

Online-Sicherheit von Kindern

SCHUTZ UND STÄRKUNG VON MINDERJÄHRIGEN IN EINER DIGITALEN WELT

BERICHT DER KO-VORSITZENDEN DES SONDERAUSSCHUSSES

FÜR DIE ONLINE-SICHERHEIT VON KINDERN

Prof. Dr. Jörg M. Fegert und Dr. Maria Melchior



Dieses Dokument stellt keinesfalls eine offizielle Stellungnahme der Europäischen Kommission dar.

Luxemburg: Amt für Veröffentlichungen der Europäischen Union, 2026.

© Europäische Union, 2026



Die Weiterverwendungspolitik der Kommission unterliegt dem Beschluss 2011/833/EU der Kommission vom 12. Dezember 2011 über die Weiterverwendung von Kommissionsdokumenten (ABl. L 330 vom 14.12.2011, S. 39, ELI: <http://data.europa.eu/eli/dec/2011/833/oj>).

Sofern nichts anderes angegeben ist, wird dieses Dokument zu den Bedingungen der Lizenz Creative Commons 4.0 International (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0/>) zur Verfügung gestellt. Dies bedeutet, dass die Weiterverwendung zulässig ist, sofern die Quelle ordnungsgemäß genannt wird und etwaige Änderungen angegeben werden.

Für jede Verwendung oder Vervielfältigung von Elementen, die nicht Eigentum der Europäischen Union sind, muss gegebenenfalls direkt bei den jeweiligen Rechteinhabern eine Genehmigung eingeholt werden.

Inhalt

VORBEMERKUNG

→ 04

VORWORT

**Sicheres Aufwachsen
in der Welt der
sozialen Medien+**

→ 07

KAPITEL 01

**Ein entwicklungsori-
entierter Ansatz für
die Online-Sicher-
heit von Kindern**

→ 29

KAPITEL 02

**Forschung zu Risiken,
denen Minderjährige
online ausgesetzt
sind**

→ 57

KAPITEL 03

**Minderjährige in der
sich rasch
wandelnden
Welt der sozialen
Medien+ schützen**

→ 86

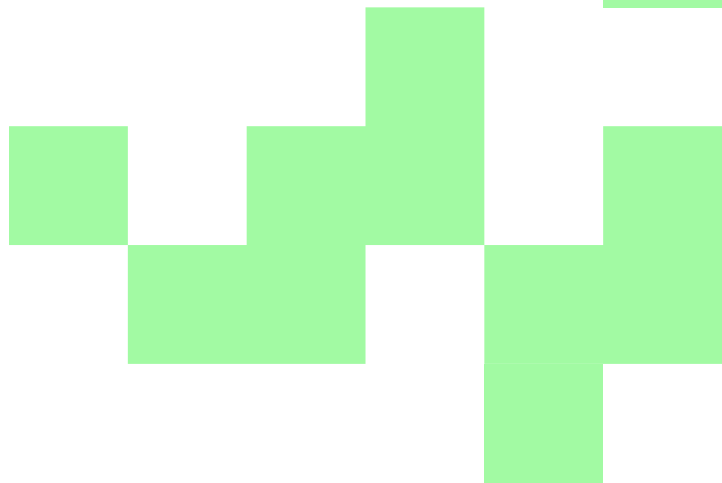
KAPITEL 04

**Minderjährige
befähigen,
sich sicher in der
digitalen Welt
zu bewegen**

→ 132

DANKSAGUNGEN

→ 158



Vorbemerkung

Im März 2026 betraute die Präsidentin der Europäischen Kommission Ursula von der Leyen zwei Sonderberater – Prof. Dr. Jörg M. Fegert und Dr. Maria Melchior – mit dem Vorsitz des Sonderausschusses für die Online-Sicherheit von Kindern und mögliche Altersbeschränkungen für die Nutzung sozialer Medien. Die Ko-Vorsitzenden wurden beauftragt, einen Bericht über die Ergebnisse der Beratungen des Ausschusses zu verfassen und Empfehlungen dazu abzugeben, wie Europa die Online-Welt für Kinder sicherer machen kann.

In dem Ausschuss, den die Kommissionspräsidentin erstmals in ihrer Rede zur Lage der Union 2025 angekündigt hatte, kamen hochrangige Wissenschaftlerinnen und Wissenschaftler, Praktikerinnen und Praktiker, Jugend- und Elternvertreterinnen und Vertreter sowie andere Fachleute aus verschiedenen Bereichen aus ganz Europa zusammen, um die Auswirkungen sozialer Medien auf Minderjährige zu prüfen.

Der Sonderausschuss trat dreimal zusammen, wobei jeweils unterschiedliche Fachleute an den Gesprächen teilnahmen. Die erste Sitzung des Sonderausschusses fand am 5. März 2026 statt und hatte die aktuellen wissenschaftlichen Erkenntnisse über die Auswirkungen sozialer Medien und des digitalen Umfelds im weiteren Sinne auf Kinder und Jugendliche zum Thema.

In der zweiten Sitzung des Sonderausschusses, die am 16. April 2026 stattfand, wurden die bestehenden Rechtsvorschriften und Instrumente der EU sowie die nationalen politischen Ansätze für den Umgang mit der Online-Sicherheit von Kindern erörtert. In der dritten Sitzung des Sonderausschusses am 16. Juni 2026 ging es vor allem um nationale Konzepte und mögliche Empfehlungen zum Schutz und zur Stärkung von Kindern und Jugendlichen in der digitalen Welt.

„[Wir werden] uns vor allem zum Ziel setzen, die Eltern zu stärken und ein sichereres Europa für unsere Kinder aufzubauen. Denn wenn es um die Sicherheit unserer Kinder im Internet geht, glaubt Europa an Eltern, nicht an Gewinne.“

— URSULA VON DER LEYEN,
PRÄSIDENTIN DER EUROPÄISCHEN
KOMMISSION, REDE ZUR LAGE
DER UNION 2025

ZU DEN WICHTIGSTEN THEMEN, DIE IN DEN SITZUNGEN DES

SONDERAUSSCHUSSES DEBATTIERT WURDEN, GEHÖRTEN FOLGENDE:

- // die positiven und negativen Auswirkungen der Einführung spezifischer Altersbeschränkungen für die Nutzung sozialer Medien und anderer digitaler Dienste,
- // maßgeschneiderte Ansätze zum Schutz und zur Stärkung Minderjähriger entsprechend den Altersgruppen, dem sozioökonomischem Hintergrund und altersspezifischen Risiken,
- // Sicherheit durch Technikgestaltung/Voreinstellungen und Verantwortung der Anbieter sozialer Medien und anderer digitaler Dienste,
- // Aufklärungs- und Sensibilisierungsmaßnahmen zur Förderung einer verantwortungsvollen Internetnutzung durch Kinder und Jugendliche, Eltern und Betreuungspersonen, Lehrkräfte und pädagogische Fachkräfte,
- // Möglichkeiten, Eltern und pädagogische Fachkräfte zu unterstützen und Kinder und Jugendliche in die Lage zu versetzen, die Chancen der digitalen Welt zu nutzen.

Die Analyse und die Empfehlungen dieses Berichts stützen sich auf wichtige Beiträge einer vielfältigen Gruppe von Sachverständigen, die zu den einzelnen Ausschusssitzungen eingeladen wurden; sie stützen sich auch auf Beiträge aus zahlreichen zusätzlichen Sitzungen mit Vertreterinnen und Vertretern der Mitgliedstaaten, insbesondere denjenigen, die vom irischen Vorsitz des Rates der EU und Luxemburg (D9+-Ministertagung) ausgerichtet wurden, von Drittländern (einschließlich Australien und Brasilien), des Europäischen Parlaments und von dessen Mitgliedern, insbesondere der interfraktionellen Arbeitsgruppe für die Rechte des Kindes, der Industrie, der Zivilgesellschaft sowie von Denkfabriken und anderen Organisationen, einschließlich des OHCHR der Vereinten Nationen und des Europäischen Datenschutzausschusses (EDSA).

Im Anschluss an diese Begegnungen arbeiteten die Ko-Vorsitzenden auf der Grundlage der gesammelten Erkenntnisse ihre Empfehlungen aus. Zwar liegt die Verantwortung für die Empfehlungen ausschließlich bei den Ko-Vorsitzenden, doch beruht ihre Arbeit in hohem Maße auf den Beiträgen anderer renommierter Sachverständiger sowie von Eltern- und Jugendvertreterinnen und -vertretern und auf dem Fachwissen der Europäischen Kommission.

Der Bericht soll als Grundlage für künftige Maßnahmen dienen, welche die Europäische Kommission und die EU-Mitgliedstaaten zur Stärkung der Online-Sicherheit von Kindern vorschlagen werden. Die vorliegende unabhängige analytische Bewertung enthält Empfehlungen und Anregungen für Kinder und Jugendliche, Eltern und Betreuungspersonen, Lehrkräfte und pädagogische Fachkräfte sowie Anbieter sozialer Medien und anderer digitaler Dienste dazu, wie Minderjährige online besser geschützt und gestärkt werden können.

GEGENSTAND UND TERMINOLOGIE

Die von Präsidentin von der Leyen vorgegebene Hauptaufgabe des Sonderausschusses bestand darin, die Online-Sicherheit von Kindern und mögliche Altersbeschränkungen für die Nutzung sozialer Medien zu erörtern. Zwar entspricht der Gegenstand dieses Berichts dieser Aufgabenstellung, doch haben die fortschreitenden Diskussionen während der Sitzungen des Sonderausschusses und andere politische Entwicklungen (z. B. der Appell der Führungsspitzen der G7 vom 17. Juni 2026 für einen sichereren digitalen Raum für Minderjährige) deutlich gemacht, dass die in diesem Bericht verwendete Terminologie präzisiert werden sollte.

Unbeschadet internationaler, EU- oder nationaler Rechtsakte werden im vorliegenden Bericht die folgenden Begriffe und die entsprechenden Begriffsbestimmungen verwendet:

Soziale Medien und andere digitale Dienste (kurz: soziale Medien+)

Im Rahmen dieses Berichts werden die Begriffe „soziale Medien+“ und „soziale Medien und andere digitale Dienste“ verwendet, um im weitesten Sinne Dienste zu definieren, die Minderjährigen zur Verfügung stehen und altersunangemessene und/oder riskante Merkmale (z. B. suchterzeugende und schädliche Merkmale, darunter unendliches Scrollen, das automatische Abspielen von Medieninhalten, Empfehlungsalgorithmen und ständige Benachrichtigungen) und/oder Inhalte enthalten können. Zu den Anbietern sozialer Medien und anderer digitaler Dienste gehören Online-Plattformen, die als Vermittler von Inhalten Dritter fungieren, z. B. soziale Medien, sowie App-Stores. Auch KI-Systeme, die Risiken für die Sicherheit und Entwicklung von Minderjährigen bergen, darunter KI-Gefährten, Videospiele, bei denen Kinder schädlichen Geschäftspraktiken oder gefährlichen Kontakten ausgesetzt sind, und Video-Sharing-Plattformen, die Minderjährigen einen nicht altersgerechten Zugang ermöglichen, fallen in diese Kategorie.

Minderjährige, Kinder und Jugendliche

Unbeschadet der gesetzlich festgelegten Bedeutung des Begriffs „Kinder“ (z. B. im Übereinkommen der Vereinten Nationen über die Rechte des Kindes) wird in diesem Bericht für einen notwendigen entwicklungsorientierten Ansatz zum Schutz Minderjähriger online plädiert, der den spezifischen Risiken und Anfälligkeiten Rechnung trägt, denen sie je nach Alter ausgesetzt sind. Für die Zwecke der vorliegenden Analyse verwenden die Autoren den Begriff „Minderjährige“ für alle Kinder und Jugendlichen unter 18 Jahren (dem Alter der Volljährigkeit). Der Begriff „Jugendliche“ bezeichnet alle Minderjährigen im Alter von 13 bis 18 Jahren. Der Begriff „Kinder“ erstreckt sich auf alle Minderjährigen unter 13 Jahren. Der Begriff „Kinderrechte“ bezeichnet in diesem Bericht die in Rechtstexten definierten Rechte aller Kinder und Jugendlichen unter 18 Jahren. Der im Mandat für die Tätigkeit des Sonderausschusses genannte Begriff „Online-Sicherheit von Kindern“ wird als Oberbegriff für den Schutz und die Stärkung von Minderjährigen in der digitalen Welt verwendet.

VORWORT

Sicheres Aufwachsen in der Welt der sozialen Medien+

Der rasche Fortschritt der digitalen Technologien hat die Art und Weise, wie Kinder und Jugendliche aufwachsen und mit Gleichaltrigen, Eltern, Lehrkräften und der Welt um sie herum interagieren, radikal verändert. Gleichzeitig sind Aktivitäten in der Offline-Welt nach wie vor von entscheidender Bedeutung für das Lernen, die Entstehung tiefgehender Beziehungen und Erfahrungen, die die Entwicklung von Minderjährigen prägen.

Die Welt der sozialen Medien+ bietet Kindern und Jugendlichen viele Möglichkeiten zu lernen, Kontakte zu knüpfen, sich zu beteiligen und kreativ zu sein. Minderjährige müssen jedoch geschult und befähigt werden, diese Chancen zu nutzen, um ihr Potenzial voll auszuschöpfen.

Gleichwohl **bergen die sozialen Medien+ auch eine Reihe von Risiken** für die gesunde Entwicklung und das Wohlbefinden von Minderjährigen. Dazu gehören das Risiko einer durch suchterzeugende Funktionen begünstigten übermäßigen Nutzung, die Substituierung entwicklungsfördernder Tätigkeiten, die Konfrontation mit schädlichen Inhalten und unangemessene Kontakte im Internet. Diese Risiken werden durch das Aufkommen neuer Technologien noch verstärkt und erfordern mutige, aber wohlüberlegte Entscheidungen zum Schutz von Kindern und Jugendlichen online.

Die breite Nutzung sozialer Medien und anderer digitaler Dienste hat **bei politischen Entscheidungsträgern und Eltern große Besorgnis über die Bedrohungen ausgelöst, denen Kinder und Jugendliche online ausgesetzt sind**. Altersbeschränkungen für den Zugang zu sozialen Medien und anderen digitalen Diensten werden zwar kritisiert, doch **können sie eine notwendige Vorsichtsmaßnahme sein**, bis nachgewiesen ist, dass der Zugang zu sozialen Medien+ für Kinder und Jugendliche sicher ist, oder bis sichere Alternativen entwickelt werden.

