die Kompetenzen sozial ungleich verteilt sind und dass pädagogische Konzepte bei der Vermittlung von Medienkompetenzen wie kritischer Quellenbewertung und Datenschutz Mängel aufweisen.[59] Angesichts dieser Lage und der Bedeutung von Medienkompetenz für die Befähigung und Resilienz junger Menschen im Umgang mit digitalen Gefahren und Risiken sind hier Verbesserungen essenziell.

3.1.4 Zwischenfazit: Vereinbarkeit von Schutz, Teilhabe und Befähigung

Die in den vorigen Abschnitten dargelegten Interessen und Ziele lassen sich mit einzelnen Maßnahmen erkennbar nicht alle gleichermaßen erfüllen. Die Priorisierung bestimmter Maßnahmen kann sich zudem negativ auf andere Interessen und Ziele auswirken. Jugendschutzmaßnahmen sollten möglichst nicht dazu führen, dass Jugendliche weniger am sozialen Austausch teilnehmen, sich vermehrt ausgeschlossen fühlen, weniger lernen, kritisch mit Online-Informationen umzugehen, und später im Berufsleben digitale Kommunikationsformen weniger beherrschen. Daher sollten jegliche erwogenen Maßnahmen sorgfältig mit Blick auf alle drei Dimensionen des Kindeswohls – Schutz, Teilhabe und Befähigung – untersucht und mögliche negative Konsequenzen ihrer Einführung, aber auch ihrer Unterlassung berücksichtigt werden.

Insbesondere pauschale Nutzungsverbote für bestimmte Dienste, die über bereits etablierte Mindestaltersgrenzen hinausgehen, würden Einschränkungen der Teilhabemöglichkeiten vieler junger Menschen im digitalen Raum bedeuten. Gleichzeitig könnten sie zu Ausweichbewegungen führen, die das Schutzbestreben unterlaufen und eine transparente Auseinandersetzung mit problematischen Merkmalen digitaler Angebote sowie deren Umgestaltung erschweren. Denn selbst gut funktionierende Zugangsbeschränkungen lassen sich mit genügend Kreativität umgehen, und die Motivation für solche Umgehungen wächst, je umfassender die Einschränkung ist. Risikobasierte Ansätze zur inhalts- und mechanismenspezifischen Risikokontrolle sind demgegenüber eher mit den Teilhabe- und Befähigungsinteressen von Kindern und Jugendlichen vereinbar und mindern aufgrund der damit verbundenen voraussichtlich höheren Akzeptanz auch das Risiko einer Verlagerung digitaler Aktivitäten in weniger regulierte Bereiche.

---

[57] Vgl. Kelly (2025). Vergleichsdaten für Erwachsene legen nahe, dass sich diese Problematik im Lebensverlauf nicht einfach „auswächst“: Auch in der erwachsenen Bevölkerung bestehen relevante Schwächen bei der Informationssuche und -bewertung sowie beim Verständnis algorithmischer Auswahlmechanismen, wobei deutliche Unterschiede nach Alter, Bildung und sozialem Status bestehen. Vgl. Eder und Sjøvaag (2024).
[58] Vgl. Eickelmann et al. (2024) 61 ff.
[59] Vgl. Eickelmann et al. (2024) 73 ff., 135 f.

Wie effektiv bestimmte Maßnahmen sind, welche möglichen Neben- und Wechselwirkungen auftreten können, ob sie mit anderen Aspekten des Kindeswohls in Konflikt stehen, und wie konkrete Ansätze zur Förderung des Kindeswohls insgesamt ethisch zu bewerten sind, hängt allerdings von weiteren Faktoren ab, die im folgenden Abschnitt näher betrachtet werden.

3.2 Ethische Herausforderungen durch soziotechnische Komplexität

Eine Verbesserung von Schutz, Teilhabe und Befähigung Minderjähriger in der digitalen Welt ist ethisch in mehrfacher Hinsicht herausfordernd. Sie muss erstens der Komplexität und Dynamik der digitalen Lebenswelt gerecht werden, zweitens der Unterschiedlichkeit der Bedürfnisse, Verletzlichkeiten und Fähigkeiten der involvierten Personen Rechnung tragen und drittens die verschiedenen auf individueller, organisationaler und staatlicher Ebene agierenden Akteure so in die Pflicht nehmen, dass sie bei der Erfüllung dieser Aufgabe effektiv zusammenwirken.

3.2.1 Vielfalt und Dynamik der digitalen Lebenswelt

Der aktuell starke Fokus des öffentlichen und politischen Diskurses auf Soziale Medien greift zu kurz. Viele Kinder und Jugendliche nutzen in ihrem Alltag ein breites Portfolio unterschiedlichster digitaler Technologien. Neben Sozialen Medien sind dies etwa einschlägige Messengerdienste (v. a. WhatsApp), Onlinespiele und Streamingplattformen sowie zunehmend Anwendungen der generativen KI, insbesondere Chatbots, aber auch Bild- und Videogeneratoren. Solche Anwendungen sind ebenfalls Quellen digitaler Risiken und Gefahren, werden teils von denselben großen Technologiefirmen betrieben, die auch hinter beliebten Sozialen Medien stehen, und sind außerdem über die in der gesamten Onlinewelt tief integrierten Trackingdienste unmittelbar vernetzt. Die Übergänge zwischen unterschiedlichen Diensten sind zudem fließend. So bietet WhatsApp inzwischen die Möglichkeit, öffentliche Kanäle zu abonnieren oder zu gestalten, der Musikdienst Spotify enthält Kopien von YouTube-Kurzvideos und Onlinespiele, die intensiv von Kindern genutzt werden, erlauben gleichzeitig beispielsweise durch Chatfunktionen Interaktionen mit Fremden.

Das sich hochdynamisch entwickelnde Portfolio generativer KI-Anwendungen bringt zusätzlich die besondere Herausforderung mit sich, dass KI-Angebote immer stärker in sämtliche Bereiche der digitalen Lebenswelt integriert und somit allgegenwärtig werden. KI-Chatbots und Angebote zum Zusammenfassen und Generieren von Inhalten sind inzwischen fester Bestandteil vieler alltäglich genutzter Softwareanwendungen und Plattformen, von Suchmaschinen über Messengerdienste und Internetbrowser bis hin zu Textverarbeitungsprogrammen, und werden auch zunehmend tiefer in die Software von Smartphones und anderen digitalen Endgeräten eingebunden, über die letztlich alle digitalen Aktivitäten laufen.[60] Sollten solche Angebote oder einige ihrer Funktionen für bestimmte Altersgruppen als ungeeignet eingestuft werden, wären mit einer altersgestaffelten Regulierung noch komplexere Herausforderungen verbunden als bei den aktuell vornehmlich diskutierten Nutzungsbeschränkungen für Soziale Medien. Die Eindämmung der mit diesen Angeboten verbundenen Risiken ist entsprechend noch deutlich schwieriger als für Soziale Medien: aufgrund der zuvor geschilderten tiefen Einbettung in vielfältige Lebensbereiche und andere Technologien, aber auch weil man sich für die Nutzung von

[60] https://android-developers.googleblog.com/2026/02/the-intelligent-os-making-ai-agents.html [21.05.2026].

KI-Werkzeugen häufig nicht registrieren muss, diese zudem nicht in Plattformen eingebettet sein müssen und dann nicht der Regulierung des DSA unterliegen.

Wie mit diesen Herausforderungen umzugehen ist, ist eine Abwägungsfrage. Wichtig ist jedoch, hierbei zusätzlich Wechselwirkungen in den Blick zu nehmen. Verbietet man den Zugang zu Sozialen Medien, lässt aber KI-Chatbots unberührt, läuft man Gefahr, dass Kinder und Jugendliche für ihre informationellen, kommunikativen und emotionalen Bedürfnisse zunehmend auf solche Angebote zurückgreifen, mit möglicherweise noch problematischeren Konsequenzen beispielsweise in Bezug auf emotionale Abhängigkeit, Suchtgefahren sowie einen Verlust kognitiver oder sozialer Kompetenzen.

3.2.2 Betroffenheit und Vulnerabilität unterschiedlicher Akteure

Kinder und Jugendliche werden zu Recht als eine besonders vulnerable Gruppe gesehen, welche vor den aufmerksamkeitsökonomischen Mechanismen insbesondere gewinnorientierter digitaler Plattformen geschützt werden soll. Allerdings betrifft die Anfälligkeit für solche Mechanismen zum einen alle Altersgruppen und zum anderen sind nicht alle Minderjährigen im gleichen Ausmaß betroffen. Kinder und Jugendliche mit besonderen Themen oder Bedürfnissen, zu denen sie im persönlichen Umfeld keine oder nicht genügend Unterstützung erfahren, Minderjährige, die von Armut oder familiären Konflikten betroffen sind, oder solche, deren Eltern aus anderen Gründen wenig positive Begleitung bei digitalen Schutzmaßnahmen oder bei der Vermittlung von Medienkompetenz anbieten können oder wollen, sind gegenüber vielen Risiken und Gefahren der digitalen Welt verletzlicher als junge Menschen, auf die solche Faktoren nicht zutreffen.

Als zweite betroffene Gruppe erscheinen die Eltern. Sie sind bei der Vermittlung von Medienkompetenzen und der Durchsetzung von Nutzungsbeschränkungen zuvorderst herausgefordert und können ebenfalls je nach Lebenssituation auf sehr unterschiedliche Ressourcen zugreifen, um sich hier zu engagieren. Nicht nur die Zeit, das Wissen und die technische Ausstattung, die zur Verfügung stehen, um eigene Kinder vor digitalen Risiken und Gefahren zu schützen, variieren erheblich, sondern auch die emotionalen Kapazitäten, um Konflikte über die Mediennutzung in der Familie zielführend auszutragen. Hinzu kommt, dass die Einflussmöglichkeiten selbst engagierter Eltern begrenzt sind, da insbesondere ab dem Jugendalter soziale Dynamiken zwischen Gleichaltrigen bei der Entstehung digitaler Nutzungsmuster eine zunehmend größere Rolle spielen.

Lehrkräfte und andere in der Jugendbildung und -begleitung engagierte Erwachsene und die Institutionen, in denen sie agieren, wie zum Beispiel Schulen, Träger der Jugendhilfe, Behörden, spielen ebenfalls eine wichtige Rolle bei der Um- und Durchsetzung von Jugendschutz in der digitalen Welt. Sie sind gleichzeitig selbst von den damit verbundenen Herausforderungen betroffen, insbesondere dann, wenn sie mit unzureichenden zeitlichen, finanziellen und fachlichen Ressourcen Risiken und Gefahren eindämmen sollen, die durch kaum kontrollierbare und sich rasant fortentwickelnde marktgetriebene Technologien ausgelöst werden, die fast sämtliche Alltagssituationen immer stärker und rascher durchdringen.

Zum Schluss kann die Gesellschaft auch insgesamt als vulnerabel gelten, wenn ihren jüngsten Mitgliedern durch diese Entwicklungen Schäden drohen. Die Vermeidung dieser Schäden ist bereits insofern herausfordernd, als die Handlungskompetenz auf politischer Ebene auf eine Vielzahl unterschiedlicher Akteure verteilt und dadurch fragmentiert ist. Vor allem aber müssen die dafür notwendigen Maßnahmen gegen die Macht international agierender Technologiekonzerne durchgesetzt werden.

3.2.3 Multiakteursverantwortung

Um Schutz, Teilhabe und Befähigung von Kindern und Jugendliche in digitalen Welten bestmöglich zu gewährleisten, bedarf es des gelingenden Zusammenwirkens verschiedener Akteure. Für derartige Situationen hat der Deutsche Ethikrat das Konzept der Multiakteursverantwortung[61] entwickelt, in dem die Verantwortlichkeiten der verschiedenen auf individueller, organisationaler und staatlicher Ebene agierenden Akteure klar benannt und voneinander abgegrenzt, aber auch in ihren Wechselwirkungen berücksichtigt werden.

Individuelle Ebene

Auf der individuellen Ebene sind in erster Linie die Eltern dafür verantwortlich, ihre Kinder vor Gefahren aus der digitalen Welt zu schützen und zugleich für eine hinreichende digitale Teilhabe und Befähigung ihrer Kinder Sorge zu tragen. Ihnen vertraut das Grundgesetz in Art. 6 Abs. 2 Satz 1 die Pflege und Erziehung ihrer Kinder an, zu der heute auch die Gestaltung der Beziehung der Kinder zur digitalen Welt gehört. Bei der Wahrnehmung dieser Verantwortung sind die Eltern dem Kindeswohl verpflichtet. Sie haben bei den ihnen im Rahmen der elterlichen Sorge obliegenden Entscheidungen über den Zugang zu digitalen Angeboten die Schutz-, Teilhabe- und Befähigungsinteressen ihrer Kinder so auszubalancieren, dass deren Wohl in bestmöglichem Maße gefördert wird.

Aufgrund ihres Erziehungsrechts können Eltern die Beurteilung, was dem Wohl ihres Kindes dienlich ist und was nicht, grundsätzlich nach Maßgabe ihrer jeweiligen Erziehungsvorstellungen vornehmen. Die staatliche Gemeinschaft wacht zwar nach Art. 6 Abs. 2 Satz 2 des Grundgesetzes darüber, dass Eltern ihrer Aufgabe und Verantwortung zur Pflege und Erziehung der Kinder gerecht werden. Aber diese Wächterfunktion berechtigt nur dann zu Eingriffen in das Elternrecht, wenn Erziehungsvorstellungen und darauf beruhende Entscheidungen der Eltern das Kindeswohl gefährden, das heißt, wenn eine gegenwärtige, erhebliche Gefahr für das körperliche, geistige oder seelische Wohl eines Minderjährigen vorliegt. Die Gefahr muss sich bei weiterer Entwicklung mit hoher Wahrscheinlichkeit zu einer erheblichen Schädigung auswachsen. Leichte Erziehungsfehler oder unbestimmte und unsichere mögliche Beeinträchtigungen lösen das Wächteramt nicht aus. Lässt sich nicht eindeutig beurteilen, ob eine Entscheidung dem Wohl des Kindes dienlich ist oder nicht, so hat der Staat das Erziehungsrecht der Eltern zu respektieren.

Dementsprechend ist den Eltern bei der Entscheidung, zu welchem Zeitpunkt und in welchem Maße sie ihren Kindern den Zugang zu digitalen Angeboten ermöglichen, ein erheblicher Gestaltungsspielraum zuzubilligen. Die für diese Entscheidung vorzunehmende Abwägung der Schutz-, Teilhabe- und Befähigungsinteressen des Kindes ist zwar in begrenztem Maße objektivierbar. Es gibt aber einen relativ breiten Bereich, in dem man mit jeweils guten Gründen unterschiedlicher Auffassung sein kann, ob dem Schutz- oder dem Teilhabe- bzw. Befähigungsinteresse der Vorrang gebührt. Innerhalb dieses Bereichs ist es Aufgabe und Verantwortung der Eltern, zu beurteilen, ob der Zugang zu den betreffenden digitalen Angeboten dem Wohl ihres Kindes dienlich ist oder nicht.