Bei Altersbeschränkungen geht es nicht darum, Eltern und Betreuungspersonen oder Kinder und Jugendliche selbst in erster Linie für die Online-Sicherheit Minderjähriger verantwortlich zu machen. Ebenso wenig geht es darum, die Anbieter von ihrer Verantwortung zu entbinden. **Anbieter sozialer Medien und anderer digitaler Dienste tragen weiterhin die Hauptverantwortung für die Sicherheit der Dienste, die sie entwickeln und anbieten.**

Die Beweislast muss bei den Anbietern liegen, nicht bei den Regulierungsbehörden, Eltern und Kindern. **Solange die Anbieter sozialer Medien und anderer digitaler Dienste nicht nachweisen, dass ihre Dienste inhärent sicher ("safe by design") sind, sollten sie nur eingeschränkten Zugang zu Kindern unter 13 Jahren in der EU erhalten.** Zusätzlich zu den EU-weiten Beschränkungen können die Mitgliedstaaten weitere vorsorgliche Altersbeschränkungen für Jugendliche über 13 Jahren einführen.

Vorsorgliche Altersbeschränkungen sind Sofortmaßnahmen, um das langfristige Ziel zu erreichen, durch die Förderung des kulturellen Wandels sicherzustellen, dass Räume in den sozialen Medien+ für Minderjährige sicher sind. Erste Ergebnisse aus Ländern, die pauschale Altersbeschränkungen für den Zugang zu sozialen Me-

dien eingeführt haben, zeigen, dass die meisten Minderjährigen einen Weg finden, diese Maßnahmen zu umgehen. Gleichzeitig haben sich einige Minderjährige aus riskanten sozialen Medien und digitalen Diensten zurückgezogen und haben nun mehr Zeit für Offline-Aktivitäten (wie Sport und persönliche soziale Begegnungen). Dies zeigt, dass ein schrittweiser Wandel bei den Normen für die Nutzung sozialer Medien+ durch Minderjährige möglich ist und anerkannt werden muss.

Der Wandel braucht jedoch Zeit. So haben sich beispielsweise die gesellschaftlichen Einstellungen in Bezug auf das gesetzliche Verbot körperlicher Züchtigung in der Erziehung über mehr als eine Generation hinweg weiterentwickelt (z. B. in Deutschland und Schweden). Mit dem Verbot der körperlichen Züchtigung wurden die Erwartungen an Eltern, Betreuungspersonen, Lehrkräfte und pädagogische Fachkräfte präzisiert und das Engagement Außenstehender gestärkt, um die gewaltfreie Erziehung Minderjähriger sicherzustellen. Der Erfolg dieser Maßnahme wurde durch die positiven Trends und die kontinuierliche Bewertung seit ihrer Einführung nachgewiesen.

Auch die Wirksamkeit von Altersbeschränkungen würde eine Änderung gesellschaftlicher Einstellungen erfordern. Kontinuierliche Bewertung und langfristige Beobachtung können den politischen Entscheidungsträgern dabei helfen, zu erkennen, ob sich die Gewohnheiten von Minderjährigen und ihren Eltern, Betreuungspersonen und pädagogischen Fachkräften im Laufe der Zeit ändern.

Kinder und Jugendliche, die in der heutigen Welt der sozialen Medien+ aufwachsen, müssen in die Lage versetzt werden, ein gesundes und erfülltes Leben zu führen und die Möglichkeiten, die soziale Medien und andere digitale Dienste bieten, zu nutzen. **Die Kinderrechte gelten im Internet genauso wie im realen Leben** – vom Recht auf Sicherheit und Schutz vor wirtschaftlicher Ausbeutung und Kriminalität in allen Formen (insbesondere sexueller Gewalt) bis hin zum Recht auf Zugang zu Informationen, Bildung und Freizeit.

Kinder haben das Recht, in einer Umgebung aufzuwachsen, die sicher ist und ihre Entwicklung fördert, und zwar sowohl online als auch offline. Natürlich sollten Minderjährige offline weiter unterstützt werden, doch müssen wir auch anerkennen, dass Online-Umgebungen zu einem immer wichtigeren Bestandteil ihres täglichen Lebens geworden sind. Deshalb muss in allen sozialen Medien und anderen digitalen Diensten standardmäßig für Schutz gesorgt werden.

Die Kinderrechte müssen die Grundlage für Online-Maßnahmen zur Sicherheit von Kindern bilden. Mögliche Altersbeschränkungen müssen unter uneingeschränkter Achtung der Rechte des Kindes umgesetzt werden, verhältnismäßig sein und gegen das Wohl des Kindes abgewogen werden. Die Mittel, mit denen dies erreicht werden soll, müssen mit den technologischen Entwicklungen Schritt halten.

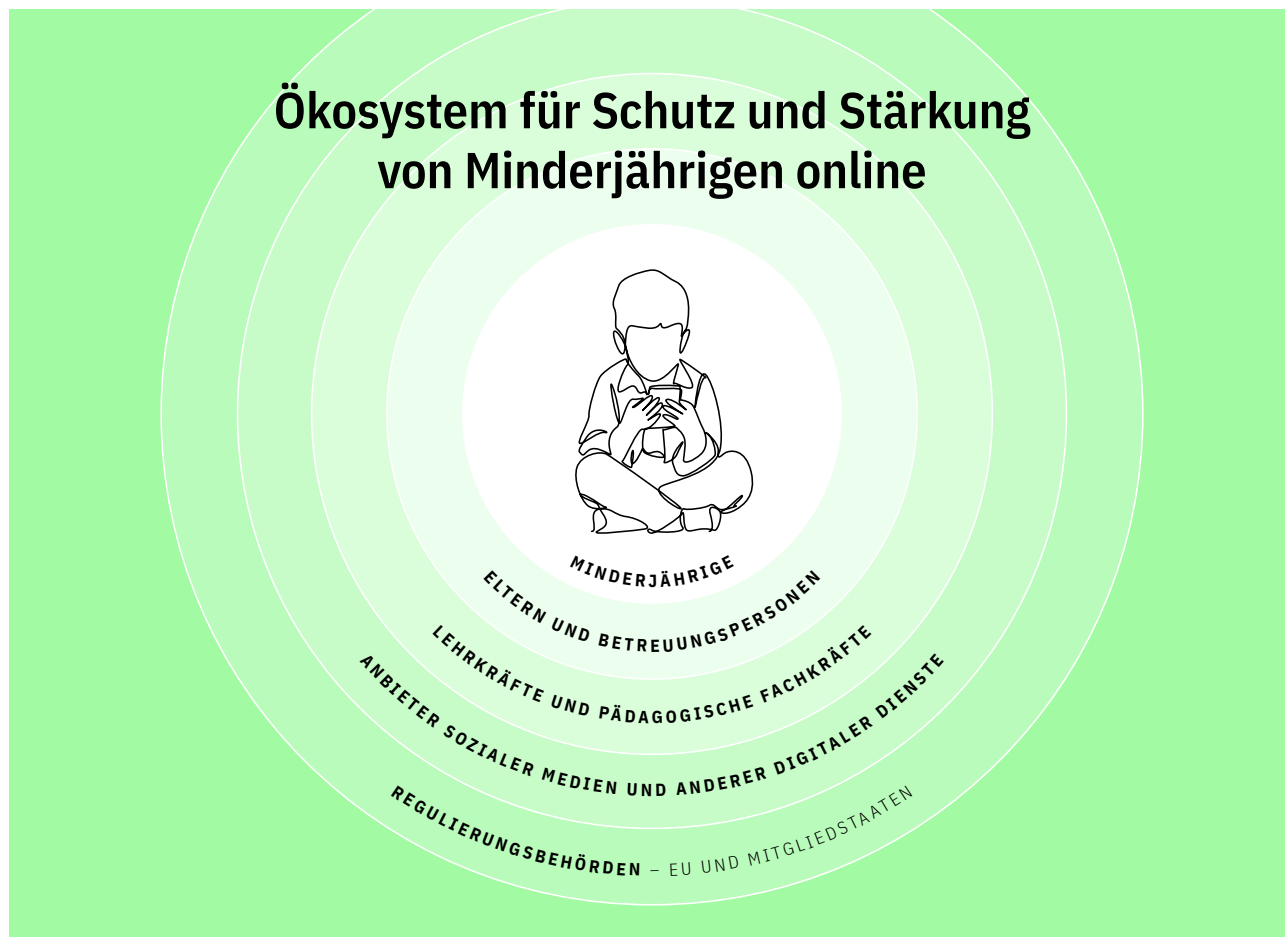
Zwar tragen nach wie vor die Anbieter sozialer Medien und anderer digitaler Dienste die Hauptverantwortung für die Sicherheit ihrer Dienste, insbesondere für Minderjährige, doch **bedarf es eines Ökosystems von Akteuren, um Kinder und Jugendliche in der Welt der sozialen Medien+ zu schützen und zu stärken.** Von den Regulierungsbehörden, die die erforderlichen Maßnahmen ergreifen müssen, über die Anbieter, die sichere und altersgerechte Dienste anbieten, bis hin zu Eltern, Betreuungspersonen, Lehrkräften und pädagogischen Fachkräften, die eine Schlüsselrolle bei der Überwachung und Anleitung der Online-Nutzung durch Minderjährige spielen. Da Minder-

„Seit Jahrzehnten arbeiten wir daran, die reale Welt für Kinder sicherer zu machen, und das Gleiche müssen wir auch in der digitalen Welt tun. Die Chancen, die uns die Technologie bietet, dürfen nicht auf Kosten der Sicherheit, Gesundheit oder des Glücks unserer Kinder gehen.“

— URSULA VON DER LEYEN, PRÄSIDENTIN DER EUROPÄISCHEN KOMMISSION

jährige reifer werden und sich die sozialen Medien+ rasch verändern, **hängt der Erfolg des Ökosystems von den miteinander verknüpften Maßnahmen aller Akteure ab**, die dieselbe Vision haben: Kinder und Jugendliche, die in einer digitalen Welt sicher aufwachsen.

Abbildung 1: Ökosystem zum Schutz und zur Stärkung von Minderjährigen online



Zunehmende politische Dynamik zugunsten einer Stärkung der Online-Sicherheit von Kindern

Die vergangenen Monate haben gezeigt, dass die Online-Sicherheit von Kindern weltweit immer größeres Gewicht in der Politik erhält. Die **Einführung, Umsetzung und kontinuierliche Evaluation des Hinauszögerns des Zugangs zu den sozialen Medien durch Australien hat der übrigen Welt wichtige Erkenntnisse geliefert**. Andere Länder wie das Vereinigte Königreich und Kanada sind dem Beispiel gefolgt und haben ebenfalls Legislativvorschläge geplant, und Indonesien hat bereits ein Verbot erlassen.

Einem aktuellen Bericht zufolge sind 92 % der Europäerinnen und Europäer der Ansicht, dass die Stärkung des Online-Schutzes von Kindern und Jugendlichen eine Priorität für die EU sein sollte^a.

a. Europäische Kommission, „[Digitale Dekade – Eurobarometer-Bericht – Februar-März 2026](#)“ (nur auf Englisch abrufbar), 2026.

Auch die politisch Verantwortlichen in Europa haben damit begonnen, sich mit diesem Thema zu befassen. Die Erklärung von Jütland^b vom September 2025 und die Entschließung des Europäischen Parlaments, in der ein EU-weites digitales Mindestalter gefordert wird^c, die Einsetzung des Sonderausschusses für die Online-Sicherheit von Kindern durch Präsidentin von der Leyen und die jüngsten Schlussfolgerungen des Europäischen Rates^d sind klare Anzeichen dafür, dass die politische Dynamik für konkrete Maßnahmen zur Bewältigung der zunehmenden Risiken, denen Kinder online ausgesetzt sind, zunimmt.

Im Juni 2026 einigten sich die G7 – Deutschland, Frankreich, Italien, Japan, Kanada, das Vereinigte Königreich, die Vereinigten Staaten und die Europäische Union – erstmals auf höchster politischer Ebene auf gemeinsame Grundsätze zum Schutz Minderjähriger vor digitalen Diensten, die Risiken bergen^e.

Darüber hinaus **erlassen mehrere EU-Mitgliedstaaten Rechtsvorschriften zur Festlegung eines Mindestalters für den Zugang zu sozialen Medien und anderen digitalen Diensten**, durch die Kinder und Jugendliche Schaden erleiden können. So schlägt Frankreich beispielsweise aktuell eine Altersgrenze von 15 Jahren auf der Grundlage einer schwarzen Liste zu beschränkender Dienste vor. Griechenland plant eine Altersgrenze von 15 Jahren für soziale Online-Netzwerke. Dänemark erwägt eine Beschränkung für Minderjährige unter 16 Jahren mit der Option, das Alter mit Zustimmung der Eltern zu senken. Schweden sieht eine Beschränkung auf der Grundlage des Jahres vor, in dem das Kind 15 Jahre alt wird, wobei mehrere Arten von Dienstleistungen ausgenommen sind. Viele andere, von Portugal und Spanien bis hin zu Deutschland und Polen, erwägen, Rechtsvorschriften zu diesem Thema zu erlassen.

Vor diesem Hintergrund stellt die Fragmentierung des europäischen Binnenmarkts für digitale Dienste ein echtes Risiko dar. Angesichts dessen fordern viele Mitgliedstaaten, dass dieses Thema auf EU-Ebene geregelt werden sollte. Es sollte anerkannt werden, dass die Mitgliedstaaten unterschiedliche kulturelle und nationale Herangehensweisen in Bezug auf Erziehung, digitale Kompetenz und den Schutz Minderjähriger haben. Eine Fragmentierung könnte dazu führen, dass Minderjährige je nach EU-Mitgliedstaat unterschiedliche Schutzniveaus genießen. Dies würde auch bedeuten, dass die Regulierungsbehörden mit praktischen Schwierigkeiten bezüglich der Durchsetzung und die Anbieter mit höheren Befolgungskosten konfrontiert sein könnten. Dies wiederum hätte Folgen für die Entwicklung sichererer sozialer Medien und anderer digitaler Dienste und für die Wirksamkeit der Rechtsvorschriften zur Online-Sicherheit.