Dem steht nicht entgegen, dass es sicherlich Eltern gibt, die es als Entlastung empfinden und begrüßen würden, wenn der Staat ihnen diese Verantwortung abnehmen und den Zugang zu digitalen Angeboten für Minderjährige mehr oder weniger vollständig regulieren würde. Das

[61] Vgl. Deutscher Ethikrat (2017) 239 ff.

Interesse dieser Eltern, den Zugang ihrer Kinder zu digitalen Angeboten wegen des dafür erforderlichen Zeitaufwands und des damit verbundenen familiären Konfliktpotenzials nicht selbst regeln zu müssen, ist zwar durchaus nachvollziehbar. Es rechtfertigt jedoch keine Beschneidung des Gestaltungsspielraums derjenigen Eltern, die nach Maßgabe ihrer eigenen Erziehungsvorstellungen selbst beurteilen wollen und sollen, ob der Zugang zu den betreffenden digitalen Angeboten dem Wohl ihres Kindes dienlich ist oder nicht.

Um diese Beurteilung sachgerecht vornehmen zu können, sollten Eltern ihre Kinder an der Entscheidung über den Zugang zu digitalen Angeboten altersadäquat beteiligen. Insbesondere die Teilhabe- und Befähigungsinteressen lassen sich in aller Regel besser beurteilen und gewichten, wenn sich die Eltern von ihren Kindern ernsthaft erklären lassen, aus welchem Grund und zu welchem Zweck sie Zugang zu dem betreffenden Angebot haben möchten. Auch individuelle, familiale Regeln zur Nutzung und zu zeitlichen und inhaltlichen Grenzen können Teil dieses Dialogs sein. Darüber hinaus ist eine altersadäquate Beteiligung vor allem deshalb geboten, um dem wachsenden Selbstbestimmungsbedürfnis von Kindern und Jugendlichen gerecht zu werden und sie durch die zunehmende Übertragung von Verantwortung auf den in vollem Maße selbstbestimmten Umgang mit digitalen Angeboten angemessen vorzubereiten.

Neben den Eltern haben auf der individuellen Ebene auch Lehrkräfte und andere in der Jugendbildung und -begleitung tätige Erwachsene die Aufgabe, die ihnen anvertrauten Kinder vor Gefahren aus der digitalen Welt zu schützen und zugleich für eine hinreichende digitale Teilhabe und Befähigung dieser Kinder Sorge zu tragen. Insbesondere für die Vermittlung der Fähigkeit, mit den vielfältigen Chancen und Risiken digitaler Technologien kompetent und zunehmend selbstverantwortlich umzugehen, sind die in Bildungseinrichtungen tätigen Personen in hohem Maße mitverantwortlich.

Organisationale und staatliche Ebene

Damit sowohl die Eltern als auch die weiteren verantwortlichen Personen ihrer Verantwortung gerecht werden können, bedarf es bestimmter Rahmenbedingungen, die im Zusammenwirken von Akteuren auf organisationaler und staatlicher Ebene gewährleistet werden müssen. Die wichtigste dieser Rahmenbedingungen besteht darin, Soziale Medien und andere digitale Technologien so zu gestalten, dass Kinder und Jugendliche durch ihre Nutzung so wenig wie möglich gefährdet werden. Dazu müssen in jedem Fall die Anforderungen, die Art. 28 DSA an für Minderjährige zugängliche Onlineplattformen stellt, erfüllt werden. Darüber hinaus sollten aber auch die digitalen Angebote für alle Menschen so gestaltet werden, dass sie systemische Risiken minimieren, so wie dies bereits in Art. 34 und 35 DSA und im zu erwartenden Digital Fairness Act angelegt ist. Dadurch könnten digitale Angebote auch von Kindern und Jugendlichen relativ gefahrlos genutzt werden, sodass Eltern den Teilhabe- und Befähigungsinteressen ihrer Kinder ohne Bedenken Rechnung tragen könnten.

Wichtig ist, in diesem Kontext auf eine bestehende Schutzlücke in Bezug auf generative KI hinzuweisen. Der DSA ist lediglich auf Onlineplattformen anwendbar, nicht jedoch auf generative KI-Anwendungen, weil jene nicht nutzergenerierte Inhalte öffentlich zugänglich machen, wie es der DSA für den Begriff der Onlineplattform definiert. Zwar fällt generative KI unter

die KI-Verordnung, welche aber keine ausdrücklichen Vorgaben zur Berücksichtigung von Jugendschutzbelangen macht.[62] Da auch der JMStV noch nicht umfassend auf Anwendungen generativer KI vorbereitet ist, bedarf es einer Modernisierung des jugendschutzrechtlichen Ordnungsrahmens, um Herausforderungen durch generative KI angemessen begegnen zu können.[63]

Die Verantwortung für eine entsprechende Gestaltung der Plattformen tragen auf organisationaler Ebene zunächst einmal die Plattformbetreiber selbst, die unabhängig von der rechtlichen Regulierung schon ethisch dazu verpflichtet sind, ihre Geschäftsinteressen nicht auf Kosten des Schutzes insbesondere Minderjähriger, aber auch anderer Nutzerinnen und Nutzer zu verfolgen. Die staatliche Ebene hat die Verantwortung, diese ethische Verpflichtung durch eine rechtliche Regulierung zu konkretisieren, sowie dafür zu Sorge tragen, dass die dadurch entstehenden rechtlichen Verpflichtungen auch tatsächlich erfüllt werden. Da die notwendige Regulierung auf europäischer Ebene mit dem DSA, aber auch durch die KI-Verordnung, die Datenschutz-Grundverordnung, die Richtlinie über audiovisuelle Mediendienste sowie den Digital Fairness Act erfolgt ist bzw. erfolgen wird, steht die Europäische Kommission gemeinsam mit den Mitgliedstaaten in der Verantwortung, für die Einhaltung der sich daraus ergebenden rechtlichen Verpflichtungen zu sorgen.

Die Akteure auf organisationaler und staatlicher Ebene haben außerdem so weit wie möglich dafür Sorge zu tragen, dass alle Eltern ihrer Verantwortung, den Zugang ihrer Kinder zu digitalen Angeboten nach Maßgabe ihrer eigenen Erziehungsvorstellungen zu regeln, auch tatsächlich gerecht werden können. Zentrale Voraussetzung für die Wahrnehmung dieser Verantwortung ist, dass den Eltern die ihren Kindern durch digitale Angebote drohenden Gefahren hinreichend bewusst sind. Obwohl diese Gefahren inzwischen auch in der breiten Öffentlichkeit diskutiert werden, ist nicht davon auszugehen, dass dieses Bewusstsein bereits allgemein in hinreichendem Maße vorhanden ist. Deshalb ist es unerlässlich, dass sowohl die Plattformanbieter als auch die zuständigen Behörden umfassend über diese Gefahren aufklären. In die notwendige Aufklärung könnten auch die Kinderarztpraxen einbezogen werden, die zum Beispiel bei Vorsorgeuntersuchungen den Konsum digitaler Medien thematisieren und die Eltern auf die damit einhergehenden Gefahren und die Notwendigkeit einer sachgerechten Begrenzung hinweisen könnten.

Um den Zugang ihres Kindes zu digitalen Angeboten nach Maßgabe ihrer eigenen Erziehungsvorstellungen verantwortlich zu regeln, benötigen die Eltern außerdem herstellerunabhängige Informationen, für welche Altersgruppe ein bestimmtes digitales Angebot geeignet ist. Darüber hinaus sind leicht handhabbare technische Möglichkeiten wichtig, mit denen der Zugriff auf einzelne Angebote bzw. einzelne Funktionen von Angeboten entweder erlaubt oder gesperrt und die digitalen Aktivitäten ihrer Kinder sowohl hinsichtlich einzelner Angebote als auch insgesamt zeitlich limitiert werden können. Wenn die Endgeräte so konfiguriert wären, dass durch die bloße Alterseingabe zunächst alle für das eingegebene Alter nicht empfohlenen digitalen Angebote gesperrt sind, diese aber – sofern es sich nicht um zwingende Vorgaben handelt – einzeln und möglichst granular wieder freigegeben werden können, wäre es mit überschaubarem Aufwand möglich, eine der individuellen Entwicklung des eigenen Kindes gerecht werdende Einstellung vorzunehmen.

Damit nicht nur die Kinder von technisch besonders versierten Eltern auf diese Weise geschützt werden, muss allerdings auch über diese technischen Möglichkeiten umfassend aufgeklärt wer-

[62] Vgl. Dreyer (2025).
[63] Vgl. Ukrow (2024).

den. Die Aufklärung ist so zu gestalten, dass sie möglichst alle Eltern dazu befähigt, die vorhandenen technischen Möglichkeiten zum Schutz ihrer Kinder verantwortungsvoll anzuwenden. Soweit dies im Einzelfall nicht gelingt, hat die staatliche Ebene dafür Sorge zu tragen, dass die betreffenden Eltern die notwendige technische Unterstützung, zum Beispiel durch Digitalpatinnen und -paten, erhalten.

Gleichwohl können Fälle verbleiben, in denen Kinder durch die elterliche Kontrolle nicht hinreichend geschützt werden. Dementsprechend haben die Akteure auf staatlicher Ebene außerdem die Verantwortung, dafür zu sorgen, dass das Kindeswohl durch den Zugang zu digitalen Angeboten nicht gefährdet wird. Wenn ein gravierendes Schutzinteresse von Kindern und Jugendlichen gegenüber ihren Teilhabe- und Befähigungsinteressen eindeutig vorrangig ist, hat der Staat den Zugang zu den betreffenden Angeboten aufgrund seiner verfassungsrechtlichen Schutzpflicht auch ohne Rücksicht auf einen etwaigen gegenteiligen Willen der Eltern zu unterbinden. Die Voraussetzungen dafür sind vor allem bei Inhalten, die Minderjährigen bereits nach dem Strafgesetzbuch oder nach § 4 JMStV nicht zugänglich gemacht werden dürfen, ohne Weiteres erfüllt. Um Kinder und Jugendliche so weit wie möglich vor solchen Inhalten zu schützen, sollte der Zugang zu entsprechenden digitalen Angeboten stets durch besonders zuverlässige Altersbestimmungstechnologien kontrolliert werden, die sicherstellen, dass die Angebote nur Erwachsenen zugänglich sind.[64]

Aber auch darüber hinaus gibt es sicherlich digitale Angebote, die das Kindeswohl zwar weniger massiv und möglicherweise nicht in jeder Altersstufe, aber zumindest bei jüngeren Kindern so erheblich beeinträchtigen, dass eine vom Willen der Eltern unabhängige Beschränkung des Zugangs geboten erscheint. Jedoch kann dies nur für die einzelnen Angebote beurteilt werden. Ein gesetzliches Mindestalter für eine ganze Dienstekategorie oder einen ganzen Angebotstypus träfe auch Angebote, die das Wohl von Kindern und Jugendlichen nicht beeinträchtigen oder dieses sogar befördern bzw. sogar besondere Vorkehrungen zu deren Schutz vorhalten (z. B. spezielle Soziale Medien für Jugendliche). Angemessener erscheint deshalb ein risikobasierter Ansatz, welcher auch den Leitlinien der Europäischen Kommission zu Art. 28 DSA zugrunde liegt. Diese sehen vor, dass die Kommission die Anbieter verpflichtet, selbst ein angemessenes Mindestalter für ihr jeweiliges Angebot zu bestimmen und dieses gegebenenfalls mit einer an das Risikoausmaß angepassten Altersbestimmungstechnologie zu kontrollieren. Allerdings sollte dann sowohl die Angemessenheit dieser Selbsteinstufung als auch deren effektive Umsetzung anbieterunabhängig überprüft werden.

3.3 Effektivität und Nebenwirkungen von Alterskontrolltechnologien

Um Kinder und Jugendliche vor sie besonders gefährdenden Inhalten im Netz wie zum Beispiel Pornografie zu schützen, ist es unerlässlich, Personen, die auf solche Angebote zugreifen möchten, in Alterskohorten zu differenzieren. Dementsprechend müssten die Anbieter von Onlineplattformen, die solche Inhalte enthalten, schon jetzt aufgrund ihrer in Art. 28 Abs. 1 DSA geregelten Verpflichtung zum Minderjährigenschutz Technologien zur Alterskontrolle anwenden. Deren Einsatz wäre in noch erheblich größerem Maße notwendig, wenn der Zugang zu Sozialen Medien und gegebenenfalls weiteren digitalen Angeboten generell von einem bestimmten Mindestalter abhängig gemacht werden würde.

[64] Für die Inhalte nach § 4 Abs. 2 Satz 1 JMStV wird in § 4 Abs. 2 Satz 2 JMStV bereits eine entsprechende Anforderung formuliert.

Aus Art. 28 Abs. 1 DSA selbst ergeben sich keine konkreten rechtlichen Vorgaben, welche Technologien zur Alterskontrolle zu verwenden sind, und auch § 24a Abs. 2 Nr. 3 JuSchG, der technische Mittel zur Altersverifikation ausdrücklich als Vorsorgemaßnahmen im Sinne des Art. 28 Abs. 1 DSA qualifiziert, enthält hierzu keinerlei Regelung. § 4 Abs. 2 Satz 2 JMStV verlangt zwar für die dem § 4 Abs. 2 Satz 1 JMStV unterfallenden Inhalte, dass „von Seiten des Anbieters sichergestellt ist, dass sie nur Erwachsenen zugänglich gemacht werden“. Aber diese Anforderung gilt nach noch nicht rechtskräftigen Urteilen des Verwaltungsgerichts Neustadt an der Weinstraße[65] nicht für die durch den DSA abschließend regulierten Plattformen und kann zudem ungeachtet der Regelung des § 2 Abs. 1 Satz 2 und 3 JMStV aufgrund des in der Europäischen Union geltenden Herkunftslandprinzips[66] dadurch ausgehebelt werden, dass sich der Anbieter in einem anderen Staat registriert.

Damit ist es nach geltender Rechtslage weitgehend den Anbietern von Onlineplattformen überlassen, welche Methode der Altersverifikation sie in welcher Weise anwenden. Dieser Rechtszustand ist ethisch insofern zu hinterfragen, als die verschiedenen Technologien zur Alterskontrolle nicht notwendigerweise gleichwertig sind. Details der technischen Implementierung, insbesondere die Frage, ob die Altersbestimmung auf den Endgeräten, durch die Plattformen selbst oder durch andere Institutionen erfolgt, können für die ethische Beurteilung von großer Bedeutung sein. Die Unterschiede sind nicht nur technischer Natur, sondern haben unmittelbare Auswirkungen auf Grundrechte, insbesondere auf Privatheit, Nichtdiskriminierung und informationelle Selbstbestimmung.

Um Chancen, aber auch Risiken der jeweiligen Ansätze und ihrer Kombinationen bewerten zu können, müssen diese einerseits hinsichtlich ihrer Effektivität und andererseits hinsichtlich ihrer Nebenwirkungen analysiert werden. Die Frage der Effektivität umfasst die Zuverlässigkeit, Genauigkeit, aber auch Umgehbarkeit technischer Lösungen. Sie ist nicht nur maßgeblich dafür, bis zu welchem Grad die jeweiligen Technologien tatsächlich verhindern können, dass Kinder und Jugendliche Zugriff auf Angebote erhalten, die als beeinträchtigend eingeschätzt werden, sondern entscheidet auch darüber, in welchem Ausmaß bei der Anwendung der jeweiligen Technologie Menschen möglicherweise zu Unrecht der Zugang zu digitalen Angeboten verweigert wird. Zu den relevanten Nebenwirkungen der jeweiligen Technologien zählen zudem Herausforderungen in Bezug auf den Schutz der Privatsphäre aller Nutzerinnen und Nutzer, aber auch hinsichtlich möglicher Verzerrungen (Biases) und Diskriminierungen, Missbrauch, Sicherheit oder Zensur sowie der Abhängigkeiten von Plattformen oder Betriebssystemanbietern.[67]

3.3.1 Effektivität von Altersbestimmungstechnologien

Altersbestimmungstechnologien dienen dazu, Personen nach ihrem Alter zu unterscheiden, um sicherzustellen, dass denjenigen, die ein bestimmtes Mindestalter noch nicht erreicht haben, der Zugriff auf für sie als ungeeignet eingeschätzte Inhalte verwehrt wird. Hier ist zunächst wichtig, dass kein System der technischen Alterskontrolle eine Umgehung vollständig verhindern kann. Solange Altersgrenzen nur in einigen Ländern gelten, kann man diese Vorgaben beispielsweise

[65] VG Neustadt, 13.01.2026 – 5 K 475/24.NW, 5 K 476/24.NW, 5 K 1204/24.NW; VG Neustadt, 04.02.2026 – 5 K 1203/24.NW.
[66] Geregelt in Art. 3 Abs. 1 und 2 der Richtlinie 2000/31/EG und umgesetzt in § 3 Abs. 1 des Digitale-Dienste-Gesetzes.
[67] Vgl. Lueks et al. (2026).

sehr leicht durch die Verwendung von VPNs umgehen, mittels derer Nutzerinnen und Nutzer vorgeben, an einem anderen Ort zu sein, an dem diese Regeln nicht gelten.

Zahlen aus Australien belegen in der Tat einen sprunghaften Anstieg der Nutzung von VPNs nach Einführung der verpflichtenden Altersüberprüfung.[68] Solche Umgehungsstrategien sind also insbesondere bei technisch versierten Minderjährigen zu erwarten. Bewertungen zur Effektivität von Altersbestimmungstechnologien müssen diese grundsätzliche Umgehbarkeit berücksichtigen. Einer Forderung nach perfekter Wirksamkeit würde kein System genügen, aber das Ignorieren von Umgehungsmöglichkeiten kann ein falsches Gefühl der Sicherheit erzeugen. Dies vorausgesetzt, zeigen sich beim Blick auf die Effektivität Unterschiede zwischen den verschiedenen Ansätzen, wobei deren jeweilige Effektivität auch von Details der technischen Ausgestaltung abhängt.

Verifikation: Dokumentenbasierte Verifizierungstechnologien bieten die höchste Zuverlässigkeit, da hier das Alter der Nutzerinnen und Nutzer durch vorhandene offizielle Dokumente wie Pässe oder Personalausweise belegt wird. Diese Verifikation kann direkt durch Vorzeigen des Dokuments gegenüber dem Diensteanbieter erfolgen, durch Eingabe der Informationen des Dokuments auf dem Endgerät oder durch sogenannte Identitätsanbieter (Identity Provider) wie zum Beispiel die durch die eIDAS-Verordnung der Europäischen Union regulierte EUDI-Wallet. Unterschiede hinsichtlich der Effektivität bestehen je nachdem, ob die Altersüberprüfung einmalig stattfindet oder jedes Mal, wenn jemand versucht, auf eine altersbeschränkte Ressource zuzugreifen. Eine Umgehung ist bei nur einmaliger Altersprüfung einfacher, beispielsweise wenn Eltern oder andere Erwachsene Kindern und Jugendlichen ihre Geräte mit ihren Dokumenten freischalten.

Obwohl aufgrund des Rückgriffs auf offizielle Dokumente die Genauigkeit von dokumentenbasierten Verifizierungsverfahren am höchsten ist, kann auch durch diese nicht ausgeschlossen werden, dass Kinder und Jugendliche Dokumente erwachsener Personen zur Registrierung bei Diensten verwenden bzw. ihre Eltern oder andere erwachsene Personen ihre Dokumente für die Verifikation zur Verfügung stellen, auch wenn dieses Risiko beispielsweise durch die Eingabe von Pins zu reduzieren ist. Umgekehrt stellt sich bei diesen dokumentenbasierten Verifikationsmechanismen die Problematik eines unberechtigten Ausschlusses vom Zugang zu digitalen Angeboten für Personen, die nicht über die notwendigen Dokumente verfügen oder bei der Anwendung der Technologie an technischen Hürden scheitern.

Elterliche Kontrolle und Zustimmung: Technische Ansätze, die auf elterlicher Kontrolle und Zustimmung beruhen und in der Regel auf Geräte- oder Diensteebene altersgerechte Einschränkungen von Inhalten und Nutzungszeiten sowie elterliche Zustimmungserfordernisse vorsehen, wie zum Beispiel Apples „Bildschirmzeit“, Googles „Family Link“ oder Kinderschutz-Apps von Drittanbietern können eine ähnlich hohe Effektivität wie die oben genannten Verifikationsverfahren erreichen. Dies gilt aber nur, wenn Eltern diese Werkzeuge tatsächlich aktivieren und konfigurieren. Kinder und Jugendliche, deren Eltern dies nicht tun, sind hingegen ungeschützt. Hinzu kommt, dass solche Tools zwar beispielsweise in den Betriebssystemen der gängigen mobilen Endgeräte (z. B. iOS, Android) oder in den Kontoeinstellungen für Minderjährige einiger Plattformen (z. B. Instagram, TikTok, ChatGPT) angelegt sind, sie allerdings in ihren Funktionalitäten durchaus verbessert werden könnten und sollten.[69] So sollte es für Eltern ei-

[68] Vgl. Kaye (2026); Taylor (2026).

[69] Apps von Drittanbietern bieten bereits jetzt erweiterte Funktionalitäten wie zum Beispiel feiner einstellbare Filtermöglichkeiten oder eine KI-basierte Überwachung der Interaktionen und Inhalte, mit denen ein Kind über Soziale Medien und Kommunikationsanwendungen in Kontakt kommt. Je nach konkreter Ausgestaltung können

nerseits deutlich einfacher werden, Altersinformationen zu hinterlegen und kindgerechte Einstellungen vorzunehmen.[70] Andererseits müssten sinnvolle, nutzerzentrierte Lösungen geschaffen werden, um granular bestimmte, spezifische Schutzmechanismen in Abhängigkeit vom tatsächlichen Schutzbedürfnis der Kinder und Jugendlichen abzuschalten, ohne dabei vollständig auf Schutz zu verzichten. Als Beispiel: Wenn man seinen Kindern Zugriff auf bestimmte Musik erlauben möchte, die von der Plattform als nicht jugendgerecht eingestufte Vulgärausdrücke enthält, sollte dies nicht nur dann möglich sein, wenn man vollständig aus der Jugendversion der Dienste aussteigt.

Altersschätzung und Ableitung: Technologien, die das Alter auf der Grundlage von biometrischen Daten oder dem Verhalten im Netz schätzen, sind weniger zuverlässig und weisen ein hohes Risiko auf, nicht altersgerechte Zugriffe auf Dienste oder Inhalte zu ermöglichen oder umgekehrt Personen zu Unrecht vom Zugang auszuschließen. Da sich Kinder und Jugendliche unterschiedlich schnell entwickeln, kann sowohl das äußere Erscheinungsbild als auch das Verhalten im Netz innerhalb einer Alterskohorte so unterschiedlich und zwischen verschiedenen Alterskohorten so ähnlich sein, dass es kaum möglich erscheint, anhand dieser Daten zuverlässig zwischen beispielsweise 13- und 14-Jährigen oder 15- und 16-Jährigen zu unterscheiden. Zwar könnten insbesondere das Zusammenführen und Auswerten einer größeren Menge und Vielfalt von Daten in Zukunft diese Genauigkeit erhöhen – allerdings geschähe dies um den Preis einer hochgradig invasiven Überwachung von Nutzerinnen und Nutzern, insbesondere wenn dies seitens der Anbieter geschieht. Dies führt direkt zu den Nebenwirkungen der Altersbestimmungstechnologien sowie zu den damit verbundenen Risiken.

3.3.2 Unerwünschte Nebenwirkungen von Altersbestimmungstechnologien

Schutz der Privatsphäre: Zu den zentralen Nebenwirkungen vieler Altersbestimmungstechnologien zählen die damit verbundenen Gefahren für den Schutz der Privatsphäre. Viele Ansätze erfordern die Preisgabe sensibler Daten und/oder das Auslesen von Nutzungsdaten und Inhalten durch die Anbieter. Von besonderer Sensibilität sind hier biometrische Daten, die von den Gesichtszügen und der Stimmlage bis zur Knochenstruktur[71] reichen können. Aber auch die Analyse von Verhaltens- und Nutzungsdaten ist hochgradig invasiv und ermöglicht – neben der Berechnung des wahrscheinlichen Alters – sehr granulare und sensible Einblicke in das Leben der ausgewerteten Nutzerinnen und Nutzer. Insbesondere eine Bestimmung des Alters anhand des Verhaltens im Netz begründet das Risiko, dass die Anbieter digitaler Dienste die Notwendigkeit einer sicheren Unterscheidung verschiedener Alterskohorten zum Anlass nehmen, in Zukunft ein noch invasiveres Tracking aller Nutzerinnen und Nutzer mit massiven Auswirkungen auf deren Privatsphäre zu betreiben.

Altersbestimmungstechnologien, bei denen sensible Daten auf den Endgeräten verbleiben und die lediglich das Signal „alt genug“ an die Plattformen und Diensteanbieter senden, sind daher grundsätzlich gegenüber Mechanismen zu bevorzugen, bei denen die Serviceanbieter selbst diese Altersabschätzung anhand erhobener Daten vornehmen. Auf der Ebene der Endgeräte

---

damit jedoch eigene Herausforderungen für die Privatsphäre und Sicherheit verbunden sein. Vgl. Maier et al. (2025).

[70] Für einen Überblick zum Umfang und zur Komplexität von aktuell empfohlenen elterlichen Einstellungen für einen umfassenden technischen Jugendmedienschutz siehe Jugendmedienschutz-Portal „Medien kindersicher“: https://www.medien-kindersicher.de [21.05.2026].

[71] Vgl. Meineck (2026).

sind hierfür entweder biometrische Schätzverfahren, analog zum „Entsperren“ des Handys mit der Kamera, oder dokumentenbasierte Verifikationsverfahren möglich.

Für den Zugang zu bestimmten Inhalten, vor allem solchen, die Minderjährigen bereits nach dem Strafgesetzbuch oder nach § 4 JMStV nicht zugänglich gemacht werden dürfen, können jedoch Verifikationsmechanismen erforderlich sein, bei denen die Anbieter prüfen, dass der Altersnachweis auch wirklich von der Person stammt, die das Angebot nutzen will. Dafür reichen weder elterliche Zustimmung noch rein endgerätbasierte Verfahren aus.

Hier kommen Lösungen wie die EUDI-Wallet ins Spiel. Sie basiert auf dem EUDI-Framework[72], einem EU-Rahmenwerk für digitale Identitäten, das gemäß der überarbeiteten eIDAS-Verordnung (eIDAS 2.0) alle EU-Mitgliedstaaten verpflichtet, eine digitale Brieftasche (Wallet) einzuführen. Diese digitale Wallet ermöglicht die Ausstellung und Überprüfung von Identitätsnachweisen in ganz Europa und könnte zur Altersverifikation herangezogen werden. Mittels dieser Technologien speichert das Endgerät einen kryptografischen Nachweis über eine erfolgte Altersüberprüfung und kann daher keine von dem Ergebnis dieser Überprüfung abweichenden Informationen mehr übermitteln. Darüber hinaus kann – zum Beispiel über die Eingabe eines Pins – sichergestellt werden, dass die Person, welche das Endgerät verwendet, auch tatsächlich die Person ist, für welche der Altersnachweis erstellt wurde.

Um eine derart starke Form der Verifikation ohne eine solche Wallet-Lösung zu gewährleisten, wäre es beispielsweise nötig, den Pass und zeitgleich das eigene Gesicht in die Kamera zu halten, um sich zu verifizieren. Ein solches Vorgehen birgt jedoch erhebliche Risiken für die Sicherheit und Privatsphäre der Nutzerinnen und Nutzer, da deutlich mehr Daten als nötig und auch sensible biometrische Daten übermittelt werden würden.[73] Die EUDI-Wallet hingegen bietet hier eine datensparsame und sicherere Alternative und wäre für diese sehr starke Form der Verifikation eindeutig vorzuziehen.

Die EUDI-Wallet muss nach den eIDAS-2.0-Vorgaben insbesondere drei Voraussetzungen erfüllen, um die Privatsphäre von Nutzerinnen und Nutzern tatsächlich zu schützen:

1. *Selektive Offenlegung:* Für die Altersüberprüfung bedeutet dies, dass, wenn ein Ausweis auch einen Namen oder ein Geburtsdatum enthält, dem Diensteanbieter lediglich angezeigt werden darf, dass die Nutzerin oder der Nutzer alt genug ist, ohne dass weitere Informationen, zum Beispiel über den Namen oder das Geburtsdatum, preisgegeben werden. Die selektive Offenlegung trägt dazu bei, die Profilerstellung und Nachverfolgung von Nutzerinnen und Nutzern zu verhindern, da sie alle benutzerspezifischen Informationen verbirgt und nur den kryptografischen Nachweis für die Information „alt genug“ sendet.[74]
2. *Unverknüpfbarkeit durch den Aussteller des Altersnachweises:* Es darf dem Aussteller des Alterssignales nicht möglich sein, zu erkennen, wo ein Altersnachweis verwendet wird. Dies verhindert, dass Identitätsanbieter (und Altersüberprüfungsdienste) Aufzeichnungen über das Onlineverhalten von Nutzerinnen und Nutzern erstellen und diese somit tracken können.[75]

---

[72] https://digital-strategy.ec.europa.eu/en/policies/eudi-regulation [05.05.2026].
[73] Beispielsweise kam es im September 2025 zu einem Datenleck von Fotos aus amtlichen Ausweisdokumenten von Nutzerinnen und Nutzern der Plattform Discord, die diese für Altersverifizierungen an einen von Discord beauftragten Dienstleister übermittelt hatten. Siehe hierzu https://discord.com/press-releases/update-on-security-incident-involving-third-party-customer-service [21.05.2026].
[74] Art. 5a Abs. 4 lit. a und Art. 5a Abs. 5 lit. a (iii) eIDAS-Verordnung (eIDAS 2.0).
[75] Art. 5a Abs. 16 lit. a eIDAS-Verordnung (eIDAS 2.0).