Die EU hat bereits konkrete Maßnahmen zum Schutz von Minderjährigen ergriffen. Die jüngsten Beschlüsse der Europäischen Kommission haben nur unterstrichen, dass das Vorgehen gegen die Bedrohungen, denen Kinder und Jugendliche online ausgesetzt sind, auf konkreten Fakten beruhen muss. Die vorläufigen Feststellungen gegen Meta und TikTok wegen mutmaßlicher Nichteinhaltung der hohen Standards für den Online-Schutz Minderjähriger, die nach dem Gesetz über digitale Dienste erforderlich sind, und wegen der nicht erfolgten Bereitstellung leicht zugänglicher Mechanismen für die Meldung von sexuellem Kindesmissbrauch darstellenden Inhalten sind deutliche Beispiele. Darüber hinaus haben die jüngsten wegweisenden Urteile US-amerikanischer Gerichte einen historischen Wendepunkt in der Debatte über die Haftung von Plattformen markiert.

- b.** [Dänischer Vorsitz, Rat der Europäischen Union, „Die Erklärung von Jütland: Gestaltung einer sicheren Online-Welt für Minderjährige“ \(nur auf Englisch abrufbar\), 2026.](#)
- c.** [Europäisches Parlament, „Schutz von Minderjährigen im Internet – Entschließung des Europäischen Parlaments vom 26. November 2025 zu dem Schutz von Minderjährigen im Internet“ \(2025/2060\(INI\)\), 2025.](#)
- d.** [Europäischer Rat, Schlussfolgerungen des Europäischen Rates, 19. März 2026.](#)
- e.** [G7, „Leaders' call on a safer digital space for minors“ \(„Staats- und Regierungschefs fordern einen sichereren digitalen Raum für Minderjährige“, nur auf Englisch abrufbar\), 2026.](#)

Eine kurze Geschichte des Online-Schutzes von Minderjährigen

Die Bemühungen um den Schutz von Kindern und Jugendlichen im Internet sind so alt wie das Internet selbst und stammen aus einer Zeit vor sozialen Medien, Smartphones und KI. Die Grundlagen der heutigen Vorschriften zum Schutz von Minderjährigen im Internet wurden in den 1990er-Jahren und Anfang der 2000er-Jahre mit Rechtsakten geschaffen, die es Diensten und Unternehmen ermöglichen sollten, grenzüberschreitend tätig zu sein und Informationen auszutauschen. Obwohl diese Vorschriften nicht ausschließlich zum Schutz von Kindern und Jugendlichen im Internet konzipiert wurden, wurden darin viele der Grundsätze festgelegt, die den aktuell geltenden Rechtsvorschriften in drei Bereichen nach wie vor zugrunde liegen.

Erstens wurden mit der Regulierung von Medien und digitalen Diensten im Binnenmarkt gemeinsame Vorschriften für Fernsehprogramme in ganz Europa eingeführt, unter anderem Schutzvorkehrungen gegen Inhalte, die für Minderjährige schädlich sein könnten. Der erste harmonisierte Rahmen für Online-Dienste oder „Dienste der Informationsgesellschaft“ (im Rahmen der Richtlinie über den elektronischen Geschäftsverkehr) förderte auch die Entwicklung grenzüberschreitender Online-Dienstleistungen innerhalb der EU.

Der zweite Bereich sind die Vorschriften zum Datenschutz und zum Schutz der Privatsphäre, beginnend mit den gemeinsamen Normen der Datenschutzrichtlinie von 1995 für die Erhebung und Nutzung personenbezogener Daten in den Mitgliedstaaten.

Der dritte Bereich ist der Verbraucherschutz. Durch gemeinsame EU-Vorschriften werden irreführende und aggressive Geschäftspraktiken bekämpft. Mit diesen Vorschriften wird anerkannt, dass schutzbedürftige Verbraucherinnen und Verbraucher zusätzlichen Schutz benötigen, was ein wichtiger Grundsatz im digitalen Umfeld ist. Dies gilt auch für Fälle, in denen Kinder und Jugendliche Geschäftspraktiken ausgesetzt sind, die sie möglicherweise anders betreffen als Erwachsene.

Als die digitalen Technologien mit der Zeit ein immer größerer Bestandteil des alltäglichen Lebens wurden, hat die EU diese Rechtsrahmen immer wieder auf den neuesten Stand gebracht, um auf neue Herausforderungen zu reagieren. Mit der Datenschutz-Grundverordnung (DSGVO) wurden spezifische Schutzmaßnahmen zum Schutz der personenbezogenen Daten und der Einwilligung von Kindern im Internet eingeführt. Die Richtlinie über audiovisuelle Mediendienste wurde auf neue Formen audiovisueller Inhalte und Video-Sharing-Plattformen ausgeweitet. Schließlich wurden mit dem Gesetz über digitale Dienste Vorschriften für Online-Vermittlungsdienste festgelegt, unter anderem für den besonderen Zweck des Schutzes Minderjähriger.

Diese Entwicklung spiegelt einen allgemeinen Trend wider: Digitale Technologien lassen sich nicht mehr eindeutig in eine einzige regulatorische oder rechtliche Kategorie einordnen. Soziale Medien und andere digitale Dienste kombinieren Elemente von Medien, Kommunikation, Handel und Datenverarbeitung, häufig innerhalb derselben Plattform. Folglich muss ein wirksamer Ansatz für den Online-Schutz von Minderjährigen ganzheitlich sein und sich auf Instrumente in mehreren Bereichen des EU-Rechts stützen, einschließlich der Regulierung von Plattformen, des Datenschutzes, des Verbraucherschutzes und der Regulierung audiovisueller Medien.

Mit der raschen Entwicklung und Verbreitung von KI vervielfachen sich die Risiken für Minderjährige online. Parallel dazu werden soziale Medien und andere digitale Dienste kontinuierlich weiterentwickelt, um die Aufmerksamkeit der Nutzer in der heutigen „Aufmerksamkeitsökonomie“ zu wecken und aufrechtzuerhalten. Es ist wichtiger denn je, dass die Regulierungsbehörden tätig werden, um den Schutz von Minderjährigen zu stärken und sie in die Lage zu versetzen, sich in der Welt der sozialen Medien+ sicher zurechtzufinden.

Die Erkenntnisse über die Risiken und Chancen für Minderjährige online

Der rasche technologische Wandel hat Kindern außerordentliche Möglichkeiten eröffnet, sich mit Gleichaltrigen auszutauschen, ihre Kreativität zum Ausdruck zu bringen und Zugang zu Wissen und Hilfe zu erhalten. Kinder sind jedoch keine Erwachsenen, und in der Umgebung der sozialen Medien+ sind sie je nach ihrem Alter unterschiedlichen Risiken für ihre körperliche und psychische Gesundheit und Entwicklung ausgesetzt. Sozioökonomische und individuelle Faktoren wie der familiäre Hintergrund und das Geschlecht sowie die Gestaltung sozialer Medien und anderer digitaler Dienste haben ebenfalls prägenden Einfluss.

Solide Erkenntnisse darüber, wie Risiken und Schäden mit sozialen Medien und anderen digitalen Diensten zusammenhängen, sind unerlässlich, um geeignete Maßnahmen zum Schutz und zur Stärkung Minderjähriger online ergreifen zu können. Spezifische Merkmale, Funktionen oder Formate, die in sozialen Medien+ implementiert werden, können je nach den sozialen und persönlichen Umständen eines Kindes oder Jugendlichen in unterschiedlichem Maße schädlich sein. Minderjährige, die ethnischen und religiösen Minderheiten angehören, Teil der LGBTIQ+-Gemeinschaft sind oder besondere pädagogische Bedürfnisse oder bereits bestehende psychische Erkrankungen haben, können besonders anfällig für Gefahren im digitalen Raum sein. Diese Anfälligkeit wird natürlich durch soziale Medien und andere digitale Dienste mit schädlichen, manipulativen oder suchterzeugenden Inhalten oder Designs noch verstärkt. Die Forschungsarbeit und die Sammlung von Erkenntnissen sollten in jedem Fall mit der Weiterentwicklung dieser Merkmale Schritt halten.

Minderjährige sind durch die sozialen Medien und andere digitale Dienste weitreichenden Risiken für ihre körperliche und psychische Gesundheit ausgesetzt. Was die körperliche Gesundheit betrifft, so verdrängt übermäßige Bildschirmzeit das Spielen im Freien und den Sport und kann sich auf die Gesundheit, die körperliche Leistungsfähigkeit und den Schlaf von Kindern auswirken. Die Nutzung von sozialen Medien+ und Endgeräten im frühen Kindesalter tritt an die Stelle des eigenständigen Erkundens und persönlicher sozialer Interaktionen. Auswirkungen auf die sozial-emotionale Entwicklung und die Anfälligkeit für psychische Probleme sind möglich. Werden Endgeräte über längere Zeiträume hinweg genutzt, kann dies auch zu Problemen wie Muskel-Skelett-Erkrankungen oder einer Überanstrengung der Augen durch digitale Medien führen.

Die Nutzung sozialer Medien und anderer digitaler Dienste ist für Kinder aber auch mit erheblichen Risiken für ihre psychische Gesundheit verbunden. Dabei besteht sowohl das Risiko, dass die sozialen Medien+ der psychischen Gesundheit von Kindern unmittelbar schaden, als auch die Gefahr, dass durch sie bestehende psychische Probleme wie Depressionen oder Ängste verschärft werden. Auch hier bestimmen soziale und individuelle Faktoren, wie stark Kinder und Jugendliche gefährdet sind.

Im Allgemeinen wird eine ausgeprägte Nutzung sozialer Medien und anderer digitaler Dienste durch Kinder und Jugendliche mit Schlaf- und Konzentrationsproblemen sowie mit einem erhöhten Auftreten von Depressionen und Ängsten in Verbindung gebracht. Durch suchterzeugende Gestaltungsmerkmale werden diese Effekte verstärkt, da sie das zwanghafte Nachsehen, die Angst, etwas zu verpassen ("fear of missing out"), und das vermehrte Vergleichen mit anderen fördern. Mögliche Folgen für Minderjährige sind ein vermindertes Selbstwertgefühl und erhöhter Stress. Algorithmische Verstärkung und Empfehlungssysteme können Desinformation und Hetze fördern. Besonders schädlich sind diese Effekte im Internet für schutzbedürftige Gruppen.

Es besteht ein beträchtliches Risiko, dass Minderjährige online mit kriminellen und illegalen Inhalten konfrontiert werden. Sowohl Erwachsene als auch Minderjährige nutzen gezielt soziale Medien und andere digitale Dienste, darunter auch Spieleplattformen, um mit Kindern und Jugendlichen in Kontakt zu treten. Dabei umfasst das Gefahrenpotenzial unter anderem sexuellen Kindesmissbrauch (oder Darstellungen davon), Grooming, Cybermobbing, Radikalisierung sowie die Anstiftung zu illegalen Handlungen, Gewalttaten oder Terrorismus. Aus der weitverbreiteten Nutzung von KI-Systemen ergibt sich eine ernsthafte Gefahr für Kinder und Jugendliche, da Darstellungen sexuellen Kindesmissbrauchs künstlich erzeugt werden können (z. B. Deepfakes). Die hier beschriebenen Arten des Missbrauchs wirken sich verheerend auf die Entwicklung sowie die psychische und körperliche Gesundheit von Minderjährigen aus und können sie im schlimmsten Fall das Leben kosten.

In erster Linie sind die Anbieter sozialer Medien und anderer digitaler Dienste dafür verantwortlich, dass bei der Nutzung ihrer Dienste die Sicherheit Minderjähriger gewährleistet ist. Darüber hinaus ist es wichtig, dass Eltern und Betreuungspersonen im Blick behalten, wie viel Zeit Kinder und Jugendliche online verbringen, und dass sie ihnen Hilfestellung bieten, um die Risiken, denen sie in den sozialen Medien+ ausgesetzt sind, gemeinsam mit ihnen zu bewältigen. Unabhängig vom Alter ist es von entscheidender Bedeutung, für angemessene Offline-Aktivitäten und persönliche Begegnungen zu sorgen.

Trotz der zahlreichen Gefahren – **die Welt der sozialen Medien+ bietet Kindern und Jugendlichen viele Möglichkeiten.** Wenn Minderjährige in die Lage versetzt werden, sich sicher online zu bewegen, und mit soliden digitalen Kompetenzen ausgestattet sind, kann die Nutzung sozialer Medien und anderer digitaler Dienste dem Wohlbefinden und der sozialen Vernetzung zugutekommen, einen unterstützenden Kontakt zu Gruppen von Gleichaltrigen ermöglichen und Chancen für Selbstentfaltung, gesellschaftliches Engagement und unabhängiges Lernen bieten. Es hat sich gezeigt, dass gezielte Initiativen für digitale Kompetenzen – wie die EU-Strategie „Besseres Internet für Kinder“, die Safer-Internet-Zentren sowie auf nationaler Ebene die Verankerung von Medienkompetenz in den Lehrplänen für die allgemeine und berufliche Bildung – kritisches Denken fördern, die Widerstandsfähigkeit gegenüber Desinformation erhöhen und Minderjährige in die Lage versetzen können, sich sicher im Internet zu bewegen.

Soziale Medien und andere digitale Dienste, die „safe by design“ sind, könnten die Position von Kindern und Jugendlichen im Internet stärken und ihnen mehr Teilhabe ermöglichen, indem sie den Erwerb von digitalen Kompetenzen und Medienkompetenz fördern. Durch eine altersgerechte digitale Bildung in den Schulen und mit der Unterstützung von Eltern und Betreuungspersonen könnten Minderjährige außerdem dazu befähigt werden, die Chancen der Online-Welt zu nutzen und mögliche Risiken und Gefahren zu bewältigen.

Altersspezifische Risiken müssen adressiert werden

Je älter und unabhängiger Kinder werden, desto weniger können Eltern sie bei ihren Online-Aktivitäten beaufsichtigen. Der Einfluss Gleichaltriger spielt eine immer wichtigere Rolle. Jugendliche können sich, je näher sie der Volljährigkeit kommen, zunehmend eigenständig online bewegen und die Risiken, denen sie dort ausgesetzt sind, besser verstehen und bewältigen. Es steht außer Frage, dass sich die Bedürfnisse eines 3-Jährigen von denen eines 16-Jährigen unterscheiden. Daher ist es wichtig, **in Bezug auf die Online-Sicherheit von Kindern einen entwicklungssensiblen Ansatz zu verfolgen, der sich im vorliegenden Bericht in der Unterscheidung verschiedener Altersgruppen** niederschlägt:

Kinder **unter 3 Jahren** sind durch passive Internetnutzung vor allem Risiken mit Blick auf den Beziehungsaufbau und „Technoferenz“^f ausgesetzt. Diese Risiken entstehen in erster Linie, wenn Betreuungspersonen versuchen, kleine Kinder mithilfe von Bildschirmen zu „beruhigen“ oder abzulenken, anstatt sich direkt mit ihnen zu beschäftigen. Dies kann sich auf die Aufmerksamkeitsspanne, den Spracherwerb und die sozial-emotionale Entwicklung von Kindern auswirken.