3. *Unverknüpfbarkeit der Verifizierer:* Verifizierer oder Diensteanbieter dürfen ebenfalls nicht in der Lage sein, Nutzerinnen und Nutzer anhand der erhaltenen kryptografischen Nachweise zu erkennen, um Tracking und Profilbildung zu verhindern. Darüber hinaus darf auch keine Verknüpfbarkeit zwischen verschiedenen Verifizierern und Diensteanbietern möglich sein.[76]

Am Markt befindliche technische Lösungen erfüllen diese drei Anforderungen nicht vollständig. Die EUDI-Wallet soll diese Garantien erfüllen, derzeit ist die Unverknüpfbarkeit jedoch nicht vollständig gewährleistet.[77] Eine im April 2026 vorgestellte EU-App zur Altersverifikation[78], welche auch unter der Bezeichnung „Mini-Wallet" bekannt ist und in verschiedenen europäischen Ländern pilotiert wird[79], hat darüber hinaus noch weitere Schwächen in Bezug auf Sicherheit, Datenschutz und Effektivität.[80] Aufgrund dieser Mängel sowie grundlegender Kritik an den Nebenwirkungen dieser Technologien haben sich noch im März 2026 über 400 Expertinnen und Experten für Cybersecurity, darunter einige, welche selbst an der Entwicklung der EUDI-Wallet beteiligt sind, gegen den Einsatz von Altersbestimmungstechnologien ausgesprochen.[81]

Systematische Verzerrungen (Biases) und Diskriminierung: Technologien zur Altersüberprüfung haben das Ziel, bestimmte Gruppen, nämlich Kinder und Jugendliche, von bestimmten Arten von Inhalten, nämlich solchen, die als ihr Wohl beeinträchtigend eingeschätzt werden, auszuschließen. Insbesondere bei Systemen, welche das Alter anhand von biometrischen oder Verhaltensdaten schätzen, sind systematische Verzerrungen in zwei Richtungen möglich: Einerseits können insbesondere bei Schätzsystemen Kinder und Jugendliche durch das Raster fallen, weil sie aufgrund ihrer biometrischen oder Trackingdaten als älter eingeschätzt werden. Umgekehrt können aber auch Nutzerinnen und Nutzer, die alt genug sind, um bestimmte Dienste zu nutzen, unberechtigterweise ausgeschlossen werden. Bei biometrischen Verfahren kann dies beispielsweise geschehen, wenn sie als jünger eingeschätzt werden, als sie tatsächlich sind.

Darüber hinaus gibt es sowohl für datenbasierte als auch andere Ansätze weitere Quellen für unberechtigte Ausschlüsse. Diese treffen vielfach und aus unterschiedlichen Gründen insbesondere Nutzergruppen, die ohnehin schon marginalisiert sind. Erstens könnten Menschen mit geringen technischen Kenntnissen, darunter auch ältere Menschen, Schwierigkeiten haben, sich an einen weiteren erforderlichen Schritt bei der Nutzung von Technologien zu gewöhnen, die für sie ohnehin schon schwierig sind. Zweitens können Techniken zur Altersüberprüfung spezifische Hardware erfordern, die manche Menschen sich nicht leisten können, zum Beispiel Mobiltelefone mit Kameras, um Selfies zur Altersschätzung aufzunehmen. Drittens werden für Verifikationssysteme bestimmte Arten von Dokumenten vorausgesetzt, über die bestimmte Gruppen gegebenenfalls nicht verfügen, beispielsweise Kinder unter einem bestimmten Alter, aber auch internationale Besucherinnen und Besucher.

---

[76] Art. 5a Abs. 5 lit. b eIDAS-Verordnung (eIDAS 2.0).
[77] https://eudi.dev/2.4.0/discussion-topics/a-privacy-risks-and-mitigations [05.05.2026].
[78] https://commission.europa.eu/news-and-media/news/european-age-verification-app-keep-children-safe-online-2026-04-15_en [21.05.2026].
[79] https://digital-strategy.ec.europa.eu/en/news/commission-makes-available-age-verification-blueprint [05.05.2026]; https://ageverification.dev/av-doc-technical-specification/docs/architecture-and-technical-specifications [05.05.2026].
[80] Vgl. Steinebach et al. (2026); Marzolf et al. (2026).
[81] Vgl. Joint Statement of Security and Privacy Scientists and Researchers on Age Assurance (2026).

Missbrauch und Zensur: Auch das Risiko eines etwaigen Missbrauchs von Altersbestimmungstechnologien ist in den Blick zu nehmen. Die Technologien sind Instrumente zur Unterscheidung und unterschiedlichen Behandlung von Nutzergruppen. Als solche können sie auch zweckentfremdet werden, und zwar sowohl zur Beschränkung des Zugangs für weitere Gruppen als auch des Zugangs zu anderen Inhalten, zum Beispiel zu Materialien zur sexuellen Aufklärung oder gar zu solchen, die politisch unerwünscht sind. Aufgrund dieser breiten Einsatzmöglichkeiten kann nicht ausgeschlossen werden, dass die Altersbestimmungstechnologien als Zensurinstrument missbraucht werden.

Institutionelle und technische Abhängigkeiten: Darüber hinaus können sich problematische institutionelle und technische Abhängigkeiten ergeben. Die verschiedenen Instrumente der Altersbestimmung bedürfen der Mitarbeit von Plattform-, App- und Betriebssystemanbietern. Auch wenn sich diese Abhängigkeiten nicht vollständig vermeiden lassen, sollte dafür Sorge getragen werden, dass gesetzliche Vorgaben zur Altersüberprüfung die Marktdominanz der großen Anbieter (wie Google, Apple, Microsoft) nicht noch weiter erhöhen.[82]

Ende des offenen Internets: Mit der verpflichtenden Nutzung von Altersbestimmungstechnologien ist zudem die Sorge verbunden, dass dies ein weiterer Schritt auf dem Weg zum Ende eines frei zugänglichen, offenen Internets wäre. Dieses stünde zu befürchten, wenn Mechanismen zur Umgehung der Altersbeschränkungen wie zum Beispiel die Nutzung von anonymen Browserfunktionen oder VPNs, mittels derer man vorgeben kann, an einem Ort zu sein, an welchem Altersbeschränkungen nicht gelten, ihrerseits verboten werden würden. Zudem könnten Vorgaben zur Alterskontrolle auch Anbieter von Open-Source-Software vor Herausforderungen stellen, da gerade kleinere Anbieter und Open-Source-Projekte gegebenenfalls nicht die Kapazitäten haben, Alterskontrollen zu garantieren.

Gesamtbetrachtung und Bewertung

In der Gesamtbetrachtung lassen sich die verschiedenen Risiken, welche sich durch technische Zugangsbeschränkungen selbst ergeben, am ehesten minimieren, wenn der altersgerechte Zugang zu digitalen Angeboten für Kinder und Jugendliche zuvorderst durch elterliche Kontroll- und Zustimmungsmechanismen auf den Endgeräten geregelt wird. Dies beinhaltet zwei Komponenten: Zum einen können Eltern bereits bei der Konfiguration der Handys oder Tablets ihrer Kinder deren Alter angeben, sodass nicht kindgerechte Angebote von vornherein gesperrt werden (elterliche Kontrolle). Zum anderen können sie ebenfalls auf den Endgeräten ihrer Kinder beispielsweise mittels Google Family Link bei Android-basierten Geräten oder unter dem Menüpunkt „Bildschirmzeit“ bei Apple-Geräten einstellen, welche Apps und Websites die Kinder nutzen können und für welchen Zeitraum. Möchte ein Kind auf diese Angebote zugreifen, müssen Eltern diesem Zugriff zustimmen, zum Beispiel durch Eingabe eines Codes (elterliche Zustimmung).

Dieser Ansatz wird erstens dem elterlichen Erziehungsprimat gerecht und knüpft zweitens den Zugang nicht an ein starres Mindestalter. Stattdessen ermöglicht er es den Eltern, unter Berücksichtigung der individuellen Entwicklung ihres Kindes zu entscheiden, in welchem Alter und in welchem Ausmaß Zugang zu digitalen Angeboten gewährt werden sollte, und diesen Zugang auch nach und nach, entwicklungsabhängig zu erweitern. So können Eltern den Teilhabe- und Befähigungsinteressen ihrer Kinder dynamisch Rechnung tragen. Da für die Nutzung der oben genannten endgerätbasierten elterlichen Kontroll- und Zustimmungstechnologien keine weitere Datensammlung und -verwertung durch Dritte notwendig ist, stellen sich drittens bei diesem

[82] Vgl. Leisegang (2026).

Ansatz viele der mit dokument- oder schätzungsbasierten Altersbestimmungstechnologien verbundenen Probleme nicht.[83] Insbesondere die oben beschriebenen zusätzlichen Gefahren für die Privatsphäre gibt es hier nicht. Darüber hinaus hat die elterliche Kontrolle viertens im Gegensatz zu Altersverifikations- oder Schätzverfahren keinerlei Auswirkungen auf erwachsene Nutzerinnen und Nutzer digitaler Angebote, da diese nicht verpflichtet sind, sich ihrerseits einer Altersüberprüfung zu unterziehen.

Allerdings hat die Beschränkung des Zugangs durch elterliche Kontrolle auch Nachteile. Kinder und Jugendliche werden durch diesen Ansatz nur geschützt, wenn und soweit ihre Eltern den Zugang zu digitalen Angeboten tatsächlich kontrollieren. Eine solche Kontrolle wird nur erfolgen, wenn den Eltern die Gefahren eines unbeschränkten Zugangs ihrer Kinder zu digitalen Angeboten bewusst sind und sie über die notwendigen materiellen und immateriellen Ressourcen verfügen, um den Zugang zu diesen Angeboten effektiv zu kontrollieren. Beides ist nicht selbstverständlich, und selbst bei vorhandenen Ressourcen gibt es sicherlich Eltern, die – um Zeit und vor allem Nerven zu sparen – den Weg des geringsten Widerstands gehen und die digitalen Aktivitäten ihrer Kinder nicht oder nur unzureichend kontrollieren.

Schließlich kann eine Beschränkung des Zugangs zu digitalen Angeboten durch die Eltern auch ein weiteres Problem für Minderjährige darstellen. Offensichtlich wird das, wenn Kinder und Jugendliche, etwa in Fällen sexuellen Missbrauchs, gerade vor ihren Eltern Schutz suchen. Aber auch sonst können Kinder und Jugendliche ein legitimes Interesse daran haben, sich zu bestimmten Themen ohne das Wissen ihrer Eltern zu informieren und zu engagieren. Das Problem einer fragwürdigen Verweigerung des Zugangs durch die Eltern bliebe allerdings auch bei der Einführung eines gesetzlichen Mindestalters bestehen, weil auch dessen Erreichung die Eltern nicht dazu verpflichten würde, ihren Kindern den Zugang zu digitalen Angeboten zu ermöglichen.

Je nach Risiko können über die elterlichen Kontrollmöglichkeiten hinaus weitere Maßnahmen in Erwägung gezogen werden. Aufgrund der zuvor skizzierten Risiken sollten hier Verfahren auf der Ebene der Endgeräte bevorzugt werden, da sie weniger negative Auswirkungen auf die Privatsphäre der Nutzerinnen und Nutzer haben – auch wenn dies unter Umständen zu Lasten der Effektivität und Sicherheit geht. Hier könnten sowohl biometrische Verfahren, bei denen Daten auf den Endgeräten verbleiben, als auch endgerätbasierte Verifikationsmechanismen als zweite Hürde für den Zugang zu Inhalten, welche das Wohl von Kindern und Jugendlichen beeinträchtigen, eingesetzt werden. Soweit auf diese Weise abgesicherte Altersbeschränkungen in den Gestaltungsspielraum der Eltern eingreifen, weil sie keine eindeutige Gefährdung des Kindeswohls abwenden, sollten jene die Möglichkeit haben, diese Altersbeschränkungen zu überschreiben oder individuelle Konfigurationen vorzunehmen.

Sofern noch schärfere Verifikationsmechanismen erforderlich werden, bei denen Anbieter prüfen müssen, dass ein Altersnachweis auch wirklich von der Person stammt, die das Angebot nutzen will, wäre die EUDI-Wallet das Mittel der Wahl. Ihre Umsetzung müsste allerding den Vorgaben der eIDAS-2.0-Verordnung vollständig entsprechen und zudem ausreichend skalierbar sein. Alternativen wie zum Beispiel das Vorzeigen von Pass und Gesicht vor der Handykamera sind aus Gründen der Sicherheit und des Schutzes der Privatsphäre abzulehnen.

[83] Sofern Werkzeuge von Drittanbietern verwendet werden, können sich allerdings auch hier Probleme für die Privatsphäre ergeben. Vgl. Maier et al. (2025).

4 Schlussfolgerungen und Empfehlungen

4.1 Schlussfolgerungen aus der ethischen Analyse

Kinder und Jugendliche sind in digitalen Kontexten zahlreichen Risiken ausgesetzt – durch schädliche Inhalte, durch Handlungen, die sie selbst oder andere gefährden, durch schädliche Kontakte im digitalen Raum, durch Verbraucherrisiken und durch Querschnittsrisiken, welche sich etwa aus der Nutzung von KI-Chatbots oder durch die übermäßige Nutzung von Onlineplattformen ergeben.[84] Daher ist ein effektiver Schutz von Kindern und Jugendlichen in digitalen Welten unerlässlich. Zugleich spielen digitale Technologien eine wichtige Rolle bei der Erfüllung grundlegender Informations-, Kommunikations- und weiterer sozialer Bedürfnisse von Kindern und Jugendlichen. Außerdem ist es für ihr weiteres Leben von großer Bedeutung, dass sie die Fähigkeiten erwerben, mit den vielfältigen Chancen und Risiken dieser Technologien kompetent umzugehen.

Damit ergibt sich ein Dreieck aus Schutz-, Teilhabe- und Befähigungsinteressen, die alle zu berücksichtigen sind, um das Wohl von Kindern und Jugendlichen in bestmöglichem Maße zu gewährleisten und zu fördern. Maßnahmen sollten vorrangig darauf abzielen, Risiken in digitalen Umgebungen kontrollierbar zu machen, ohne Teilhabe und Befähigung unnötig einzuschränken. Restriktivere Maßnahmen sind nur dann gerechtfertigt, wenn ein hinreichendes Schutzniveau anders nicht erreichbar ist oder besonders gravierende Gefährdungen vorliegen.