Kinder **zwischen 3 und 5 Jahren** sind im Rahmen einer zunehmend unabhängigen Nutzung unter Aufsicht zunehmend den Risiken in der digitalen Welt und einer längeren Bildschirmnutzung ausgesetzt. Soziale Medien und andere digitale Dienste sind mit ihrer Auslegung auf sofortige und wiederkehrende Belohnung sowie kontinuierliche externe Stimulation dem Entwicklungsstand von Kindern grundsätzlich nicht angemessen und können deren langfristige Entwicklung beeinträchtigen.

Kinder **zwischen 6 und 9 Jahren** nutzen soziale Medien und andere digitale Dienste in stark zunehmendem Umfang. Die Bewertung von außen in der Online-Welt (z. B. Likes, Punktzahlen und Bestenlisten) vermischt sich mit dem entstehenden Selbstwertgefühl, das auf der Entwicklung von Fähigkeiten in der realen Welt beruht. Dadurch können leistungsbezogene Ängste sowie der Vergleich mit Gleichaltrigen verstärkt und die Anfälligkeit für Cybermobbing, Hetze und Belästigung durch Gleichaltrige erhöht werden.

^f Die Unterbrechung der Interaktionen zwischen Eltern und Kindern durch Technologie.

Für Kinder **zwischen 10 und 12 Jahren** ist der Zugang zu sozialen Medien+ eine zentrale Voraussetzung für die Teilnahme am Sozialleben. In diesem Alter sind Kinder am stärksten dem Zusammenspiel von entwicklungsbedingten Anfälligkeiten und plattformgesteuerter Verstärkung ausgesetzt. Algorithmische Empfehlungssysteme fördern den sozialen Vergleich sowie die Konfrontation mit gefährlichen oder illegalen Inhalten (einschließlich Darstellungen sexuellen Kindesmissbrauchs, extremistischer Propaganda und Desinformation) und mit suchterzeugenden Gestaltungsmustern, die das Auftreten von Depressionen und Ängsten begünstigen. Jüngste prospektive Untersuchungen deuten darauf hin, dass bei Kindern, die mit 12 Jahren (statt mit 13) ihr erstes Smartphone bekommen, nach einem Jahr ein erhöhtes Risiko für Depressionen und andere psychische Probleme bestehen könnte^g. Anhand dieses Beispiels zeigt sich, dass Kinder unter 13 Jahren im Allgemeinen besonders schutzbedürftig sind.

Bei Jugendlichen **zwischen 13 und 15 Jahren** findet mit Blick auf soziale Medien und andere digitale Dienste ein Übergang von einer Nutzung unter Aufsicht zu einer zunehmend eigenständigen Nutzung statt. In diesem Alter nimmt die Wirksamkeit herkömmlicher Aufsicht durch Betreuungspersonen und Schulpersonal ab. Die Risiken ergeben sich zunehmend aus den Strukturen der sozialen Medien und anderen digitalen Dienste und nicht mehr nur aus dem individuellen Verhalten. Eine zentrale Herausforderung besteht im Umgang mit algorithmischen Systemen, die angezeigte Inhalte vorgeben und das Verhalten beeinflussen, gleichzeitig aber nur begrenzt transparent sind.

Eine zunehmende Eigenständigkeit gehört heutzutage nicht nur offline, sondern auch in der Online-Welt zum Aufwachsen dazu. Es geht also nicht darum, Jugendliche in ihrem Übergang zur Eigenständigkeit zurückzuhalten, sondern vielmehr dafür zu sorgen, dass sie in einer mit großer Verwundbarkeit einhergehenden Entwicklungsphase weniger Gefahren ausgesetzt sind. Ein wirksamer Schutz erfordert einen entwicklungsorientierten, vielschichtigen Ansatz, bei dem die Regulierung sozialer Medien und anderer digitaler Dienste, Bildungsmaßnahmen sowie Unterstützung zur Selbstregulierung und kritischen Mediennutzung ineinandergreifen.

Jugendliche **zwischen 16 und 18 Jahren** befinden sich in einer Phase, in der sich ihre Identität zunehmend festigt und ihre Eigenständigkeit zunimmt. Ihre Fähigkeiten entwickeln sich weiter, sodass sie die Risiken, denen sie im Internet ausgesetzt sind, besser verstehen und bewältigen können. Ihre neurobiologische Entwicklung ist jedoch bei Weitem noch nicht abgeschlossen, und die Nutzung sozialer Medien und anderer digitaler Dienste geht mit einem erhöhten Risiko für Sucht, Ängste und psychische Probleme einher. In diesem Alter müssen Jugendliche Kompetenzen (z. B. kritisches Denken und Bewerten) erwerben, die sie benötigen, um sich erfolgreich und sicher in der digitalen Welt zu bewegen und die sich dort bietenden Möglichkeiten voll auszuschöpfen.

g. [Children's Hospital of Philadelphia, „Age Limits Alone Won't Fix Smartphone Risks, Suggests Children's Hospital of Philadelphia Study“, 2026, abgerufen am 12. Juli 2026.](#)

Sechs Leitprinzipien für den Schutz und die Stärkung Minderjähriger online

Da die sozialen Medien+ für Kinder und Jugendliche sowohl Risiken als auch Chancen bergen können, bedarf es eines umfassenden politischen Rahmens, durch den Minderjährige online geschützt und gestärkt werden. Die folgenden **sechs von den Ko-Vorsitzenden ausgearbeiteten Leitprinzipien dienen als Richtschnur für die Arbeit des Sonderausschusses** und bilden das Gerüst für den vorliegenden Bericht. Als Grundlage für Maßnahmen sollten eine solide Datenlage und Analyse in Bezug auf die Herausforderungen und Chancen für Kinder in der digitalen Welt dienen. Damit die Maßnahmen Wirkung zeigen, müssen sie effektiv umgesetzt und evaluiert werden.

LEITPRINZIP 1

Entwicklungsorientierter Ansatz (siehe Kapitel 1)

Regulierung muss altersgerecht sein und Orientierungshilfen müssen differenziert sein. Da die Entwicklung von Kindern und Jugendlichen in Phasen verläuft, sollten Schutzmaßnahmen so gestaltet und umgesetzt werden, dass sie den für die jeweiligen Altersgruppen relevanten Risiken Rechnung tragen. Nach Möglichkeit sollte bei diesen Maßnahmen der persönliche und soziale Hintergrund der Kinder berücksichtigt werden, der sich verstärkend auf die Risikoanfälligkeit auswirken kann.

LEITPRINZIP 2

Gleichstellung und Diversität (siehe Kapitel 2)

Ungleichheiten zwischen Altersgruppen und sozioökonomischen Gruppen mit Blick auf die Risiken und die Anfälligkeit für Gefahren im Internet sollten anerkannt werden. Geschlecht, Sexualität, ethnischer und religiöser Hintergrund, sonderpädagogischer Förderbedarf und bereits bestehende psychische Probleme sind ausschlaggebend dafür, wie anfällig Minderjährige für Online-Gefahren sind. Diese Faktoren beeinflussen auch, welche Ressourcen und Kapazitäten Eltern und Betreuungspersonen zur Verfügung stehen, um Kinder und Jugendliche auf ihrem Weg zur Eigenständigkeit zu unterstützen.

LEITPRINZIP 3

Schutz Minderjähriger (siehe Kapitel 3)

Kinder und Jugendliche müssen die Vorteile sicherer sozialer Medien+ nutzen können. Der Schutz Minderjähriger vor schädlichen Inhalten, suchterzeugenden Funktionen, digitaler Vernachlässigung^h und Internetkriminalität (z. B. sexuellem Missbrauch) sollte in die Gestaltung sozialer Medien und anderer digitaler Dienste einfließen. Schädliche Inhalte oder Funktionen sollten für Minderjährige leicht zu melden sein. Die Anbieter sollten solche Meldungen vorrangig behandeln und schädliche Inhalte oder Funktionen unverzüglich entfernen.

h. Das wiederholte Versäumnis einer Betreuungsperson, ein dem Entwicklungsstand angemessenes Maß an Aufmerksamkeit, Zugewandtheit, Aufsicht oder Schutz zu bieten, da wesentliche Betreuungsaufgaben durch digitale Technologien gestört, ersetzt oder beeinträchtigt werden.

LEITPRINZIP 4**Rechenschaftspflicht digitaler Dienste und Verbraucherrechte (siehe Kapitel 3)**

Die Anbieter sozialer Medien und anderer digitaler Dienste müssen die Hauptverantwortung dafür tragen, dass der Zugang zu Online-Räumen und deren Nutzung für Minderjährige sicher sind. Digitale Dienste sollten dazu angelegt werden, Maßnahmen für „safety by design“ umzusetzen, und eine inhaltsbezogene Regulierung sollte schnell durchgesetzt werden. Die Beweislast muss auf den Anbietern sozialer Medien und anderer digitaler Dienste liegen, nachzuweisen, dass die Funktionen ihrer Dienste nicht schädlich sind, bevor sie Zugang zu Kindern und Jugendlichen erhalten.

LEITPRINZIP 5**Stärkung und Vermittlung von Medienkompetenz (siehe Kapitel 4)**

Eltern und Betreuungspersonen, Lehrkräfte und pädagogische Fachkräfte sollten in die Lage versetzt werden, Kinder und Jugendliche bei ihrem schrittweisen Übergang zu einer sicheren und eigenständigen Online-Nutzung zu unterstützen. Es sollten ausreichend Möglichkeiten (z. B. Schulungen zur digitalen Kompetenz und Medienkompetenz) und eine angemessene Infrastruktur geschaffen werden, um Eltern dazu zu befähigen, über ihr eigenes Handeln nachzudenken und Minderjährige bei ihren Online-Aktivitäten anzuleiten. Die entsprechenden Maßnahmen müssen auf die Rollen der Betreuungspersonen und pädagogischen Fachkräfte zugeschnitten sein, die sich mit zunehmendem Alter der Kinder und Jugendlichen verändern.

LEITPRINZIP 6**Rechte und Teilhabe von Kindern (siehe Kapitel 4)**

Das Recht von Kindern auf sichere Teilhabe, Interaktion und gemeinsame Gestaltung sollte online wie offline geschützt werden. Die in den einschlägigen internationalen Rahmenwerkenⁱ verankerten Rechte von Kindern sollten stets als Grundlage für Kinderschutzmaßnahmen dienen. Altersbezogene Zugangsbeschränkungen müssen die Rechte des Kindes online achten und verhältnismäßig, zeitlich begrenzt sowie auf das Wohl des Kindes abgestimmt sein. Dies unterstreicht die Notwendigkeit, Offline-Aktivitäten für Minderjährige aller Altersgruppen finanziell zu fördern und zu bewerben.

Sonderberater/Sonderberaterin der Präsidentin und Ko-Vorsitzende des Sonderausschusses für die Online-Sicherheit von Kindern



Prof. Dr. Jörg M. Fegert

Ärztlicher Direktor der Klinik für
Kinder- und Jugendpsychiatrie,
Psychosomatik und Psychotherapie
am Universitätsklinikum Ulm



Dr. Maria Melchior

Forschungsdirektorin am
französischen Institut für
Gesundheit und medizinische
Forschung (INSERM)

- i. Insbesondere das Übereinkommen der Vereinten Nationen über die Rechte des Kindes und die Allgemeinen Bemerkungen des Ausschusses für die Rechte des Kindes, die Charta der Grundrechte der Europäischen Union und die EU-Kinderrechtsstrategie.

SECHS LEITPRINZIPIEN für den Schutz und die Stärkung Minderjähriger online

ONLINE - SICHERHEIT VON KINDERN

ANALYSE DER SITUATION

ENTWICKLUNGSORIENTIERTER ANSATZ

altersgerechte Regulierung und differenzierte Leitlinien
sicherstellen

GLEICHSTELLUNG UND DIVERSITÄT

Ungleichheiten zwischen verschiedenen Gruppen mit Blick auf Risiken,
Anfälligkeit und digitale Gefahren anerkennen

SCHUTZ MINDERJÄHRIGER

vor schädlichen Inhalten, suchterzeugenden Gestaltungsmerkmalen, digitaler
Vernachlässigung und Kriminalität (z. B. sexuellem Missbrauch, Mobbing) schützen

RECHENSCHAFTSPFLICHT DIGITALER DIENSTE UND VERBRAUCHERRECHTE

inhärente Sicherheit und inhaltsbezogene Regulierung durchsetzen

STÄRKUNG UND VERMITTLUNG VON MEDIENKOMPETENZ

Eltern und Betreuungspersonen in die Lage versetzen, die digitalen Kompetenzen
und die Medienkompetenz von Kindern und Jugendlichen im Sinne einer
verantwortungsvollen Nutzung zu fördern

RECHTE VON KINDERN UND TEILHABE

das Recht auf sichere Teilhabe und gemeinsame Gestaltung
online schützen

MAßNAHMEN

EVALUIERUNG

Zentrale Empfehlungen zum Schutz und zur Stärkung Minderjähriger online

Das übergeordnete Ziel der in diesem Bericht enthaltenen Empfehlungen, die auf einem entwicklungssensiblen Ansatz und den sechs Leitprinzipien beruhen, besteht darin, sowohl die Notwendigkeit, Kinder und Jugendliche online zu schützen, als auch ihr Recht auf Teilhabe in den sozialen Medien+ und auf Nutzung der sich dort bietenden Chancen in ausgewogener Weise zu berücksichtigen.

Empfehlungen zur altersgerechten Nutzung sozialer Medien und anderer digitaler Dienste

0 BIS 2 JAHRE

Bildschirme und soziale Medien+ vermeiden

Längere Bildschirmnutzung in der frühen Kindheit zu vermeiden, bedeutet kein vollständiges Verbot. Vielmehr bedeutet es, die entwicklungsbedingten Bedürfnisse von Kindern in Bezug auf Bindung, Entwicklung der Sinne und frühkindlichen Spracherwerb zu respektieren. Eltern und Betreuungspersonen sollten vor allem auf persönliche Interaktion setzen und ihre eigene Nutzung digitaler Endgeräte im Auge behalten, um eine Vorbildfunktion zu übernehmen und „Technoferenz“ zu vermeiden. Dieser Ansatz steht im Einklang mit den Empfehlungen der Weltgesundheitsorganisation zur Vermeidung von Störungen der neurobiologischen und kognitiven Entwicklung und der Bildung emotionaler Bindungen sowie körperlicher Probleme (z. B. Beeinträchtigungen des Sehvermögens) bei Kindern.

3 BIS 12 JAHRE

Nutzung altersgerechter sozialer Medien+ und von Endgeräten unter Aufsicht

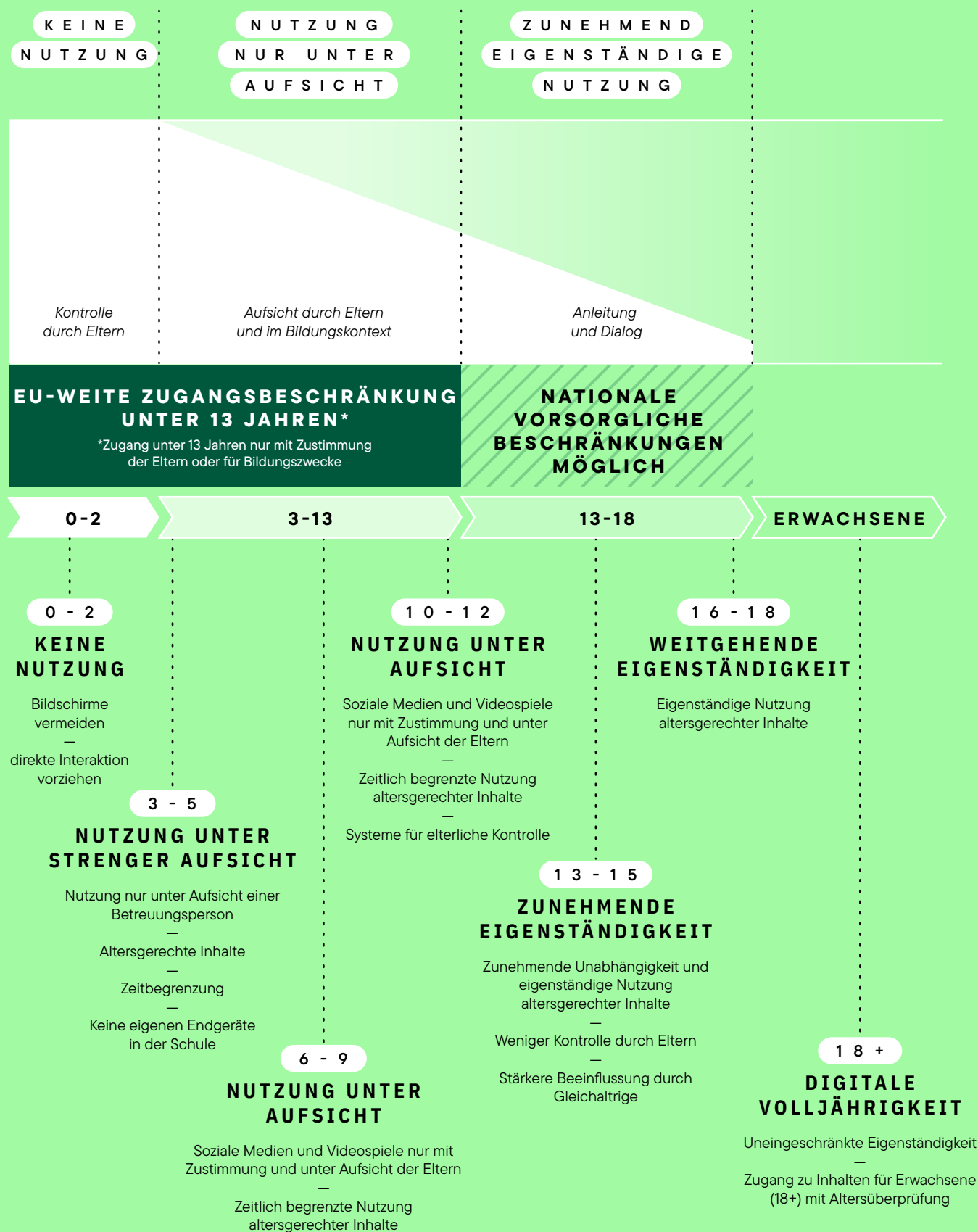
Kindern sollte nicht erlaubt werden, internetfähige Endgeräte unbeaufsichtigt zu nutzen. Schulen sollten die Gegebenheiten für eine beaufsichtigte und begrenzte Nutzung von internetfähigen Endgeräten für Bildungszwecke schaffen und digitale Kompetenzen, Medienkompetenz, emotionale Resilienz und die kritische Auseinandersetzung mit den Risiken fördern. Eltern und Betreuungspersonen sollten Kinder beaufsichtigen und ihre digitale Autonomie schrittweise mit altersgerechten sozialen Medien und anderen digitalen Diensten unterstützen. Sie sollten außerdem regelmäßig mit Kindern über die Chancen und Risiken sprechen, die sich für Minderjährige aus der Online-Nutzung ergeben. Betreuungspersonen und pädagogische Fachkräfte sollten Kinder in diesem Alter weiter dazu ermuntern, sich an Offline-Aktivitäten zu beteiligen.

13 BIS 18 JAHRE

Zunehmend eigenständige Nutzung altersgerechter sozialer Medien+

Im Alter von 13 bis 18 Jahren sollten Jugendliche nur Zugang zu altersgerechten und auf „safety by default“ beruhenden sozialen Medien und anderen digitalen Diensten haben, bei denen zentrale Sicherheitsfunktionen aktiv umgesetzt wurden (z. B. Beschränkungen für endloses Scrollen und Empfehlungssysteme). Bis solche auf „safety by default“ beruhenden sozialen Medien und anderen digitalen Dienste zur Verfügung stehen, spielt die individuelle und altersgerechte Kontrolle und Aufsicht durch die Eltern weiterhin eine wichtige Rolle. Zusätzliche Vorsichtsmaßnahmen vonseiten der Regulierungsbehörden sind denkbar. Auch mit zunehmender digitaler Autonomie bestehen bei Jugendlichen über 16 Jahren weiterhin Risiken im Zusammenhang mit schädlichen Online-Inhalten. Daher sollten Eltern und Betreuungspersonen weiter mit ihnen über ihre Online-Erfahrungen sprechen. Jugendliche sollten beim Zugang zu Hilfsdiensten und Beschwerdesystemen Vorrang haben und außerdem von unterstützenden Netzwerken Gleichaltriger („peer support networks“) profitieren, wodurch eine verantwortungsvolle Nutzung sozialer Medien und anderer digitaler Dienste gefördert würde.

Altersgerechte Nutzung sozialer Medien+ durch Minderjährige



Empfehlungen zum Schutz von Kindern und Jugendlichen online

// Eine harmonisierte EU-weite Zugangsbeschränkung für soziale Medien und andere digitale Dienste für Kinder unter 13 Jahren vorschlagen.

Eine harmonisierte EU-weite Zugangsbeschränkung für soziale Medien und andere digitale Dienste, einschließlich KI-Gefährten, für Kinder unter 13 Jahren ist notwendig. Eine solche harmonisierte Zugangsbeschränkung würde einerseits die Umsetzung einer verhältnismäßigen, rechtskonformen Altersfeststellung erleichtern und andererseits die Festlegung von Anforderungen an die Anbieter sozialer Medien und anderer digitaler Dienste hinsichtlich „safety by design“ begünstigen. Kinder unter 13 Jahren sollten nur mit Zustimmung und unter Aufsicht der Eltern oder im Bildungskontext zeitlich begrenzten Zugang zu altersgerechten sozialen Medien+ haben. Ab dem Alter von 13 Jahren sollten Jugendliche die Vorteile einer zunehmend eigenständigen Nutzung altersgerechter und sicherer sozialer Medien und anderer digitaler Dienste genießen können.

Harmonisierte Vorschriften über ein EU-weites Mindestalter von 13 Jahren würden zum reibungslosen Funktionieren des Binnenmarkts beitragen, indem ein einheitlicher Rahmen geschaffen würde, an den sich die Anbieter halten müssten. Durchsetzung und Aufsicht würden den Regulierungsbehörden sowohl auf nationaler Ebene als auch auf EU-Ebene durch harmonisierte Vorschriften erleichtert. Außerdem würde so dafür gesorgt, dass alle Minderjährigen in der EU dasselbe Maß an Schutz genießen, unabhängig von sozioökonomischen, kulturellen und einzelstaatlichen Faktoren.

// Funktionierende Systeme zur Altersfeststellung einführen, damit auf „safety by design“ beruhende und altersgerechte Systeme zum Schutz und zur Stärkung Minderjähriger online ihre Wirkung entfalten können.

Methoden der Altersfeststellung – Altersüberprüfung und Altersschätzung – müssen verhältnismäßig sein und Mindestanforderungen unterliegen, insbesondere in Bezug auf die Grundrechte der Nutzerinnen und Nutzer, wozu auch Kinderrechte und die damit verbundenen Schutzvorkehrungen zählen. Alle zur Altersfeststellung genutzten Methoden sollten höchsten Anforderungen in Bezug auf den Schutz der Privatsphäre und den Datenschutz genügen und auf die Verarbeitung von Ausweisdokumenten oder biometrischen Daten zum Zwecke der Altersschätzung verzichten. Es sollten technische Normen wie der „Null-Wissen-Beweis“ angewandt werden, um sicherzustellen, dass sowohl die zur Altersfeststellung verpflichtete Plattform als auch der Anbieter, der die Altersüberprüfung durchführt, keine Informationen erhalten, die das Tracking oder die Identifizierung der Nutzerinnen und Nutzer erlauben.

Die Methoden zur Altersfeststellung sollten das Alter oder Altersgruppen entsprechend den Anforderungen präzise bestimmen können, und für eine einfache und zuverlässige Praxisanwendung unter realen Bedingungen geeignet sein. Die Methoden sollten robust sein, um einer Umgehung sowie Sicherheitsbedrohungen entgegenzuwirken, sie sollten inklusiv (und diskriminierungsfrei) sein und allen, die sie benötigen, gleichermaßen zur Verfügung stehen. Anbieter sozialer Medien und anderer digitaler Dienste müssen ihrer Verpflichtung nachkommen, zu verhindern, dass Minderjährige Dienste mit hohem Risikopotenzial nutzen oder mit Personen in Kontakt kommen, die sich als Kinder oder Jugendliche ausgeben.

// Vorschriften für zentrale Sicherheitsfunktionen bei der Gestaltung sozialer Medien und anderer digitaler Dienste erweitern und harmonisieren.

Eine klar definierte „safety by design“-Sicherung sowie altersgerechte Schutzvorkehrungen (z. B. potenzielle Beschränkungen für endloses Scrollen, automatische Wiedergabe, Push-Benachrichtigungen und problematische Systeme für personalisierte Empfehlungen) sollten in soziale Medien und andere digitale Dienste integriert werden. Soziale Medien und andere digitale Dienste sollten durch entsprechende integrierte Standardeinstellungen Schutz vor suchterzeugenden Gestaltungsmerkmalen, Dark Patterns, unerwünschter Kontaktaufnahme und dem Rabbit-Hole-Effekt bieten. Eine Erweiterung und Harmonisierung der Vorschriften über zentrale Sicherheitsfunktionen würde für Gewissheit und Einheitlichkeit im Bereich der sozialen Medien+ sorgen. Aufgrund der raschen technologischen Entwicklung sollten die Vorschriften über zentrale Sicherheitsfunktionen anpassbar sein, damit kontinuierlich auf neue schädliche Gestaltungsmerkmale reagiert werden kann.

// Beweislast, dass Produkte und Dienste für Minderjährige sicher sind, auf Anbieter sozialer Medien und anderer digitaler Dienste verlagern.

Spezifische Altersbeschränkungen sollten gelten, bis die Anbieter sozialer Medien und anderer digitaler Dienste zentrale Sicherheitsfunktionen zum Schutz von Kindern und Jugendlichen einführen. Nur wenn Anbieter nachweisen können, dass sie sichere und altersgerechte Funktionen eingeführt haben und somit den von der EU und den Mitgliedstaaten ergriffenen Maßnahmen entsprechen, sollten sie ihre Dienste Minderjährigen anbieten dürfen. Wenn eine „safety by default“-Version vorhanden ist, sollten nicht altersgerechte Funktionen (Funktionen für Erwachsene) nur nach einer erfolgreichen Altersfeststellung aktiviert werden können.

// Durchsetzungs- und Evaluierungskapazitäten stärken.

Angeichts der zahlreichen Vorschriften, die inzwischen in Bezug auf die Online-Sicherheit von Kindern gelten (Gesetz über digitale Dienste, DSGVO, Verordnung über Künstliche Intelligenz usw.), sollten die Aufsichtsbehörden aus unterschiedlichen Rechtsfeldern intensiver zusammenarbeiten und Informationen austauschen. So können Unstimmigkeiten vermieden und kohärente, verlässliche und wirksame rechtliche Rahmenbedingungen gewährleistet werden, deren Fundament der Schutz der Grundrechte bildet. Die Europäische Kommission sollte prüfen, durch welche Mechanismen eine nahtlose Zusammenarbeit zwischen den Aufsichtsbehörden ermöglicht werden kann, um bestehende Strukturen für die Rechtsdurchsetzung zu nutzen. Darüber hinaus muss beurteilt werden, ob die für die Durchsetzung und Evaluierung zuständigen Regulierungsbehörden zusätzliche Ressourcen oder Umstrukturierungen benötigen. Es sollten Maßnahmen in Betracht gezogen werden, durch die die Zivilgesellschaft eine wichtigere Rolle bei der Durchsetzung einnehmen und einen größeren Beitrag zur Erweiterung der Durchsetzungskapazitäten leisten kann, was auch innerhalb bestehender Strukturen erfolgen kann. Die Durchsetzungsmechanismen sollten ergänzend ineinandergreifen und Überschneidungen sollten vermieden werden.

// Rasche Maßnahmen ergreifen, um Anbietern sozialer Medien und anderer digitaler Dienste klare Verpflichtungen aufzuerlegen, sexuellen Missbrauch von Kindern im Internet, auch im Rahmen interpersoneller Kommunikation, zu verhindern, aufzudecken, zu melden und zu stoppen.

Die Lücke im Bereich der Sicherheit von Kindern, die sich infolge des Auslaufens der Übergangsverordnung zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern aufgetan hat, muss rasch geschlossen werden. Der EU-Gesetzgeber sollte die vorgeschlagene langfristige Verordnung für die Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern rasch beschließen. Mehr als 80 % der Ermittlungen im Zusammenhang mit sexuellem Missbrauch von Kindern gehen auf Meldungen von Anbietern sozialer Medien und anderer digitaler Dienste zurück. Kinder haben oft zu große Angst, um Missbrauch zu melden. Die Aufdeckung von Material über sexuellen Missbrauch von Kindern, einschließlich im Rahmen interpersoneller Kommunikation ausgetauschten Materials, ist häufig die einzige Möglichkeit, den Missbrauch zu stoppen.