In der öffentlichen und politischen Diskussion liegt der Schwerpunkt der Diskussion auf dem Schutz vor Risiken, welche Soziale Medien für Kinder und Jugendliche bergen. Jedoch beinhalten andere digitale Dienste und Anwendungen wie zum Beispiel Messengerdienste, unmoderierte Spieleplattformen oder vor allem auch Anwendungen der generativen KI, insbesondere Chatbots und Bild- und Videogeneratoren, vergleichbare Risiken wie Soziale Medien. Daher greift ein alleiniger Fokus der politischen und gesellschaftlichen Diskurse auf Soziale Medien deutlich zu kurz. Würde allein der Zugang zu Sozialen Medien für Kinder und Jugendliche beschränkt, so könnten diese ihre kommunikativen und emotionalen Bedürfnisse beispielsweise in Richtung Chatbots verlagern, mit möglicherweise noch problematischeren Konsequenzen für ihre psychische, soziale und gesundheitliche Entwicklung. In Bezug auf Anwendungen der generativen KI besteht jedoch eine erhebliche Schutzlücke, da diese nicht notwendigerweise unter den Digital Services Act fallen und auch der Jugendmedienschutz-Staatsvertrag bislang nur unzureichende Vorgaben zu KI beinhaltet. Die KI-Verordnung selbst enthält wiederum keine ausdrücklichen und einfach handhabbaren Regelungen für den Kinder- und Jugendschutz.

Will man die vielfältigen Risiken für Kinder und Jugendliche in digitalen Umgebungen wirksam adressieren, so dürfen mögliche Maßnahmen sich also nicht nur auf Soziale Medien beschränken. Vielmehr müssen die unterschiedlichen digitalen Technologien gemeinsam sowie in ihren Überschneidungen und Wechselwirkungen betrachtet werden. Hierzu bedarf es eines differenzierten Verständnisses der sozio-technischen Grundlagen einer zunehmend komplexen und dynamischen, digital vernetzten Welt. Maßnahmen zum Kinder- und Jugendschutz in der digitalen Welt müssen dieser Komplexität und Dynamik Rechnung tragen, um angemessen und wirksam zu sein, aber auch um unerwünschte Nebeneffekte und negative Wechselwirkungen zu vermeiden.

---

[84] Vgl. die fünf Risikokategorien der Jugendschutzleitlinien zum Gesetz über digitale Dienste der Europäischen Kommission: http://data.europa.eu/eli/C/2025/5519/oj [05.05.2026].

Neben der Komplexität und Dynamik der digitalen Welt hat eine Regulierung des Zugangs von Kindern und Jugendlichen zu digitalen Angeboten auch der Vielfalt der beteiligten Akteure mit jeweils sehr unterschiedlichen Interessen und Möglichkeiten Rechnung zu tragen. Einerseits müssen die Rechte aller Beteiligten gewährleistet werden, andererseits müssen Pflichten und Verantwortlichkeiten klar benannt und voneinander abgegrenzt werden, um eine Verantwortungsdiffusion zu vermeiden. Der Deutsche Ethikrat schlägt für die Zuschreibung von Pflichten und Verantwortlichkeiten in komplexen Sachlagen das Konzept der Multiakteursverantwortung vor. Unsere Empfehlungen orientieren sich an diesem Konzept und adressieren damit jeweils spezifische Akteure.

Primärer Adressat, um Kinder- und Jugendschutz in der digitalen Welt zu verbessern, sind die Anbieter von Plattformen und anderen digitalen Technologien, da es vielfach ihre Produkte und die zugrunde liegenden Geschäftsmodelle sind, welche nicht nur Kindern und Jugendlichen, sondern auch anderen Nutzergruppen schaden können. Digitale Umgebungen sollten also für alle Menschen besser und sicherer gestaltet werden. Dies umfasst zuvorderst die effektive Umsetzung des Digital Services Act. Damit bedürfte es zugleich weniger Barrieren, um Kinder und Jugendliche von digitalen Angeboten fernzuhalten.

Gleichwohl wird ein gewisses Maß an Kontrolle des Zugangs zu digitalen Angeboten für Kinder und Jugendliche weiterhin notwendig sein. Hierzu bedarf es effektiver, aber zugleich nebenwirkungsarmer technischer Lösungen.

Der Deutsche Ethikrat schlägt ein dreistufiges, risikobasiertes Modell für den technischen Kinder- und Jugendschutz vor[85], um die sozio-technischen Rahmenbedingungen für digitale Technologien durch ein Zusammenspiel verschiedenster Maßnahmen so zu gestalten, dass Schutz, Teilhabe und Befähigung bestmöglich gewährleistet werden (vgl. Empfehlung 7.b-d).

Stufe 1: Die erste Stufe des Schutzes sollte durch die Eltern erfolgen, die aufgrund ihres Erziehungsprimats in erster Linie dazu berufen sind, ihre Kinder vor den Risiken digitaler Welten zu schützen, sie zu befähigen, sich in digitalen Welten sicher zu bewegen, und auf ihre Teilhabe an digitalen Welten zu achten. Technisch würde diese Kontrolle durch die Eingabe des Alters der Kinder bei der Konfiguration der Endgeräte sowie durch die Regulierung von Nutzungszeiten oder des Zugangs auf Apps auf den Endgeräten erfolgen.

Stufe 2: Um auch das Wohl der Kinder zu schützen, deren Eltern diese Werkzeuge nicht oder nur unzureichend nutzen, und um die Verantwortung für den Schutz von Kindern und Jugendlichen nicht allein den Eltern aufzubürden, können zusätzliche Alterskontrollen auf der Ebene der Endgeräte eine zweite Schutzstufe bilden. Eine Variante sind hier biometrische Verfahren der Altersschätzung, welche aufgrund ihrer eingeschränkten Effektivität allerdings nur als ergänzendes Mittel empfehlenswert und aufgrund der Sensibilität der Daten nur zulässig sind, wenn diese Daten auf dem Endgerät verbleiben. Verfahren, bei denen Plattformen das Alter von Nutzerinnen und Nutzern auf Basis biometrischer Daten oder Verhaltensdaten schätzen, sollten hingegen nicht erlaubt sein, da diese Verfahren einerseits nicht hinreichend genau bzw. sicher und andererseits hochgradig invasiv sind. Eine zweite Variante sind endgerätbasierte Verifikationsverfahren, bei denen die Endgeräte das Alter der Nutzerinnen und Nutzer mittels offizieller Dokumente verifizieren.

Stufe 3: Für den Zugang zu bestimmten Inhalten, vor allem solchen, die Minderjährigen bereits nach dem Strafgesetzbuch oder nach § 4 JMStV nicht zugänglich gemacht werden dürfen, sind

[85] Dieses Modell basiert auf der Analyse von Lueks et al. (2026).

jedoch Verifikationsmechanismen erforderlich, bei denen die Anbieter verifizieren, dass der Altersnachweis auch wirklich von der Person stammt, die das Angebot nutzen will. Um sicherzustellen, dass *ausschließlich* das Signal „alt genug" gesendet wird, andere Daten aber geschützt sind, ist in diesen Fällen die EUDI-Wallet zu bevorzugen, da sie, sofern sie den Vorgaben der eIDAS-Verordnung hinsichtlich selektiver Datenweitergabe und Unverknüpfbarkeit entspricht, über starke Garantien für den Schutz der Privatsphäre verfügen würde. Hierfür ist neben der Umsetzung dieser Vorgaben aber auch nötig, dass die verwendeten Techniken ausreichend skalierbar für den breiten Einsatz sind.

4.2 Empfehlungen

1. Um Kinder und Jugendliche besser zu schützen, sollte ein risikobasiertes Schutzkonzept mit altersgerechten Beschränkungen spezifischer Inhalte und Funktionen effektiver umgesetzt werden.

Der Deutsche Ethikrat empfiehlt, den bereits im Digital Services Act und im deutschen Jugendschutzrecht etablierten risikobasierten Ansatz zur altersgerechten Beschränkung von Inhalten und Funktionen, welche das Wohl von Kindern und Jugendlichen beeinträchtigen, effektiver umzusetzen und die verfügbaren Ermittlungs- und Sanktionsmaßnahmen konsequent auszuschöpfen. Maßnahmen zum Schutz von Kindern und Jugendlichen sollten vorrangig darauf abzielen, Risiken in digitalen Umgebungen zu verringern und kontrollierbar zu halten, statt die Nutzung umfassend zu unterbinden. Risikobasierte Ansätze ermöglichen in der Regel ein höheres Maß an Teilhabe und fördern die Entwicklung von Medienkompetenz. Sie stehen damit in einem geringeren Spannungsverhältnis zu Teilhabe und Befähigung als weiteren zentralen Dimensionen des Kindeswohls.

Ein risikobasiertes Schutzkonzept ermöglicht in Kontexten mit gravierenden Gefährdungen durchaus weitreichende Zugangsbeschränkungen. Es ist allerdings notwendigerweise komplex und deshalb mit der Gefahr verbunden, dass Akteure überfordert und ungewollt Schlupflöcher gerade für Plattformen eröffnet werden. Um dem zu begegnen, müssen seine Regelungen so detailliert und granular wie nötig, aber auch so einfach und klar wie möglich sein. Zur Umsetzung des Konzepts könnte unter anderem auf bereits etablierte Regelungen, Praktiken und Institutionen wie zum Beispiel die Bundeszentrale für Kinder- und Jugendmedienschutz, die Kommission für Jugendmedienschutz und die Organisationen der Freiwilligen Selbstkontrolle zurückgegriffen werden.

Primäre Adressaten: Plattformen, Diensteanbieter, Politik (Bund, Europäische Kommission)

2. Konkrete Maßnahmen zur Verbesserung digitaler Umgebungen müssen Anbieter in die Pflicht nehmen und sollten auf europäischer Ebene umgesetzt werden.

Primäre Verantwortungsträger für die Gestaltung von Plattformen und anderen digitalen Diensten sind die Anbieter, welche Sorge dafür zu tragen haben, dass ihre Angebote Kinder und Jugendliche nicht schädigen. Aufgrund der vollharmonisierenden Wirkung des Digital Services Act können Regulierungen, die Plattformanbieter adressieren, nur auf europäischer Ebene ansetzen. Aus diesem Grund und um die bei einer Fragmentierung der Regelungen absehbare Beeinträchtigung der Rechtsdurchsetzung zu verhindern, empfiehlt der Deutsche Ethikrat, Anstrengungen zur Umsetzung weiterer Maßnahmen von vorneherein auf die europäische Ebene zu konzentrieren. Hier sollten wesentliche Punkte der „Leitlinien für Maßnahmen zur Gewährleistung eines hohen Maßes an Privatsphäre, Sicherheit und Schutz von Minderjährigen im Internet gemäß Artikel 28 Absatz 4 der Verordnung (EU) 2022/2065" in den Digital Services Act

integriert und damit rechtsverbindlich gemacht werden. Dies könnte auch verbindliche Vorgaben zu Altersgrenzen und Methoden ihrer Überprüfung umfassen.

Primäre Adressaten: Plattformen, Diensteanbieter, Politik (Bundesregierung, Europäische Kommission)

2.a Zu exzessiver Nutzung anreizende Funktionen digitaler Angebote sollten generell verboten werden.

Ein zentrales Risiko, das in letzter Zeit insbesondere im Zusammenhang mit Sozialen Medien die größte Aufmerksamkeit erregt hat, besteht darin, dass bestimmte Designmerkmale zu übermäßigem Konsum und suchtähnlichem Verhalten führen sowie psychische und physische Schäden verursachen bzw. verstärken können. Kinder und Jugendliche sind hier besonders vulnerabel, aber auch für andere Nutzerinnen und Nutzer sind diese Mechanismen schädlich. Daher empfiehlt der Deutsche Ethikrat, Art. 34 und 35 DSA konsequent anzuwenden, um Funktionen, die zu exzessiver Nutzung anreizen, generell zu verbieten.

Primäre Adressaten: Politik (Europäische Kommission), Plattformen, Diensteanbieter

2.b Anbieter müssen für Minderjährige zugängliche digitale Räume so gestalten, dass Kinder und Jugendliche effektiver geschützt werden als bisher.

In für Kinder und Jugendliche ungehindert zugänglichen Angeboten sollte entsprechend den Leitlinien der Europäischen Kommission gemäß Art. 28 Abs. 4 DSA auf alle für sie schädlichen Funktionen und Mechanismen konsequent verzichtet werden. Dies umfasst neben dem Verzicht auf süchtig machende Funktionen auch zahlreiche weitere Maßnahmen wie zum Beispiel den Verzicht auf Profiling, Tracking und algorithmisch gesteuerte Feeds oder Empfehlungssysteme; sichere Voreinstellungen, die sowohl Kontaktmöglichkeiten als auch die Möglichkeit der Kommentierung von eigenen erstellten Inhalten, der Markierung und des Teilens auf bestätigte Kontakte beschränken; sowie bessere Möglichkeiten, um problematische Inhalte und Interaktionen zu blockieren und zu melden.

Darüber hinaus sollte die Identifikation von Inhalten, die schädlich für Kinder und Jugendliche sind, verbessert werden. In Anbetracht der Menge an (auch nutzergenerierten) Inhalten, mit welchen Nutzerinnen und Nutzer auf Plattformen in Berührung kommen können, halten wir eine Nutzung von geeigneter KI-Tools zur Klassifizierung von Inhalten und zur Identifizierung schädlicher Inhalte zur Unterstützung menschlicher Moderation für gerechtfertigt. Diese Tools müssen jedoch hinreichend spezifizierten Qualitätsmetriken entsprechen, um Fehlklassifikationen zu minimieren. Neben dem Problem des sogenannten Underblockings (schädliche Inhalte werden nicht identifiziert) gilt es auch, Overblocking (Inhalte werden zu Unrecht als schädlich klassifiziert) zu minimieren. Nutzerinnen und Nutzer sollten die Möglichkeit haben, Filter individuell zu konfigurieren, und dabei auch auf Angebote von Drittanbietern oder lokal installierte KI-Systeme zurückgreifen können. Dies würde Risiken durch Under- und Overblocking zusätzlich reduzieren.

Primäre Adressaten: Politik (Europäische Kommission), Plattformen, Diensteanbieter

3. Die mit generativen KI-Anwendungen verbunden Risiken für das Kindeswohl müssen im Jugendmedienschutz stärker berücksichtigt werden.

Anwendungen der generativen KI verursachen die gleichen und mitunter höhere Risiken für das Kindeswohl als Soziale Medien. Insbesondere Chatbots mit ihren über natürliche Sprache erschließbaren vielseitigen Einsatz- und Gestaltungsmöglichkeiten werden immer häufiger zur

ersten Anlaufstelle für die Fragen, Interessen und Bedürfnisse von Kindern und Jugendlichen in der digitalen Welt. Dadurch gewinnen sie nicht nur an Bedeutung als Quelle einschlägiger digitaler Risiken, sondern bringen zusätzliche Gefahren für das Kindeswohl mit sich.