// Mitgliedstaaten können zusätzliche vorsorgliche Zugangsbeschränkungen für soziale Medien und andere digitale Dienste für Kinder ab 13 Jahren einführen.

Zusätzliche vorsorgliche Zugangsbeschränkungen sollten als Ergänzung zu der EU-weit gültigen Zugangsbeschränkung für soziale Medien und andere digitale Dienste für unter 13-Jährige dienen. Jugendliche dürfen nur Zugang zu sozialen Medien+ haben, die in Bezug auf Inhalte und Gestaltung sicher und altersgerecht sind und bei deren Gestaltung ihre Rechte und Bedürfnisse berücksichtigt wurden. Die Situation hat sich in den Mitgliedstaaten von Land zu Land unterschiedlich entwickelt, und manche Mitgliedstaaten ziehen vielleicht eine Altersgrenze von mehr als 13 Jahren in Betracht. Alle auf nationaler Ebene erlassenen zusätzlichen vorsorglichen Zugangsbeschränkungen sollten laufend evaluiert und gegebenenfalls neu bewertet werden, sobald soziale Medien und andere digitale Dienste für Kinder und Jugendliche „safe by default“ gemacht wurden.

// Vorschriften über den Zugang der Forschung zu Daten und über die Kontrolle stärker durchsetzen.

Mit der delegierten Verordnung über Datenzugang nach Artikel 40 des Gesetzes über digitale Dienste vom Juli 2025 wurde zugelassenen Forschenden grundsätzlich ein neuer Weg eröffnet, Zugang zu Daten von Online-Plattformen zu erhalten. Diese Daten können für Forschungsarbeiten verwendet werden, die dabei helfen werden, systemimmanente Risiken zu erkennen, festzustellen und zu verstehen sowie Risikominderungsmaßnahmen zur Förderung der Sicherheit von Kindern online zu bewerten.

Ob die verfolgten Ziele erreicht werden, hängt davon ab, ob die Vorschriften von den Anbietern sozialer Medien und anderer digitaler Dienste eingehalten und von den Regulierungsbehörden wirksam durchgesetzt werden. Der Erfolg ist auch von der Bandbreite der abgedeckten Dienste und von der Qualität und der Kontinuität der zur Verfügung gestellten Daten abhängig. Die Kommission sollte die praktische Wirksamkeit des Artikels 40 über Datenzugang und Kontrolle unter Berücksichtigung der ersten Erfahrungen von Forschenden mit der delegierten Verordnung prüfen. Nur so kann sichergestellt werden, dass Online-Plattformen Anträgen auf Datenzugang aus Compliance-Gründen, für Risikobewertungen und zu Forschungszwecken nachkommen.

Die Verpflichtungen zur Datenauskunft sind nicht nur ein zentraler Bestandteil der Transparenzvorschriften nach dem Gesetz über digitale Dienste, sondern fallen auch unter die umfassendere Verantwortung der Anbieter sozialer Medien und anderer digitaler Dienste für Risikominderung. Angesichts der Risiken, die kleinere Plattformen für Minderjährige darstellen, und der Rolle einer unabhängigen Kontrolle bei der Bewältigung dieser Risiken sollten auch diese Plattformen ermutigt werden, der Forschung Zugang zu Daten zu gewähren. Bei der Umsetzung von Artikel 40 sollten standardmäßig die FAIR-Prinzipien^j für das Forschungsdatenmanagement angewandt werden.

Empfehlungen zur Stärkung von Kindern und Jugendlichen online

// Minderjährigen mehr Möglichkeiten bieten, die Welt der sozialen Medien+ in einem geschützten Rahmen aktiv mitzugestalten.

Kinder und Jugendliche sollten die Möglichkeit erhalten, Rechtsvorschriften, Strategien und Bildungsinitiativen zur Förderung der Sicherheit und Stärkung von Kindern im Internet aktiv und wirksam mitzugestalten. Dementsprechend sollten mehr Maßnahmen für die Beteiligung von Kindern und Jugendlichen an einschlägigen Vorhaben ergriffen werden. So sollten Kinder beispielsweise bei der Gestaltung von Sicherheitsstrategien, Lernprogrammen, Evaluierungen und Leitfäden einbezogen werden. Die Auswirkungen dieser Maßnahmen auf die Sicherheit und die Rechte von Kindern sollten kontinuierlich beobachtet und evaluiert werden.

Bei Verfahren zur Beteiligung von Kindern sollte sichergestellt werden, dass die Kinder klare Informationen erhalten, dass sie verstehen, wie ihre Beiträge weiterverwendet werden, und dass sie über die weiteren Entwicklungen am Laufenden gehalten werden. Insbesondere sollten auch Kinder aus benachteiligten, marginalisierten und schutzbedürftigen Gruppen einbezogen werden. Für alle Aktivitäten, an denen Kinder beteiligt sind, müssen geeignete Schutzmaßnahmen vorgesehen werden.

// Beschwerdemechanismen und Verbraucherrechte von Kindern und Jugendlichen ausweiten.

Meldungen und Beschwerden von Kindern und Jugendlichen sollten bei der Moderation von Inhalten durch Anbieter sozialer Medien und anderer digitaler Dienste vorrangig behandelt werden. Die Anbieter müssen intensiver

j. Die FAIR-Prinzipien für das Forschungsdatenmanagement wurden erstmals 2016 in einem Artikel in der Zeitschrift *Scientific Data* vorgestellt. Ziel ist es, die Infrastruktur für die Nachnutzung von Forschungsdaten zu verbessern, indem Maschinen und Menschen das Auffinden und Nutzen von Daten erleichtert wird. Siehe: Wilkinson, M.D., et al., [The FAIR Guiding Principles for scientific data management and stewardship](#), *Scientific Data*, 3, 2016.

in die Pflicht genommen werden, damit für Beratungs- und Hilfsangebote und Beschwerdemechanismen ausreichende Mittel zur Verfügung stehen. Diese Mechanismen müssen altersgerecht, benutzerfreundlich, zugänglich und wirksam sein und die Privatsphäre wahren.

// Programme für digitale Bildung und zur Förderung digitaler Kompetenzen für Minderjährige, Eltern und Betreuungspersonen, Lehrkräfte und pädagogische Fachkräfte etablieren.

Digitale Bildung und digitale Kompetenz sollten auf allen Bildungsebenen als zentrale Grundfertigkeit für Minderjährige, Eltern und Lehrkräfte verankert werden. Wohlbefinden im digitalen Raum sollte Teil der digitalen Bildung für alle sein.

Bildung sollte Kinder und Jugendliche in die Lage versetzen, Informationen und Quellen online kritisch zu bewerten und Manipulationstechniken wie z. B. Desinformation, Deepfakes und personalisierte Werbung zu erkennen. Außerdem sollten Minderjährige, Eltern und Lehrkräfte darüber aufgeklärt werden, wie digitale Inhalte erstellt und geteilt werden und wie Algorithmen das Wahrnehmen und Erleben in der Welt der sozialen Medien+ beeinflussen.

Durch strukturierte Bildungsangebote für Sicherheit im Internet sollten praktische Kompetenzen in Bezug auf den Schutz personenbezogener Daten, die Verwaltung von Datenschutzeinstellungen, die Wahrung sicherer digitaler Identitäten und die Ermittlung von Risiken insbesondere in sozialen Medien, bei Nachrichtenübermittlungsdiensten und in Spielumgebungen aufgebaut werden. Diese Kompetenzen sollten laufend ausgebaut werden, ausgehend von einfachen Verhaltensweisen für mehr Sicherheit hin zu einem Verstehen komplexerer Konzepte wie digitaler Fußabdruck, Einwilligungserklärungen und Risiken auf Plattformen. Für ein gesundes Bildschirmverhalten sollten Kinder angeleitet werden, eine ausgewogene Nutzung zu erlernen, ihre Aufmerksamkeit zu regulieren und übermäßiges oder schädliches Nutzungsverhalten zu erkennen.

// Mehr Angebot und geeignete Infrastruktur für Offline-Aktivitäten schaffen.

Die Mitgliedstaaten und die lokalen Behörden sollten das Angebot an erschwinglichen Sport-, Kunst- und Kulturstätten, Jugendclubs, Bibliotheken und Gemeinschaftsräumen erhalten und erweitern und den Zugang dazu erleichtern, um Minderjährige verstärkt für gesunde Offline-Aktivitäten zu gewinnen und attraktive Alternativen zur übermäßigen Bildschirmnutzung zu schaffen. Dafür bedarf es Investitionen in sichere, inklusive und altersgerechte Räume, in denen Minderjährige miteinander in Kontakt treten, lernen, spielen und positive Beziehungen in ihrem Umfeld aufbauen können.

// Gemeinsam Leitfäden für Eltern ausarbeiten.

Gemeinsam mit Elternvereinigungen sollten sich die EU und die Mitgliedstaaten dafür einsetzen, dass Leitfäden für Eltern ausgearbeitet werden. Die Leitfäden würden Eltern und Betreuungspersonen als klare und leicht zugängliche Ratgeber dabei unterstützen, Minderjährige im sicheren, verantwortungsvollen und positiven Umgang mit den sozialen Medien+ zu begleiten. Die Leitfäden sollten praktische Hilfestellungen zu wichtigen Themen wie Sicherheit im Internet und Datenschutz, digitales Wohlbefinden, ethische und verantwortungsvolle Nutzung und Hilfsangeboten bieten.

// Ausreichende öffentliche Finanzierung und gemeinsame Standards für Organisationen der Zivilgesellschaft und Peer-Beratung sichern.

Die EU und die Mitgliedstaaten sollten sicherstellen, dass die Safer-Internet-Zentren und ähnliche Organisationen der Zivilgesellschaft auch künftig mit ausreichenden finanziellen Mitteln ausgestattet werden und dass ihre Arbeit sich nach gemeinsamen, von Fachleuten entwickelten Standards richtet. Nur so können sie weiter Sensibilisierungs-, Schulungs- und Unterstützungsdienste anbieten und ihr Angebot weiterentwickeln. Öffentliche Mittel sind von entscheidender Bedeutung, damit sie weiter unabhängig agieren können und das Angebot kohärent bleibt.

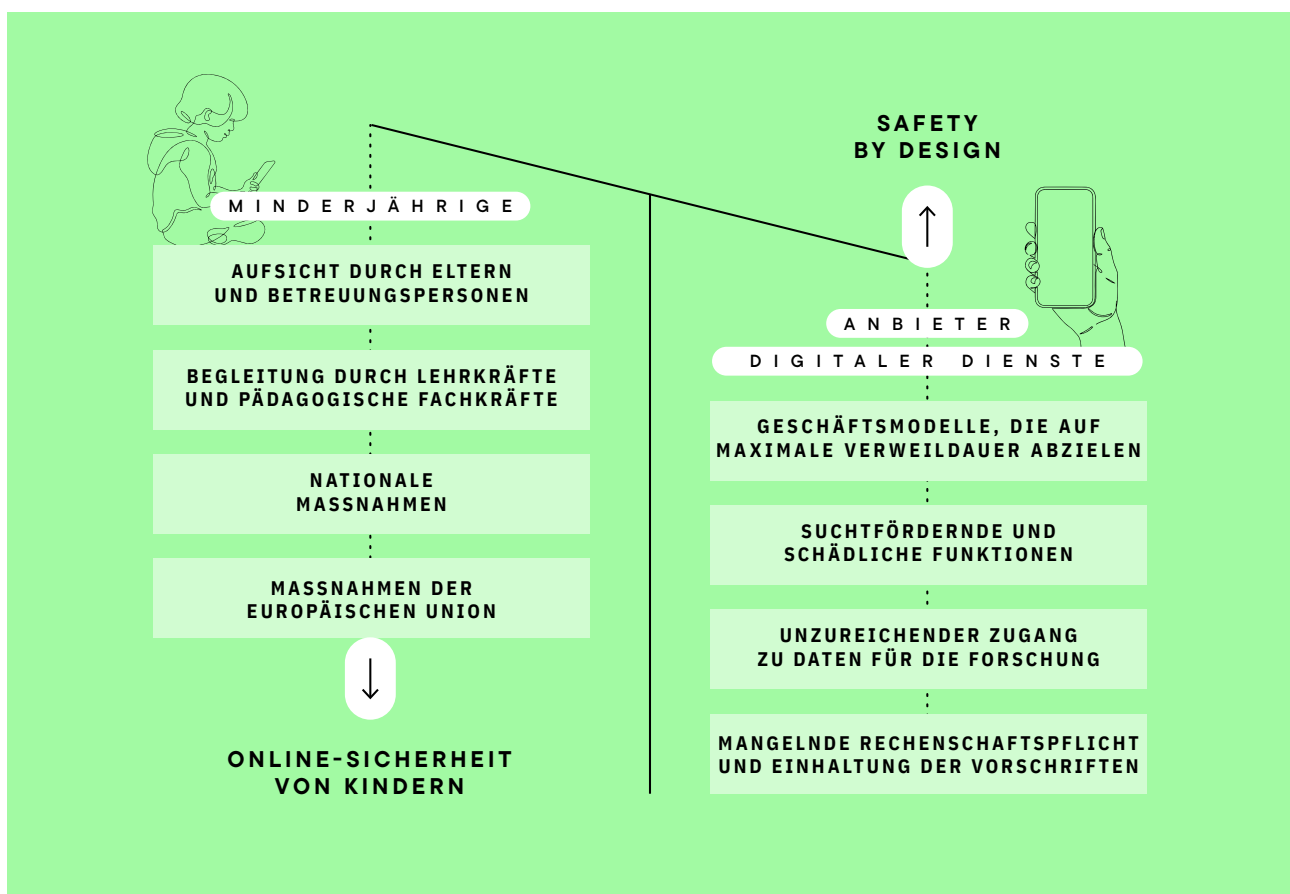
Auch Peer-Beratung, Beratungs- und Hilfsangebote, Bildungsressourcen, Sensibilisierungskampagnen und Maßnahmen für Kapazitätsaufbau sollten von der öffentlichen Hand finanziert werden. Mit weiteren Investitionen sollten die Sichtbarkeit, Zugänglichkeit und Reichweite dieser Einrichtungen – auch für schutzbedürftige Minderjährige – erhöht und Initiativen zur Förderung sichererer Umgebungen in den sozialen Medien+ unterstützt werden.

// Langfristige Finanzierung für groß angelegte europäische Langzeitstudien bereitstellen und randomisierte kontrollierte Studien weiter fördern.

Groß angelegte europäische Langzeitstudien zur Sicherheit von Kindern im Internet könnten sich beispielsweise an der nordamerikanischen Langzeitstudie zur Gehirnentwicklung und Gesundheit von Kindern (Adolescent Brain Cognitive Development (ABCD)-Studie) orientieren. Um bei Fragen der Sicherheit von Kindern im Internet einen entwicklungsorientierten und neurobiologischen Ansatz verfolgen zu können, braucht es umfassende europäische Langzeitdaten (die einen Zeitraum von zehn Jahren oder mehr abdecken). So könnten Lücken in den weitgehend korrelierenden Forschungsergebnissen im europäischen Kontext zu den Auswirkungen der Nutzung sozialer Medien und anderer digitaler Dienste auf die Entwicklung, die körperliche und psychische Gesundheit von Minderjährigen und Gefahren im Internet geschlossen werden.

Auch randomisierte kontrollierte Studien sind wichtige Werkzeuge, um die faktengesicherten Grundlagen für die evidenzbasierte Politik zu stärken. Die Forschungsförderung sollte ausdrücklich entwicklungsorientierte und psychopathologische Ansätze zur Untersuchung der Anfälligkeiten von Minderjährigen für Risiken im Internet unterstützen, wobei auch soziale und individuelle Faktoren in Kindheit und Jugend berücksichtigt werden sollten.

Abbildung 2: Das Ökosystem in die Balance bringen: „Safety by Design“ in sozialen Medien+



- k. Die ABCD-Studie ist die größte Langzeitstudie zur Gehirnentwicklung und Gesundheit von Kindern in den Vereinigten Staaten. Die Studie verfolgt die Verhaltensentwicklungen von mehr als 11 000 Kindern im Alter von 9 bis 10 Jahren von der frühen Jugend bis ins junge Erwachsenenalter. Anhand der gesammelten Daten werden grundlegende Standards für Gehirnentwicklung von Jugendlichen erarbeitet und die Auswirkungen von biologischem und sozialem Geschlecht, Schlaf, körperlicher Aktivität und Bildschirmzeit auf die Entwicklung von Jugendlichen untersucht. Die Ergebnisse werden auch ein besseres Verständnis der Entwicklung psychischer Probleme im Kindes- und Jugendalter und des Zusammenhangs mit Alkohol- und Drogenmissbrauch ermöglichen.

Sicher online

TIPPS FÜR KINDER UND JUGENDLICHE



Kenn deine Rechte – denk dran, du hast das Recht auf Sicherheit und respektvollen Umgang im Internet.



Sei nett zu anderen im Internet – soziale Medien und Spiele sollten für alle eine gute Erfahrung sein. Behandle andere so respektvoll, wie du selbst behandelt werden möchtest.



Denk nach, bevor du postest – Fotos, Videos und Kommentare können für immer im Internet bleiben. Teile jetzt nur Inhalte, bei denen du auch Jahre später kein Problem hast, wenn andere sie sehen.



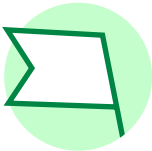
Schütze private Informationen – gib online keine privaten Informationen wie deinen vollständigen Namen, deine Wohnadresse, deine Schule, deine Telefonnummer, deine Passwörter oder deinen Live-Standort weiter.



Denk dran, dass KI ein Hilfsmittel ist und keine echte Person – KI kann Fehler machen und falsche Informationen, gefälschte Bilder, Videos, Stimmen und Nachrichten generieren.



Prüf nach, bevor du vertraust oder teilst – nicht alles im Internet ist wahr. Hinterfrage Informationen, insbesondere verwunderliche Geschichten, Videos oder Nachrichten, und vergewissere dich bei zuverlässigen Quellen, bevor du sie teilst.



Erkenne Gefahren – halte inne und denk nach, wenn du seltsame Anfragen von „Freunden von Freunden“ erhältst, Angebote, die „zu gut, um wahr zu sein“ sind, oder Nachrichten, die dich zu einer Entscheidung drängen.



Nimm keine Bilder oder Chat-Anfragen von Fremden an – wenn du nicht sicher bist, wie alt jemand ist oder wer dich kontaktiert, bitte einen Erwachsenen, zu überprüfen, wer die Person ist (oder sag der Person, „mein Vater/meine Mutter sitzt neben mir“ und schau, wie die Person reagiert).



Aktiviere Datenschutz- und Sicherheitseinstellungen – halte deine Konten privat, verwende sichere Passwörter und aktiviere nach Möglichkeit zusätzliche Sicherheitseinstellungen.



Teile keine intimen Aufnahmen – teile niemals intime Fotos oder Videos, selbst wenn dich jemand unter Druck setzt (vor allem wenn du jünger als 18 Jahre bist). Sind sie einmal geteilt, hast du keine Kontrolle mehr darüber.



Blockiere, melde und sichere Beweise – wenn du im Internet gemobbt, betrogen oder bedroht wirst oder du dich unwohl fühlst, melde und blockiere die Konten und speichere Screenshots oder Nachrichten.



Sprich mit einem Erwachsenen, dem du vertraust, wenn sich etwas falsch anfühlt – es ist nicht albern und du kommst nicht in Schwierigkeiten, wenn du um Hilfe bittest.



Hilf dabei, das Internet sicherer zu machen – lerne, wie Apps, Spiele, Websites, Algorithmen und KI funktionieren, und hilf auch anderen, auf sich aufzupassen.



Werde aktiv – engagiere dich und gestalte die Zukunft der digitalen Welt mit.



Sicher online

TIPPS FÜR ELTERN UND BETREUUNGSPERSONEN



Helfen Sie Ihrem Kind dabei, ein gesundes Bildschirmverhalten zu entwickeln – begrenzen Sie die Bildschirmzeit: gar keine Bildschirmzeit für Kinder im Alter von 0 bis 2 Jahren und altersgerechte Zeitbeschränkungen für Kinder bis ins Alter von 10 bis 12 Jahren; Nutzung unter Ihrer Aufsicht. Ob Beschränkungen der Bildschirmzeit für Jugendliche im Alter von 13 bis 18 Jahren eingeführt werden sollen, damit sie genügend Zeit haben, um zu lernen und Freunde im echten Leben zu treffen, ist noch zu erörtern.



Vergewissern Sie sich, dass Apps und Spiele altersgerecht für Ihr Kind sind.



Jüngere Kinder (bis zu 12 Jahre) sollten **Konsolen und Geräte nur nutzen, wenn eine erwachsene Person anwesend ist.**



Erlauben sie nicht, dass Geräte im Badezimmer, im Schlafzimmer oder während der Mahlzeiten genutzt werden.



Achten Sie auf den Tonfall bei Online-Gesprächen und Videospielen. Geben Sie Acht auf Warnsignale.



Verbringen Sie zusammen Zeit im Internet – bitten Sie Ihr Kind, seine Lieblingsinhalte gemeinsam anzusehen.



Kritisieren Sie nicht, womit sich Ihr Kind beschäftigt – helfen Sie Ihrem Kind, sich ein eigenes Urteil zu bilden (so bekommen Sie auch einen Eindruck davon, welche Inhalte der Algorithmus ihnen vorschlägt).



Ermutigen Sie Ihr Kind dazu, mit Ihnen zu sprechen, wenn es sich wegen etwas im Internet Sorgen macht – versichern Sie ihm, dass Sie ihm helfen werden, es nicht tadeln oder bestrafen und das Gerät nicht wegnehmen werden.



Sprechen Sie weiter über Sicherheit im Internet, wenn Ihr Kind älter wird – auch mit Kindern über 16 und über 18-Jährigen.



Teilen Sie keine Kinderfotos im Internet – Stichwort Sharenting: Denken Sie gut darüber nach, bevor Sie Fotos oder Videos von Ihren Kindern oder Teenagern online teilen. Fremde und KI können diese Informationen auf verschiedenste Arten nutzen.



Gehen Sie mit gutem Beispiel voran – kleben sie nicht an Ihrem Gerät, wenn Ihre Kinder anwesend sind. Geben Sie ihnen die Aufmerksamkeit, die sie verdienen, und verpassen Sie keine wichtigen Momente und Gespräche mit Ihrem Kind.



Liste aller Empfehlungen der Ko-Vorsitzenden nach Kapitel

KAPITEL 1

Ein entwicklungsorientierter Ansatz für die Online-Sicherheit von Kindern

- // Maßnahmen für altersgerechten Schutz von Kindern online erarbeiten und einführen
- // Sichere Online-Räume für Minderjährige gewährleisten
- // Minderjährige und ihr Umfeld stärken
- // (0 bis 2 Jahre) – Betreuungspersonen dafür sensibilisieren, wie wichtig direkte menschliche Interaktion ab der frühen Kindheit für die Entwicklung ist
- // (0 bis 2 Jahre) – Nutzung sozialer Medien und anderer digitaler Dienste vermeiden und für minimale Bildschirmnutzung sorgen, insbesondere bei Kindern unter 3 Jahren
- // (0 bis 2 Jahre) – Verbreitung von Daten von Kindern über Profile in den sozialen Medien begrenzen
- // (3 bis 12 Jahre) – Nutzung nach klaren Regeln unter Aufsicht
- // (3 bis 12 Jahre) – Kindern und ihrem Umfeld hochwertige Bildungsinhalte für den Erwerb digitaler Kompetenzen und für Wohlbefinden bereitstellen
- // (13 bis 18 Jahre) – Zunehmend eigenständige Nutzung für Jugendliche

KAPITEL 2

Forschung zu Risiken, denen Minderjährige online ausgesetzt sind

- // Evidenz-basierte Politik stärken, indem Evidenz in wenig erforschten Bereichen erarbeitet wird
- // Soziale Medien und andere digitale Dienste sollten unabhängige wissenschaftliche Fachleute aktiv in die Gestaltung von Risikominderungsstrategien und -instrumenten einbeziehen
- // Langfristige Finanzierung für groß angelegte europäische Langzeitstudien bereitstellen und randomisierte kontrollierte Studien weiter fördern
- // In eine geschützte, gemeinsame europäische Forschungsinfrastruktur investieren, um sicheren Zugang zu den Daten von Minderjährigen zu ermöglichen
- // Vorschriften über den Zugang der Forschung zu Daten und über die Kontrolle stärker durchsetzen

KAPITEL 3

Minderjährige in der sich rasch wandelnden Welt der sozialen Medien+ schützen

- // Eine harmonisierte EU-weite Zugangsbeschränkung zu sozialen Medien und anderen digitalen Diensten für Kinder unter 13 Jahren vorschlagen
- // Funktionierende Systeme zur Altersfeststellung einführen, damit auf "safety by design" beruhende und altersgerechte Systeme zum Schutz und zur Stärkung Minderjähriger online ihre Wirkung entfalten können
- // Vorschriften für zentrale Sicherheitsfunktionen bei der Gestaltung sozialer Medien und anderer digitaler Dienste erweitern und harmonisieren

- // Beweislast, dass Produkte und Dienste für Minderjährige sicher sind, auf Anbieter sozialer Medien und anderer digitaler Dienste verlagern
- // Durchsetzungs- und Evaluierungskapazitäten stärken
- // Rasche Maßnahmen ergreifen, um sicherzustellen, dass für Anbieter sozialer Medien und anderer digitaler Dienste klare Verpflichtungen gelten, sexuellen Missbrauch von Kindern im Internet, auch im Rahmen interpersoneller Kommunikation, zu verhindern, aufzudecken, zu melden und zu stoppen
- // Mitgliedstaaten können zusätzliche vorsorgliche Zugangsbeschränkungen für soziale Medien und andere digitale Dienste für Kinder ab 13 Jahren einführen
- // Verbraucherschutzvorgaben zum Schutz Minderjähriger im Internet nachschärfen
- // Auswirkungen der umgesetzten Maßnahmen laufend beobachten und bewerten
- // Bei der Verarbeitung von Daten von Kindern im Rahmen der DSGVO durch Anbieter sozialer Medien und anderer digitaler Dienste sollte das Wohl der Kinder an erster Stelle stehen
- // Wirksame Umsetzung der Produkthaftungsrichtlinie sicherstellen
- // Programme für digitale Bildung und zur Förderung digitaler Kompetenzen für Minderjährige, Eltern und Betreuungspersonen, Lehrkräfte und pädagogische Fachkräfte etablieren
- // Mehr Angebot und geeignete Infrastruktur für Offline-Aktivitäten schaffen
- // Gemeinsam Leitfäden für Eltern ausarbeiten
- // Eltern und Betreuungspersonen mit den modernsten Hilfsmitteln für Kontrolle und Aufsicht unterstützen, die laufend an den neuesten Stand der Technik angepasst werden
- // Ausreichende öffentliche Finanzierung und gemeinsame Standards für Organisationen der Zivilgesellschaft und Peer-Beratung sichern
- // Das Gesundheitssystem in die Lage versetzen, Suchterkrankungen und andere psychische Erkrankungen im Zusammenhang mit der Nutzung sozialer Medien und anderer digitaler Dienste zu diagnostizieren und zu behandeln
- // Aus- und Weiterbildung von Lehrkräften im Bereich digitaler Kompetenzen und Medienkompetenz fördern und Eltern einbeziehen
- // KI-Kompetenz als integralen Bestandteil der digitalen Bildung aufnehmen
- // Schulen sollten strukturierte Möglichkeiten zur Verbesserung der psychischen Gesundheit und des digitalen Wohlbefindens anbieten
- // Bei bildungspolitischen Maßnahmen besonderes Augenmerk auf schutzbedürftige Gruppen legen
- // In eine sichere, präventive, robuste und vertrauenswürdige digitale Bildungsinfrastruktur investieren

KAPITEL 4

Minderjährige befähigen, sich sicher in der digitalen Welt zu bewegen

- // Minderjährigen mehr Möglichkeiten bieten, die Welt der sozialen Medien+ in einem geschützten Rahmen aktiv mitzugestalten
- // Beschwerdemechanismen und Verbraucherrechte von Kindern und Jugendlichen ausweiten
- // Aufbau und Nutzung von sozialen Medien und anderen digitalen Diensten, die auf den Werten der EU aufbauen, und wo Minderjährige sicher miteinander in Kontakt treten können, finanzieren und bewerben

01

Ein entwicklungsorientierter Ansatz für die Online-Sicherheit von Kindern

Kindheit als eigenständige, geschützte Lebensphase

Aus entwicklungsgeschichtlicher Perspektive wird die Kindheit erst seit vergleichsweise kurzer Zeit als eigenständige Lebensphase anerkannt. Lange Zeit wurde davon ausgegangen, dass sich Kinder nicht grundlegend von Erwachsenen unterscheiden.