Insbesondere die Teilhabe und Befähigung junger Menschen kann beeinträchtigt werden, wenn der Einsatz von KI Lern- und Bildungsprozesse, die soziale und emotionale Entwicklung oder zwischenmenschliche Beziehungen behindert oder beschädigt. Auch Bildgeneratoren verursachen Risiken, zum Beispiel hinsichtlich der Erstellung pornografischer Materialien, aber auch für sexuelle Nötigung und Erpressung. Angesichts der rasant zunehmenden Verbreitung sowohl eigenständiger KI-Anwendungen als auch der tiefen Integration von KI in viele digitale Dienste müssen die mit diesen Angeboten verbundenen Risiken für das Kindeswohl bei allen Bemühungen um einen verbesserten Jugendmedienschutz daher dringend stärker beachtet werden. Da der Digital Services Act auf die meisten Angebote generativer KI nicht anwendbar ist, empfiehlt der Deutsche Ethikrat, auf europäischer Ebene auch für die generative KI Jugendschutzanforderungen zu schaffen, die strukturell dem risikobasierten Ansatz nach Art. 28 DSA folgen. Auf nationaler Ebene müsste der Jugendmedienschutz-Staatsvertrag dahingehend erweitert werden, dass er KI-Anwendungen auch reguliert, wenn deren Output ausschließlich auf dem Input der nutzenden Person beruht – was derzeit nicht der Fall ist.

Primäre Adressaten: Politik (Europäische Kommission), Plattformen, Diensteanbieter

4. Der Zugang zu digitalen Angeboten sollte auf einer ersten Stufe durch die Eltern geregelt werden und diese sollten dabei deutlich besser unterstützt werden als bisher.

Das Ausbalancieren der Schutz-, Teilhabe- und Befähigungsinteressen von Kindern und Jugendlichen obliegt in erster Linie ihren Eltern, denen das Grundgesetz die Pflege und Erziehung ihrer Kinder anvertraut. Die Eltern haben dabei einen Gestaltungsspielraum, der erst überschritten ist, wenn das Kindeswohl konkret gefährdet wird. Nur unter dieser Voraussetzung ist der Staat aufgrund seines verfassungsrechtlichen Schutzauftrags zum Eingreifen berechtigt und verpflichtet. Dementsprechend empfiehlt der Deutsche Ethikrat, den Zugang zu digitalen Angeboten, die noch keine unzweifelhafte Gefährdung des Kindeswohls begründen, durch die Eltern regeln zu lassen. Diese sollten über die ihren Kindern durch digitale Angebote drohenden Gefahren unter Einbeziehung der Kinderarztpraxen umfassend aufgeklärt und bei der Wahrnehmung ihrer Verantwortung in mehrfacher Hinsicht besser unterstützt werden.

Erstens bedarf es einer Verbesserung der technischen Möglichkeiten, mit denen Erziehungsberechtigte den Zugang zu Apps, Funktionen und Inhalten sowie die Gesamtnutzungszeit einfach, sicher und passgenau beschränken können. Entsprechende Werkzeuge gibt es bereits für die gängigen mobilen Betriebssysteme, allerdings sind sie zumeist nicht leicht zu handhaben und nur begrenzt leistungsfähig. Um den Eltern mit überschaubarem Aufwand eine der individuellen Entwicklung ihres Kindes gerecht werdende Entscheidung zu ermöglichen, sollten die Endgeräte so konfiguriert werden, dass durch die bloße Alterseingabe zunächst alle für das eingegebene Alter nicht vorgesehenen digitalen Angebote zuverlässig gesperrt sind, diese aber – sofern es sich nicht um zwingende Vorgaben handelt – einzeln und möglichst granular wieder freigegeben werden können.

Zweitens ist so weit wie möglich dafür Sorge zu tragen, dass Eltern von diesen technischen Möglichkeiten auch tatsächlich Gebrauch machen. Dazu bedarf es einer eindringlichen Aufklärung darüber, wie Eltern ihre Kinder durch die Nutzung der betreffenden technischen Möglichkeiten effektiv vor digitalen Gefahren schützen können. Außerdem sind diese Möglichkeiten so zu gestalten und zu erklären, dass sie auch von technisch wenig versierten Eltern ohne Probleme gehandhabt werden können. Soweit Eltern gleichwohl bei der technischen Handhabung

Unterstützung benötigen, muss gewährleistet sein, dass sie diese Unterstützung tatsächlich erhalten. Dies ließe sich beispielsweise durch über die Familienhilfe zu vermittelnde Digitalpatinnen und -paten organisieren.

Drittens sollten sich Eltern bei ihrer Entscheidung, welche digitalen Angebote für ihre Kinder geeignet sind, nicht nur an den Altersvorgaben der Anbieter selbst, sondern auch an denen neutraler Institutionen orientieren können. Um dies zu ermöglichen, kommt insbesondere eine Erweiterung des Systems der Freiwilligen Selbstkontrolle in Betracht. Anerkannte Organisationen der Freiwilligen Selbstkontrolle könnten zwar aufgrund der Schnelllebigkeit des Internets nicht für jedes einzelne Angebot, aber für größere Anbieter und Plattformen auf Antrag durchaus Altersbewertungen abgeben, die für App-Marktplätze zu übernehmen wären.

Primäre Adressaten: Politik, Betriebssystemanbieter, Diensteanbieter

5. Kinder und Jugendliche sollten angemessen an der Ausgestaltung von Schutzkonzepten beteiligt werden.

Um nicht nur *über* ihre Kinder zu entscheiden, sondern auch deren Wünsche und Interessen angemessen zu berücksichtigen, sollten Eltern ihre Kinder bei der Entscheidung über den Zugang zu digitalen Angeboten altersadäquat beteiligen.

Darüber hinaus sollten Kinder und Jugendliche an der Ausgestaltung allgemeiner Regelungen zum digitalen Kinder- und Jugendschutz angemessen beteiligt werden. Daher ist bei der politischen Entscheidungsfindung zum Kinder- und Jugendschutz in der digitalen Welt eine institutionalisierte Beteiligung der betroffenen Altersgruppe zu empfehlen. Eine strukturierte Partizipation – etwa über Jugendvertretungen, Anhörungen oder Beteiligungsformate im Rahmen parlamentarischer Verfahren – trägt dazu bei, die Verhältnismäßigkeit und Praxistauglichkeit regulatorischer Eingriffe besser zu prüfen. Zugleich stärkt sie das Vertrauen in staatliche Institutionen und fördert politische Mündigkeit.

Primäre Adressaten: Eltern/Erziehungsberechtigte, Politik (Bund, Länder)

6. Von pauschalen Nutzungsverboten für soziale Medien und andere digitale Dienste auf Grundlage neuer gesetzlicher Mindestaltersgrenzen sollte abgesehen werden.

Der Deutsche Ethikrat spricht sich aus vier Gründen gegen die Einführung pauschaler Mindestaltersgrenzen für den Zugang zu Sozialen Medien und vergleichbaren Dienste aus. Erstens wird eine pauschale Altersgrenze für digitale Technologien nicht der Tatsache gerecht, dass sich deren Risiken nicht allgemein für Klassen von Angeboten, sondern aufgrund bestimmter Merkmale wie zum Beispiel Endlos-Feeds ergeben, welche in jugendschutzfreundlichen Versionen abgestellt werden könnten. Zweitens unterscheiden sich Kinder in ihrem Reifegrad innerhalb und zwischen Alterskohorten mitunter deutlich. Drittens ignoriert ein ausschließlicher Fokus auf Soziale Medien Risiken, welche von anderen digitalen Diensten ausgehen oder sich durch Umgehungsstrategien von Kindern und Jugendlichen im Falle eines Verbots ergeben können. Und viertens würde ein allgemein geltendes Mindestalter sowohl die Teilhabe als auch die Entwicklung der Medienkompetenz von Kindern und Jugendlichen beeinträchtigen und auf unverhältnismäßige Art und Weise in das Recht der Eltern eingreifen, bei dem Zugang zu digitalen Angeboten die Schutz-, Teilhabe- und Befähigungsbelange ihres Kindes individuell auszubalancieren.

Sofern politisch dennoch ein gesetzliches Mindestalter für den Zugang zu Sozialen Medien befürwortet wird, sollte eine einheitliche Lösung auf europäischer Ebene angestrebt werden.

Nationale Verbote mit möglicherweise unterschiedlichen Altersgrenzen könnten einen regulatorischen europäischen Flickenteppich verursachen, der einer effektiven Rechtsum- und -durchsetzung im Wege stehen würde.

Primäre Adressaten: Politik (Europäische Kommission, Bund, Länder)

7. Alterskontrolltechnologien sollten klarer geregelt werden.

Wenn altersgestaffelte Zugangsbeschränkungen zu Diensten oder Inhalten zum Einsatz kommen, sollte die Entscheidung über die anzuwendenden Verfahren zur Altersbestimmung nicht länger den Anbietern überlassen werden, sondern durch rechtlich verbindliche Vorgaben festgelegt werden. Lösungen müssen erstens hinreichend zuverlässig und umgehungssicher sein, zweitens geringe Nebenwirkungen haben. Können diese beiden Anforderungen nicht gleichzeitig erfüllt werden, laufen Maßnahmen Gefahr, entweder wirkungslos zu sein oder unverhältnismäßig in Grundrechte einzugreifen. Die Wahl der geeigneten Altersbestimmungstechnologie muss zudem im Verhältnis zu den Gefahren stehen, die sich durch die jeweiligen Dienste oder Inhalte für Kinder und Jugendliche ergeben. Daraus ergeben sich folgende Empfehlungen:

7.a Alterskontrolle sollte primär auf Ebene der Endgeräte stattfinden.

Alterskontrollen, die seitens der Anbieter erfolgen, können mit starken Eingriffen in die Privatsphäre der Nutzerinnen und Nutzer verbunden sein. Insbesondere datenbasierte Schätzverfahren sind problematisch, da sie entweder biometrische Daten (Altersschätzung) oder aber invasives Tracking (Altersinferenzen) erfordern, wobei umfassende Daten aus verschiedenen Quellen zusammengeführt werden, um detaillierte Profile zu erstellen. Daher spricht sich der Deutsche Ethikrat gegen den Einsatz von Technologien zur Altersableitung oder Altersschätzung aus, bei denen Daten das Endgerät der Nutzerinnen und Nutzer verlassen. Stattdessen sollten Altersnachweise primär auf der Ebene der Endgeräte hinterlegt werden, um die Privatsphäre von Nutzerinnen und Nutzern zu schützen.

Primäre Adressaten: Politik (Europäische Kommission), Betriebssystemanbieter

7.b Elterliche Kontrollsysteme sollten die Standardmethode zur Alterskontrolle sein.

Um Kinder und Jugendliche vor den verschiedenen Risiken in digitalen Kontexten zu schützen, sollten Zugangsbeschränkungen vorrangig durch Mechanismen der elterlichen Kontrolle und Einwilligung auf den Endgeräten erfolgen (vgl. Empfehlung 4). Dieses Verfahren verbindet hinreichende Effektivität mit vergleichsweise geringen Nebenwirkungen und entspricht zudem dem Primat der elterlichen Erziehungsfreiheit.

Primäre Adressaten: Politik (Europäische Kommission), Eltern/Erziehungsberechtigte, Betriebssystemanbieter

7.c Alterskontrollverfahren auf Geräteebene können ergänzend eingesetzt werden.

Da elterliche Kontrollmechanismen nur Wirkung entfalten, wenn Eltern diese Funktionen verwenden, kann je nach Einsatzgebiet oder Anwendung als zweite Maßnahme zusätzlich auf verpflichtende Alterskontrolltechnologien auf den Endgeräten zurückgegriffen werden. Dies beinhaltet Überprüfungen, ob Nutzerinnen und Nutzer das erforderliche Alter für die Nutzung eines Dienstes haben, etwa anhand von Altersschätzung durch die Kamera oder durch die Verifikation mit offiziellen Dokumenten. Aufgrund der Sensibilität insbesondere biometrischer Daten ist es hier jedoch wichtig, dass diese Daten auf dem Endgerät verbleiben und nur für diese

Altersschätzung verwendet werden. Auch im Falle dokumentenbasierter Verifikation ist es wichtig, dass nur das relevante Alterssignal übermittelt wird.

Primäre Adressaten: Politik (Europäische Kommission), Betriebssystemanbieter

7.d Bei erhöhten rechtlichen Anforderungen an eine Altersverifikation ist die EUDI-Wallet empfehlenswert, sofern Unverknüpfbarkeit und selektive Weitergabe von Daten garantiert sind.

Für den Zugang zu bestimmten Inhalten, vor allem solchen, die Minderjährigen bereits nach dem Strafgesetzbuch oder nach § 4 JMStV nicht zugänglich gemacht werden dürfen, müssen Anbieter nicht nur das Alter der Nutzerinnen und Nutzer mittels offizieller Dokumente verifizieren, sondern auch kontrollieren, dass der Altersnachweis auch tatsächlich zu der Person gehört, die auf ein Angebot zugreifen will. Für diese Fälle empfiehlt der Deutsche Ethikrat die Verwendung der EUDI-Wallet, sofern die Vorgaben der eIDAS-2.0-Verordnung vollständig erfüllt sind und auch die technischen und infrastrukturellen Voraussetzungen für diesen Einsatzzweck gegeben sind. Unter dieser Voraussetzung bietet die EUDI-Wallet starke Garantien für den Schutz der Privatsphäre der Nutzerinnen und Nutzer. Alternativen wie die Mini-Wallet oder gar das Vorzeigen von Pass und Gesicht vor der Handykamera sind aus Gründen der Sicherheit und des Schutzes der Privatsphäre abzulehnen.

Primäre Adressaten: Politik (Europäische Kommission), Forschung & Entwicklung

7.e Für Altersbestimmungstechnologien müssen konkrete technische Anforderungen gesetzlich vorgegeben werden.

Gesetzgeber sollten sich bei der Festlegung von Altersbestimmungstechnologien oder der Definition ihrer Merkmale nicht auf allgemeine Prinzipien wie „Datenschutz durch Technikgestaltung“ beschränken, da diese zu abstrakt sind, um stark voneinander abweichende Implementierungen zu verhindern, von denen manche lediglich formale Konformität mit dem Datenschutz aufweisen, obwohl sie tief in die Privatsphäre von Nutzerinnen und Nutzern eindringen.

Stattdessen sollten Gesetzgeber ähnlich der Anforderungen in der eIDAS-2.0-Verordnung auch für Altersbestimmungstechnologien insgesamt folgende Mindestvorgaben festlegen: Anforderungen an die Unverknüpfbarkeit von Aussteller und Prüfer sowie an die selektive Offenlegung; die Verarbeitung biometrischer Daten und Identitätsdaten auf dem Endgerät oder unter Kontrolle der Nutzerin oder des Nutzers; das Verbot der Datenspeicherung über die Altersbestätigung hinaus und die Konformität mit öffentlich geprüften, offengelegten kryptografischen Protokollen.

Primäre Adressaten: Politik (insbesondere Europäische Kommission)

8. Gatekeeping und Marktdominanz sollte aktiv entgegengewirkt werden.

Große Plattformbetreiber könnten Vorgaben zum Kinder- und Jugendschutz ausnutzen, um ihre Marktmacht bzw. Gatekeeper-Positionen zu festigen und die Datenerfassung auszuweiten. Erstens könnten sich Plattformanbieter wie Google, Apple oder Meta, die bereits über verifizierte Identitätsdaten verfügen, als vertrauenswürdige Anbieter von Altersbestätigungen positionieren und so zu Identitäts- und Compliance-Brokern werden, die die Kontrolle stillschweigend wieder zentralisieren. Zweitens generieren Altersschätzungstechnologien neue Datensignale (Altersgrenzen, Verifizierungszeitpunkt, Geräteinformationen), die Plattformen für Profiling und

Werbung nutzen können. Der Gesetzgeber sollte sicherstellen, dass Vorgaben für Altersbestimmungstechnologien nicht unbeabsichtigt neue Vorteile für Gatekeeper schaffen, die die Ziele des Digital Markets Act untergraben.

Um Vormachtstellungen entgegenzuwirken, Wettbewerb zu befördern und insgesamt Anreize für altersangemessen gestaltete digitale Räume zu schaffen, sollten alternative digitale Plattformen, Dienste und Angebote gefördert werden, die europäischen Werten, Normen und Gesetzen entsprechen. Die Politik kann hier durch Forschungs- und Innovationsförderung Anreize setzen.

Primäre Adressaten: Politik als Regulator und Forschungsförderer, öffentliche Verwaltung als Anwender, Forschung, Industrie

9. Kinder und Jugendliche, aber auch der demokratische Prozess insgesamt müssen vor Formen manipulativer Beeinflussung besser geschützt werden.

Digitale Räume bieten verschiedenen Akteuren Möglichkeiten zur koordinierten Einflussnahme und Manipulation. Das Spektrum reicht dabei von verdeckter Werbung bis hin zu Propaganda und kognitiver Kriegsführung, mit dem Ziel, das Vertrauen in demokratische Prozesse und Institutionen zu untergraben. Diese Gefahren betreffen zwar alle, Heranwachsende sind dafür jedoch besonders vulnerabel. Daher bedarf es zum Schutz von Kindern und Jugendlichen, aber auch des demokratischen Gemeinwesens geeigneter Maßnahmen zu deren Minimierung. Solche Maßnahmen umfassen beispielsweise Anbieterpflichten zur Erkennung und Eindämmung von Botnetzen und anderen manipulativen Kommunikationstaktiken sowie Krisenprotokolle für massive Desinformations- oder Hasskampagnen.

Primäre Adressaten: Politik, Behörden, Diensteanbieter

10. Wissenschaftliche Forschung zu digitalen Technologien, ihren Folgen und Risiken sollte erweitert und gestärkt werden.

Um die Risiken digitaler Technologien besser verstehen und adressieren zu können, sollten Möglichkeiten des Datenzugangs zu Plattformen für wissenschaftliche Forschung verbessert werden. Aufgrund der großen Bedeutung digitaler Technologien für Kinder und Jugendliche sowie der Komplexität und Dynamik der Entwicklungen empfiehlt der Deutsche Ethikrat darüber hinaus neben der grundsätzlichen ethischen, rechtlichen und sozialwissenschaftlichen Begleitforschung dezidierte Programme zur pädagogischen, psychologischen und medizinischen Begleitforschung, um auch zukünftige Entwicklungen in diesem hochdynamischen Feld zu beobachten und empirisch gesichert darauf reagieren zu können.

Primäre Adressaten: Forschung, Industrie, Politik als Regulator und Forschungsförderer, öffentliche Verwaltung als Anwender

11. Die Rahmenbedingungen für den Erwerb digitaler Kompetenz müssen grundlegend verbessert werden.

Um Schutz, Teilhabe und Befähigung von Kindern und Jugendlichen in der digitalen Welt zu gewährlisten, bedarf es effektiver Maßnahmen zur Stärkung der digitalen Kompetenz von Kindern und Jugendlichen, aber auch von Lehrkräften, Fachkräften und insbesondere auch von Erziehungsberechtigten. Medienpädagogische Angebote, auch für diese Zielgruppen, sollten daher stärker gefördert werden. Insbesondere für Schulen kann es allerdings nicht darum gehen, Lehrpläne noch weiter zu befrachten. Vielmehr müssen zum einen Freiräume geschaffen werden, um sich mit digitalen Technologien selbst, aber auch mit den neuen Fragen, die sich daraus

ergeben, auseinanderzusetzen. Zum anderen müssen Schülerinnen und Schüler, Lehrkräfte sowie Eltern und andere beteiligte Personen durch passgenaue und flexible Initiativen in ihren Kompetenzen unterstützt werden. Hierzu gehören auch sichere und geschützte digitale wie analoge Räume, in denen Kinder und Jugendliche lernen, sich begegnen und ausprobieren können.

Primäre Adressaten: Politik (insbesondere Länder)

12. Die private Nutzung digitaler Endgeräte an Schulen sollte weitgehend eingeschränkt werden.

Die allgemeine Schulpflicht versetzt den Staat in eine besondere Verantwortung, Schulen als geschützte Räume des Lernens und der persönlichen Entwicklung sowie der unmittelbaren persönlichen Begegnung auszugestalten. Angesichts der vielfältigen Risiken, die die private Nutzung digitaler Technologien für die Konzentration, die Lernprozesse und das soziale Miteinander von Schülerinnen und Schülern wie auch von Lehrkräften mit sich bringen können, erscheint es sinnvoll, den Schutzraum Schule durch eine weitgehende Einschränkung der privaten Nutzung digitaler Endgeräte zu stärken, wie bereits in einigen Bundesländern umgesetzt. Solche Regelungen könnten beispielsweise Umsetzungsmodelle umfassen, in denen private Geräte während des Aufenthalts in der Schule abgegeben werden. Die Nutzung digitaler Technologien im Unterricht sollte vorzugsweise auf Geräten mit jugendfreundlichen Einstellungen erfolgen. Pausen sollten wieder mehr Freiräume für nicht-digitale soziale Interaktion eröffnen.

Primäre Adressaten: Politik (insbesondere Länder)

13. Analoge (Frei-)Räume und (Frei-)Zeiten sollten gestärkt werden.

Für ihr psychisches und körperliches Wohlbefinden benötigen Kinder und Jugendliche auch jenseits der Schule bildschirmfreie Zeiten, um Raum und Zeit zu schaffen für analoge Aktivitäten wie Sport und Bewegung, Zeit in der Natur, musikalische oder andere kreativen Tätigkeiten sowie soziale Begegnung in physischen Räumen. Daher sollten Freiräume und Freizeiten für diese Aspekte generell gefördert werden – etwa durch bewegungsfreundliche Schulen mit aktiven Pausen und Sportangeboten, attraktive Jugend- und Begegnungsräume, niedrigschwellige Vereins- und Kulturangebote, naturpädagogische Freizeitprogramme. Auch individuelle und familiale Praktiken spielen hier eine zentrale Rolle, zum Beispiel familienfreundliche Routinen wie bildschirmfreie Mahlzeiten, gemeinsame Offlinezeiten oder digitale Ruhezeiten vor dem Schlafengehen.

Primäre Adressaten: Politik (insbesondere Länder und Kommunen), aber auch Schule, Vereine und Eltern

Literatur

Age Check Certification Scheme (Hrsg.) (2025): Age Assurance Technology Trial. Part A: Main Report. Verfügbar unter https://ageassurance.com.au/wp-content/uploads/2025/08/AATT_Part_A_DIGITAL.pdf, zugegriffen am 20.05.2026.

Agyapong-Opoku, Nadine; Agyapong-Opoku, Felix; Greenshaw, Andrew J. (2025): Effects of social media use on youth and adolescent mental health: a scoping review of reviews. In: *Behavioral Sciences*, 15 (5), 574. DOI: https://doi.org/10.3390/bs15050574.

Behre, Julia; Hölig, Sascha; Stöwing, Ezra; Möller, Judith (2025): Reuters Institute Digital News Report 2025. Ergebnisse für Deutschland. Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (Arbeitspapiere des Hans-Bredow-Instituts | Projektergebnisse). DOI: https://doi.org/10.21241/ssoar.102887.

Block, Hans; Riesewieck, Moritz (Reg.) (2018): The Cleaners. Farbfilm Verleih. Verfügbar unter https://www.bpb.de/mediathek/video/273199/the-cleaners, zugegriffen am 20.05.2026.

Brailovskaia, Julia; Buchmann, Johannes; Hertwig, Ralph; Metzinger, Thomas; Montag, Christian; Sadeghi, Ahmad-Reza; Schneider, Silvia; Spiecker gen. Döhmann, Indra; Waldherr, Annie (2025): Soziale Medien und die psychische Gesundheit von Kindern und Jugendlichen. Halle (Saale): Deutsche Akademie der Naturforscher Leopoldina (Diskussion). DOI: https://doi.org/10.26164/leopoldina_03_01307.

Brand, Alexander (2026): Handyverbot an Schulen – ja oder nein? Mehrheit der Jugendlichen ist dagegen. *Deutsches Schulportal*. Verfügbar unter https://deutsches-schulportal.de/schulkultur/handyverbot-an-schulen-ja-oder-nein-was-sagen-die-studien, zugegriffen am 21.05.2026.

Brüggen, Niels; Dreyer, Stephan; Gebel, Christa; Lauber, Achim; Materna, Georg; Müller, Raphaela; Schober, Maximilian; Stecher, Sina (2022): Gefährdungsatlas. Digitales Aufwachsen. Vom Kind aus denken. Zukunftssicher handeln. (2. Aufl.). Bonn: Bundeszentrale für Kinder- und Jugendmedienschutz. Verfügbar unter https://www.bzkj.de/bzkj/service/publikationen/gefaehrdungsatlas-digitales-aufwachsen-vom-kind-aus-denken-zukunftssicher-handeln-aktualisierte-und-erweiterte-2-auflage--197812, zugegriffen am 14.04.2026.

Bundestagsfraktion Bündnis 90/Die Grünen (Hrsg.) (2026): Bessere Plattformen für alle - Junge Menschen schützen und stärken. Verfügbar unter https://www.gruene-bundestag.de/fileadmin/dateien/downloads/Beschluesse/Fraktionsbeschluss_Social_Media_04-2026.pdf, zugegriffen am 20.05.2026.

Burns, Mary; Winthrop, Rebecca; Luther, Natasha; Venetis, Emma; Karim, Rida (2026): A new direction for students in an AI world: Prosper, prepare, protect. The Brookings Institution. Verfügbar unter https://www.brookings.edu/wp-content/uploads/2026/01/A-New-Direction-for-Students-in-an-AI-World-FULL-REPORT.pdf, zugegriffen am 29.05.2026.

CDU Deutschlands (Hrsg.) (2026): Angenommene Sach- und Initiativanträge des 38. Parteitages der CDU Deutschlands. Verfügbar unter https://www.cdu.de/app/uploads/2026/02/2026_02_26_Angenommene-Sach_und-Initiativantraege.pdf, zugegriffen am 05.05.2026.

Common Sense Media (Hrsg.) (2025): Social AI Companions. Common Sense Media. Verfügbar unter https://www.commonsensemedia.org/sites/default/files/pug/csm-ai-risk-assessment-social-ai-companions_final.pdf, zugegriffen am 05.05.2026.

Davis, Christopher G.; Goldfield, Gary S. (2025): Limiting social media use decreases depression, anxiety, and fear of missing out in youth with emotional distress: A randomized controlled trial. In: *Psychology of Popular Media*, 14 (1), 1–11. DOI: https://doi.org/10.1037/ppm0000536.

Deutscher Ethikrat (Hrsg.) (2017): Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung. Deutscher Ethikrat (Stellungnahme). Verfügbar unter https://www.ethikrat.org/fileadmin/Publikationen/Stellungnahmen/deutsch/stellungnahme-big-data-und-gesundheit.pdf, zugegriffen am 21.05.2026.

Deutscher Ethikrat (Hrsg.) (2023): Mensch und Maschine – Herausforderungen durch Künstliche Intelligenz. Deutscher Ethikrat (Stellungnahme). Verfügbar unter https://www.ethikrat.org/fileadmin/Publikationen/Stellungnahmen/deutsch/stellungnahme-mensch-und-maschine.pdf, zugegriffen am 20.05.2026.

Dreyer, Stephan (2025): Die KI-Verordnung, ihr Verhältnis zu Kinderrechten im digitalen Raum und Optionen für Advocacy-Zugänge. Deutsches Kinderhilfswerk (Schriftenreihe). Verfügbar unter https://www.dkhw.de/filestorage/1_Informieren/1.1_Unsere_Themen/Kinder_und_Medien/Kinderrechte_und_KI/DKHW_Schriftenreihe_Kinderrechte_und_KI.pdf, zugegriffen am 20.05.2026.

Eder, Maximilian; Sjøvaag, Helle (2024): Artificial intelligence and the dawn of an algorithmic divide. In: *Frontiers in Communication*, 9 (September), 1453251. DOI: https://doi.org/10.3389/fcomm.2024.1453251.

Eickelmann, Birgit; Fröhlich, Nadine; Bos, Wilfried; Gerick, Julia; Goldhammer, Frank; Schaumburg, Heike; Schwippert, Knut; Senkbeil, Martin; Vahrenhold, Jan (Hrsg.) (2024): ICILS 2023 #Deutschland. Computer- und informationsbezogene Kompetenzen und Kompetenzen im Bereich Computational Thinking von Schüler*innen im internationalen Vergleich. Münster: Waxmann. DOI: https://doi.org/10.31244/9783830999492.

Feierabend, Sabine; Rathgeb, Thomas (Hrsg.) (2005): JIM-Studie 2005: Jugend, Information, (Multi-)Media. Basisstudie zum Medienumgang 12- bis 19-Jähriger in Deutschland. Medienpädagogischer Forschungsverbund Südwest. Verfügbar unter https://mpfs.de/app/uploads/2024/11/JIM_Studie_2005.pdf, zugegriffen am 21.05.2026.

Feierabend, Sabine; Rathgeb, Thomas; Gerigk, Yvonne; Glöckler, Stephan (2025a): JIM-Studie 2025: Jugend, Information, Medien Basisuntersuchung zum Medienumgang 12- bis 19-Jähriger. Medienpädagogischer Forschungsverbund Südwest. Verfügbar unter https://mpfs.de/app/uploads/2025/11/JIM_2025_PDF_barrierearm.pdf.

Feierabend, Sabine; Rathgeb, Thomas; Gerigk, Yvonne; Glöckler, Stephan (2025b): KIM-Studie 2024: Kindheit, Internet, Medien. Basisuntersuchung zum Medienumgang 6- bis 13-Jähriger. Medienpädagogischer Forschungsverbund Südwest. Verfügbar unter https://mpfs.de/app/uploads/2025/05/KIM-Studie-2024.pdf, zugegriffen am 05.05.2026.

Gesellschaft für Innovative Marktforschung (Hrsg.) (2022): Social Media als Infokanal. Gewichtungsstudie zur Relevanz der Medien für die Meinungsbildung in Deutschland, 2022-

I. die medienanstalten. Verfügbar unter https://www.die-medienanstalten.de/fileadmin/user_upload/die_medienanstalten/Forschung/Intermediaere_und_Meinungsbildung/Social_Media_als_Infokanal_2022-I.pdf, zugegriffen am 21.05.2026.

Hunt, Melissa G.; Marx, Rachel; Lipson, Courtney; Young, Jordyn (2018): No more FOMO: limiting social media decreases loneliness and depression. In: *Journal of Social and Clinical Psychology*, 37 (10), 751–68. DOI: https://doi.org/10.1521/jscp.2018.37.10.751.

Institut für Jugendkulturforschung und Kulturvermittlung (Hrsg.) (2024): Schönheitsideale im Internet. Saferinternet.at. Verfügbar unter https://www.saferinternet.at/news-detail/neue-studie-schoenheitsideale-im-internet, zugegriffen am 21.05.2026.

Institut für Jugendkulturforschung und Kulturvermittlung (Hrsg.) (2026): KI-Chatbots als Alltagsbegleiter für Jugendliche. Saferinternet.at. Verfügbar unter https://www.saferinternet.at/news-detail/neue-studie-ki-chatbots-als-alltagsbegleiter-fuer-jugendliche, zugegriffen am 21.05.2026.

Joint Statement of Security and Privacy Scientists and Researchers on Age Assurance (2026):, 2. März 2026. Verfügbar unter https://csa-scientist-open-letter.org/ageverif-Feb2026, zugegriffen am 05.05.2026.

Kang, Cecilia; Mac, Ryan; Tan, Eli (2026): Meta and YouTube found negligent in landmark social media addiction case. In: *The New York Times*, 25. März 2026. Verfügbar unter https://www.nytimes.com/2026/03/25/technology/social-media-trial-verdict.html, zugegriffen am 21.05.2026.

Kang, Cecilia; Tan, Eli (2026): Meta ordered to pay $375 million over child safety violations. In: *The New York Times*, 24. März 2026. Verfügbar unter https://www.nytimes.com/2026/03/24/technology/meta-new-mexico-child-safety-violations.html, zugegriffen am 21.05.2026.

Kaye, Byron (2026): Australians reach for VPNs, find porn sites blocked as online age restrictions take effect. In: *Reuters*, 9. März 2026. Verfügbar unter https://www.reuters.com/world/asia-pacific/vpns-up-porn-websites-down-australia-brings-new-online-age-restrictions-2026-03-09, zugegriffen am 21.05.2026.

Kelly, Dominique (2025): Youth Perspectives on Privacy Dark Patterns. Western University. Verfügbar unter https://hdl.handle.net/20.500.14721/37637, zugegriffen am 05.05.2026.

Kieninger, Julia; Feierabend, Sabine; Rathgeb, Thomas; Gerigk, Yvonne; Glöckler, Stephan; Spang, Emil (2024): miniKIM-Studie 2023: Kleinkinder und Medien. Basisuntersuchung zum Medienumgang 2- bis 5-Jähriger in Deutschland. Medienpädagogischer Forschungsverbund Südwest. Verfügbar unter https://mpfs.de/app/uploads/2025/01/miniKIM-2023_PDF_barrierearm.pdf, zugegriffen am 05.05.2026.

Kops, Maxime; Schittenhelm, Catherine; Wachs, Sebastian (2025): Young people and false information: A scoping review of responses, influential factors, consequences, and prevention programs. In: *Computers in Human Behavior*, 169 (August), 108650. DOI: https://doi.org/10.1016/j.chb.2025.108650.

Kosmyna, Nataliya; Hauptmann, Eugene; Yuan, Ye Tong; Situ, Jessica; Liao, Xian-Hao; Beresnitzky, Ashly Vivian; Braunstein, Iris; Maes, Pattie (2025): Your brain on ChatGPT:

accumulation of cognitive debt when using an AI assistant for essay writing task. arXiv. DOI: https://doi.org/10.48550/arXiv.2506.08872.

Leisegang, Daniel (2026): In der Alterskontroll-App schlägt ein Herz von Google. In: *netzpolitik.org*, 7. Mai 2026. Verfügbar unter https://netzpolitik.org/2026/europaeische-kommission-in-der-alterskontroll-app-schlaegt-ein-herz-von-google, zugegriffen am 21.05.2026.

Livingstone, Sonia; Stoilova, Mariya (2021): The 4Cs: classifying online risk to children. CO:RE short report series: key topics. Hamburg: Leibniz-Institut Für Medienforschung | Hans-Bredow-Institut (CO:RE Children Online: Research and Evidence). DOI: https://doi.org/10.21241/SSOAR.71817.

Lueks, Wouter; Dreyer, Stephan; Federrath, Hannes; Simon, Judith (2026): Assessing age assurance technologies: effectiveness, side-effects, and acceptance. arXiv. DOI: https://doi.org/10.48550/arXiv.2603.25695.

Ma, Ili; Sultan, Mubashir; Kozyreva, Anastasia; Bos, Wouter van den (2026): Understanding the impact of misinformation on adolescents. In: *Nature Human Behaviour*, 10 (1), 18–28. DOI: https://doi.org/10.1038/s41562-025-02338-8.

Maier, Eva-Maria; Tanczer, Leonie Maria; Klausner, Lukas Daniel (2025): Surveillance disguised as protection: a comparative analysis of sideloaded and in-store parental control apps. In: *Proceedings on Privacy Enhancing Technologies* (2), 107–24. DOI: https://doi.org/10.56553/popets-2025-0052.

Marzolf, Émile; O'Regan, Ellen; Gkritsi, Eliza (2026): Brussels launched an age checking app. Hackers say it takes 2 minutes to break it. In: *Politico*, 17. April 2026. Verfügbar unter https://www.politico.eu/article/eu-brussels-launched-age-checking-app-hackers-say-took-them-2-minutes-break-it, zugegriffen am 05.05.2026.

Meineck, Sebastian (2026): Meta will uns bis auf die Knochen überwachen. In: *netzpolitik.org*, 7. Mai 2026. Verfügbar unter https://netzpolitik.org/2026/du-siehst-aber-jung-aus-meta-will-uns-bis-auf-die-knochen-ueberwachen, zugegriffen am 21.05.2026.

Molly Rose Foundation (Hrsg.) (2026): Australia's social media ban – is it working? Molly Rose Foundation. Verfügbar unter https://mollyrosefoundation.org/wp-content/uploads/2026/04/MRF_Australia-Social-Media-Ban-Research_Briefing-April-26.pdf.

Nuñez, Tania R.; Radtke, Theda (2024): Is socially disruptive smartphone use detrimental to well-being? A systematic meta-analytic review on being phubbed. In: *Behaviour & Information Technology*, 43 (7), 1283–1311. DOI: https://doi.org/10.1080/0144929X.2023.2209213.

OECD (Hrsg.) (2026): OECD Digital Education Outlook 2026: Exploring Effective Uses of Generative AI in Education. Paris: OECD Publishing. DOI: https://doi.org/10.1787/062a7394-en.

Orben, Amy; Meier, Adrian; Dalgleish, Tim; Blakemore, Sarah-Jayne (2024): Mechanisms linking social media use to adolescent mental health vulnerability. In: *Nature Reviews Psychology*, 3 (6), 407–23. DOI: https://doi.org/10.1038/s44159-024-00307-y.

Raffoul, Amanda; Ward, Zachary J.; Santoso, Monique; Kavanaugh, Jill R.; Austin, S. Bryn (2023): Social media platforms generate billions of dollars in revenue from U.S. youth: Findings from a simulated revenue model. In: *PLOS ONE*, 18 (12), e0295337. DOI: https://doi.org/10.1371/journal.pone.0295337.

Rohleder, Bernhard (2023): Wie die Deutschen Social Media nutzen. Bitkom. Verfügbar unter https://www.bitkom.org/sites/main/files/2023-02/BitkomChartsSocialMedia2023.pdf, zugegriffen am 21.05.2026.

Salehi, Nasim; Marshall, Georgia Rose; Maziarfar, Mohammad Hossein; Zubrinich, Alice; Madani, Nazanin; Nickbakht, Mansoureh; Moustafa, Ahmed A. (2025): A double-edged sword perspective on young australians' use of social media: a structured narrative review. In: *Health Promotion Journal of Australia*, 36 (4), e70093. DOI: https://doi.org/10.1002/hpja.70093.

Scheiter, Katharina; Bauer, Elisabeth; Omarchevska, Yoana; Schumacher, Clara; Sailer, Michael (2025): Künstliche Intelligenz in der Schule. Eine Handreichung zum Stand in Wissenschaft und Praxis. Rahmenprogramm Empirische Bildungsforschung. Verfügbar unter https://www.empirische-bildungsforschung-bmbfsfj.de/img/KI_Review.pdf, zugegriffen am 29.05.2026.

SPD-Bundestagsfraktion (Hrsg.) (2026): Sichere Soziale Medien. Schutz von Kindern und Jugendlichen im digitalen Raum stärken. Verfügbar unter https://www.spdfraktion.de/system/files/documents/impulspapier-sichere-soziale-medien.pdf, zugegriffen am 05.05.2026.

Stadler, Matthias; Bannert, Maria; Sailer, Michael (2024): Cognitive ease at a cost: LLMs reduce mental effort but compromise depth in student scientific inquiry. In: *Computers in Human Behavior*, 160 (November), 108386. DOI: https://doi.org/10.1016/j.chb.2024.108386.

Staksrud, Elisabeth; Livingstone, Sonia; Ólafsson, Kjartan (2026): Use, views and worries on age bans on social media: responses from 29,169 children in 19 European countries. LSE Research Online (EU Kids Online). DOI: https://doi.org/10.21953/researchonline.lse.ac.uk.00138705.

Steinebach, Martin; Jager, Tibor; Simon, Judith; Lehmann, Anja (2026): EU-App zur Altersverifikation. In: *Science Media Center Germany*, 17. April 2026. Verfügbar unter https://www.sciencemediacenter.de/angebote/eu-app-zur-altersverifikation-26083, zugegriffen am 05.05.2026.

Taylor, Josh (2026): VPN apps rocket up download charts in Australia as porn websites begin blocking users. In: *The Guardian*, 9. März 2026. Verfügbar unter https://www.theguardian.com/australia-news/2026/mar/09/vpn-downloads-australia-porn-sites-blocking-users, zugegriffen am 21.05.2026.

Ukrow, Jörg (2024): Kinder- und Jugendmedienschutz und Künstliche Intelligenz – Herausforderung für den Jugendmedienschutz-Staatsvertrag (JMStV)? Stand und Reformüberlegungen unter besonderer Beachtung generativer KI und unter Berücksichtigung des geplanten Gesetzes über künstliche Intelligenz der EU. Kommission für Jugendmedienschutz. Verfügbar unter https://www.kjm-online.de/fileadmin/user_upload/KJM/Service/Publikationen/Studien_Gutachten/KI_Gutachten_2024.pdf, zugegriffen am 20.05.2026.

Unabhängige Expertenkommission „Kinder- und Jugendschutz in der digitalen Welt“ (Hrsg.) (2026): Bestandsaufnahme. Bundesministerium für Bildung, Familie, Senioren, Frauen und Jugend. Verfügbar unter https://www.bmbfsfj.bund.de/resource/blob/284628/c22a5e3075220368a8591bca19ff288b/20260420-exertenkommission-kinder-und-jugendmedienschutz-bestandsaufnahme-data.pdf, zugegriffen am 21.05.2026.

Wiedemann, Hanna; Busch, Katharina; Schlichter, Nele; Gebhardt, Lucie; Paschke, Kerstin (2026): Zwischen Fortnite, TikTok und ChatGPT: Mediennutzung, Risiken und neue Nutzungstrends bei Kindern und Jugendlichen in Deutschland. Ergebnisbericht 2025/2026. DAK-Gesundheit. Verfügbar unter https://www.dak.de/dak/unternehmen/reporte-forschung/dak-studie-mediensucht-2026_164552, zugegriffen am 05.05.2026.

Wiedemann, Hanna; Thomasius, Rainer; Paschke, Kerstin (2025): Problematische Mediennutzung bei Kindern und Jugendlichen in Deutschland. Ergebnisbericht 2024/2025. DAK-Gesundheit. Verfügbar unter https://www.dak.de/dak/unternehmen/reporte-forschung/dak-studie-mediensucht-2024_91442, zugegriffen am 06.05.2026.

Wissenschaftliche Dienste des Deutschen Bundestages (Hrsg.) (2006): Die UN-Kinderrechtskonvention und ihre Bindungswirkung in der deutschen Rechtsordnung. Deutscher Bundestag (WD 2-160/06). Verfügbar unter https://www.bundestag.de/resource/blob/414972/WD-2-160-06-pdf.pdf, zugegriffen am 21.05.2026.

Wissenschaftliche Dienste des Deutschen Bundestages (Hrsg.) (2026): Zur Beschränkung und zum Verbot von Social-Media-Plattformen. Deutscher Bundestag (WD 7-004/26). Verfügbar unter https://www.bundestag.de/resource/blob/1158560/WD-7-004-26.pdf.

Yu, Yaman; Liu, Yiren; Zhang, Jacky; Huang, Yun; Wang, Yang (2025): Understanding generative AI risks for youth: a taxonomy based on empirical data. arXiv. DOI: https://doi.org/10.48550/arXiv.2502.16383.

Mitglieder des Deutschen Ethikrates

zum Zeitpunkt der Verabschiedung der Stellungnahme am 21. Mai 2026

Prof. Dr. iur. Helmut Frister (Vorsitzender)
Prof. Dr. rer. nat. Susanne Schreiber (Stellvertretende Vorsitzende)
Prof. Dr. phil. Judith Simon (Stellvertretende Vorsitzende)
Prof. Dr. med. Dr. phil. Eva Winkler (Stellvertretende Vorsitzende)

Prof. Dr. Dr. h.c. Jutta Allmendinger
Prof. Dr. Rana Alsoufi
Prof. Dr. phil. Cornelia Betsch
Prof. Dr. iur. Hans-Georg Dederer
Dr. rer. nat. Uta Eser
Prof. Dr. Aldo Faisal
Militärbischof Dr. theol. Bernhard Felmberg
Prof. Dr. rer. pol. Nils Goldschmidt
Prof. Dr. theol. Elisabeth Gräb-Schmidt
Prof. Dr. med. Winfried Hardinghaus
Dr. phil. Ute Kalender
Hedy Kerek-Bodden
Prof. Dr. phil. Armin Nassehi
Prof. Dr. phil. habil. Annette Riedel
Prof. Dr. iur. Dr. phil. Frauke Rostalski
Prof. Dr. rer. soc. Dr. theol. Jochen Sautermeister
Prof. Dr. theol. Kerstin Schlögl-Flierl
Dr. med. Dr. h.c. Josef Schuster
Prof. Dr. phil. Mark Schweda
Prof. Dr. iur. Gregor Thüsing
Prof. Dr. Achim Wambach