In vormodernen und frühindustriellen Gesellschaften war diese Auffassung eng mit den materiellen Bedingungen verknüpft, insbesondere mit der „wirtschaftlichen Notwendigkeit“ der Kinderarbeit. Kinder galten als „kleine Erwachsene“⁰¹, was ihren spezifischen Bedürfnissen und ihrer Schutzbedürftigkeit nicht gerecht wurde und die Entwicklung günstiger Rahmenbedingungen für den Schutz von Kindern behinderte.

Das Aufkommen moderner Wissenschaftsdisziplinen wie der Entwicklungsmedizin und der Psychologie leitete einen Paradigmenwechsel ein. So wurde deutlich, dass die kognitive, emotionale und soziale Entwicklung von Kindern spezifischen Entwicklungsverläufen folgt. Diese Fortschritte trugen dazu bei, die Kindheit als eigenständige, durch eine besondere Schutzbedürftigkeit gekennzeichnete Lebensphase⁰² neu zu definieren.

Untermauert wurde dieser Ansatz durch Erkenntnisse aus der Kinder- und Jugendpsychiatrie, die die langfristigen Folgen negativer Erfahrungen in frühen Lebensphasen verdeutlichten. Die Auffassung, Kindheit und Jugend als eigenständige Lebensphasen anzuerkennen, in denen ein besonderer Schutz- und Unterstützungsbedarf⁰³ besteht, setzte sich allmählich durch.

Die kindliche Entwicklung verläuft in Phasen

Durch diese Wissensentwicklung wurden im Laufe des 20. Jahrhunderts die Grundlagen für moderne Rahmenbedingungen im Bereich des Kinder- und Jugendschutzes geschaffen. Schwerpunkt dieser Rahmenbedingungen war zunächst der Schutz von Kindern in der physischen Welt.

Ein wichtiges Beispiel hierfür ist das Übereinkommen der Vereinten Nationen über die Rechte des Kindes. Gemäß diesem Übereinkommen werden Kinder unter 18 Jahren^a als homogene Gruppe behandelt.

Digitale Technologien und Dienste, darunter soziale Medien, haben sich in rasantem Tempo entwickelt und das Leben der Kinder verändert. Dennoch beruhen viele Ansätze zum Schutz von Kindern nach wie vor implizit – oder auch explizit – auf der Vorstellung, „Kinder“ seien eine homogene Gruppe.

Diese Annahme ist irreführend. Entwicklungswissenschaftlich ist belegt, dass sich die Entwicklung von Kindern in qualitativ unterschiedlichen Phasen vollzieht, die jeweils durch einzigartige kognitive, emotionale und soziale Fähigkeiten gekennzeichnet sind. Diese Fähigkeiten prägen die Wahrnehmung, die Interaktion und die Kommunikation von Kindern in ihrem Umfeld, darunter auch online.

Die Notwendigkeit eines altersgerechten Schutzes

Die Exposition von Kindern gegenüber der Welt der sozialen Medien⁺ beginnt früh im Leben und nimmt im Laufe der Kindheit in Bezug auf Intensität, Komplexität und Personalisierung stetig zu⁰⁴. Eine Studie zeigt, dass Kinder unter zwei Jahren täglich durchschnittlich 49 Minuten Bildschirmzeit ausgesetzt sind. Bis zum achten Lebensjahr hat sich diese Zahl mehr als verdreifacht und liegt bei rund drei Stunden pro Tag⁰⁵. Digitale Technologien haben nachweislich eine tiefgreifende, strukturierende Wirkung auf die Entwicklung von Kindern und sind Teil des komplexen Umfelds, in dem Kinder und Jugendliche lernen, ein Selbstverständnis zu entwickeln und Beziehungen zu anderen aufzubauen.

Vereinfacht ausgedrückt, beeinflusst die Entwicklung der Kinder ihre Online-Interaktionen, wird aber auch durch diese Interaktionen beeinflusst. Die digitale Welt als solche kann nicht getrennt von der kindlichen Entwicklung betrachtet werden, sondern ist vielmehr ein wesentlicher Bestandteil dieser Entwicklung, insbesondere in späteren Phasen⁰⁶. Diese wechselseitige Beziehung unterstreicht die Notwendigkeit altersgerechter Maßnahmen, um Kinder zu schützen und sie in die Lage zu versetzen, sich online sicher und selbstbewusst zurechtzufinden.

„Der Schutz von Kindern kann dann als entwicklungsgerecht bezeichnet werden, wenn er der Tatsache Rechnung trägt, dass die kognitive Kontrolle, die emotionale Regulierung und das Risikobewusstsein von Kindern einem Reifeprozess unterliegen.“

— PROF. DR. EVA MÖHLER

DIREKTORIN DER KLINIK FÜR
KINDER- UND JUGENDPSYCHIATRIE,
UNIVERSITÄTSKLINIKUM DES SAARLANDES

^{a.} Im Sinne dieses Übereinkommens ist ein Kind definiert als „jeder Mensch, der das achtzehnte Lebensjahr noch nicht vollendet hat“, soweit die Volljährigkeit nach dem auf das Kind anzuwendenden Recht nicht früher eintritt. Siehe Vereinte Nationen (1989), Übereinkommen über die Rechte des Kindes, Teil 1 Artikel 1.

Die größten Herausforderungen im Zusammenhang mit einem altersgerechten Schutz

DIE TENDENZ, „KINDER“ ALS EINE EINHEITLICHE GRUPPE

ZU BETRACHTEN

Die bestehenden Ansätze in Bezug auf die Sicherheit von Kindern im Internet beruhen häufig auf der Annahme, dass Kinder eine einheitliche Gruppe mit einheitlichen Bedürfnissen bilden. Diese Annahme muss revidiert werden. Heute wird davon ausgegangen, dass die kindliche Entwicklung in Phasen erfolgt, die bestimmen, wie Kinder (zwischen 0 und 12 Jahren) und Jugendliche (zwischen 13 und 18 Jahren) mit der Online-Welt interagieren und in welchem Maße sie gegenüber unterschiedlichen Risiken schutzbedürftig sind.

Soziale Faktoren, Geschlecht und Sexualität, sozioökonomischer Hintergrund, ethnische Herkunft, Religion, Migrationshintergrund und sonderpädagogische Bedürfnisse haben ebenfalls erhebliche Auswirkungen auf die Interaktionen und die Schutzbedürftigkeit von Kindern und Jugendlichen im Internet⁰⁷.

DAS MISSVERHÄLTNIS ZWISCHEN DEN FÄHIGKEITEN

MINDERJÄHRIGER UND DEN SOZIALEN MEDIEN+

Digitale Dienste, darunter auch soziale Medien, basieren auf hochoptimierten Interaktionsarchitekturen mit algorithmischen Empfehlungssystemen, die praktisch unendliches Scrollen ermöglichen und einen schnellen, konstanten Informationsfluss liefern. Diese Funktionen sind bewusst so konzipiert, dass sie die Aufmerksamkeit der Nutzer maximieren⁰⁸.

Die Fähigkeiten von Kindern und Jugendlichen entwickeln sich hingegen schrittweise und bleiben bis weit ins Jugendalter hinein unvollständig ausgereift⁰⁹. Folglich sind Minderjährige zunehmend dem Umfeld und Inhalten sozialer Medien+ ausgesetzt, denen sie nicht gewachsen sind und die ihnen schweren Schaden zufügen können.

DIE SICH ENTWICKELNDE AUTONOMIE MINDERJÄHRIGER

ALS INTERNETNUTZER

Wie bereits erwähnt und in den folgenden Abschnitten ausführlicher untersucht, beeinflussen die sich im Altersverlauf entwickelnden Fähigkeiten von Kindern und Jugendlichen das Vermögen, online sicher und selbstbewusst zu agieren.

Kleinkinder sind noch vollständig von Eltern und Betreuungspersonen abhängig. Mit zunehmendem Alter entwickeln sie schrittweise mehr Autonomie, bis sie schließlich als Erwachsene weitgehend selbstständig handeln können. Die Gestaltung sozialer Medien und anderer digitaler Dienste hat einen zunehmenden Einfluss auf die Entwicklung Minderjähriger. Je älter und unabhängiger Kinder werden, desto weniger sind die sie unterstützenden Netzwerke (Eltern und Betreuungspersonen, Lehrkräfte und Erzieher) in der Lage, Minderjährige online zu schützen, zu beaufsichtigen und anzuleiten.

EMPFEHLUNGEN

Maßnahmen für altersgerechten Schutz von Kindern im Internet erarbeiten und einführen

Die Maßnahmen zum Schutz von Kindern und Jugendlichen müssen so gestaltet und umgesetzt werden, dass sie den sich entwickelnden Fähigkeiten Heranwachsender, aber auch den Risiken, denen sie in verschiedenen Altersgruppen ausgesetzt sind, Rechnung tragen. Dabei sollten die persönlichen und sozialen Umstände Minderjähriger nach Möglichkeit berücksichtigt werden.

Sichere Online-Räume für Minderjährige gewährleisten

Die Anbieter sozialer Medien und anderer digitaler Dienste tragen die Hauptverantwortung dafür, dass ihre Dienste für alle Kinder und Jugendlichen sicher sind. Dies schließt eine sichere Gestaltung dieser Angebote ein. Die Anbieter müssen die Hauptverantwortung dafür übernehmen, dass der Zugang zu ihren Diensten und deren Nutzung für Minderjährige sicher sind.

Minderjährige und ihr Umfeld stärken

Damit die durchgeführten Maßnahmen zum Schutz und zur Stärkung von Kindern und Jugendlichen im Internet wirksam sind, müssen sie den sich wandelnden Bedürfnissen und Fähigkeiten der Zielgruppe Rechnung tragen. Sie müssen zudem geeignet sein, die sich wandelnde Rolle von Eltern und Betreuungspersonen, Lehrkräften und Erziehern (das Umfeld der Kinder) beim Schutz Minderjähriger zu unterstützen; zudem müssen sie eine Überwachung und Steuerung der Nutzung sozialer Medien und anderer digitaler Dienste durch sie während ihrer gesamten Entwicklung ermöglichen.

Altersspezifische Herausforderungen

Im vorhergehenden Abschnitt wurde auf drei der größten Herausforderungen bei der Gestaltung und Umsetzung eines entwicklungsorientierten Ansatzes für die Sicherheit von Kindern im Internet sowie entsprechende Empfehlungen eingegangen.

Darauf aufbauend werden in den folgenden Abschnitten die verschiedenen Merkmale und Anfälligkeiten untersucht, die die Entwicklung von Minderjährigen in drei Hauptentwicklungsphasen bestimmen: 0-2 Jahre (frühe Kindheit), 3-12 Jahre (Kindheit) und 13-18 Jahre (Jugend).

Diese primären Phasen umfassen sowohl die sich entwickelnden Fähigkeiten Minderjähriger als auch die sich verändernde Rolle des Umfelds beim Schutz und bei der Stärkung von Kindern und Jugendlichen online:

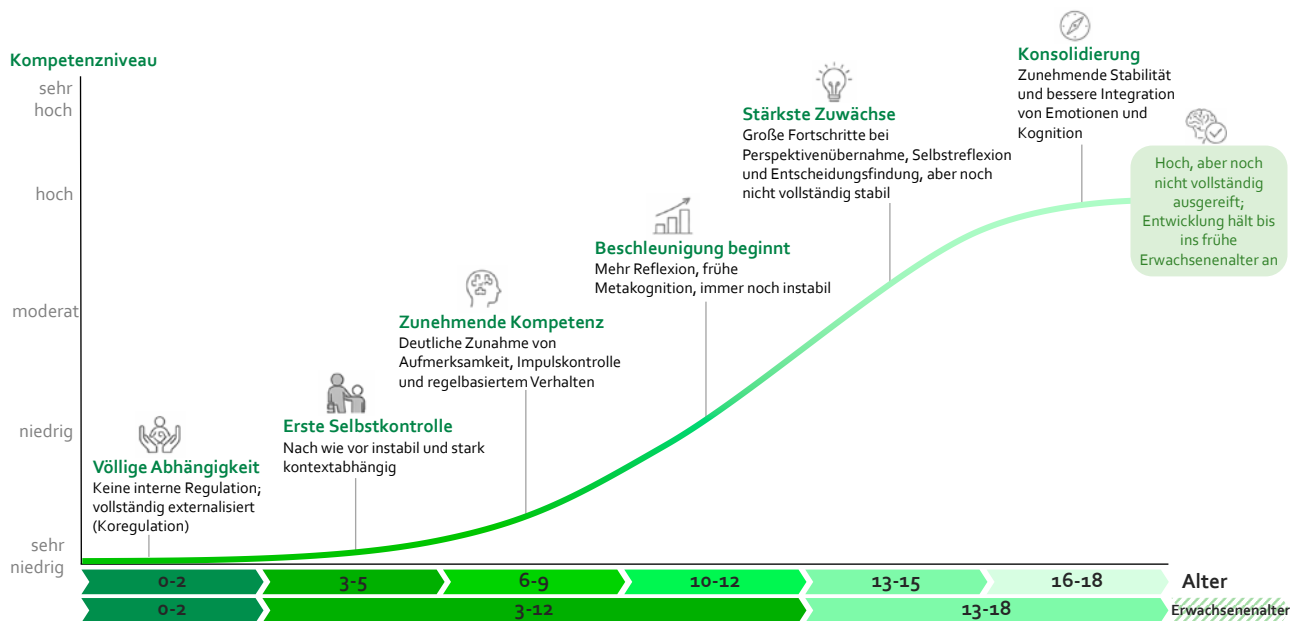
// **0-2 Jahre:** frühe Kindheit als besonders geschützte Entwicklungsphase,

// **3-12 Jahre:** Kindheit als beaufsichtigte Entwicklungsphase,

// **13-18 Jahre:** Jugend als Phase der sich entwickelnden Autonomie.

Abbildung 1 – Die in Phasen ablaufende Entwicklung von Kernkompetenzen

Selbstregulation, Urteilsvermögen und kritisches Denken



In diesem Bericht wird untersucht, welchen Risiken Minderjährige online ausgesetzt sind, und es werden Empfehlungen zur Bewältigung dieser Risiken entsprechend diesen drei Hauptentwicklungsphasen gegeben, die für die Zwecke dieser Analyse als frühe Kindheit, Kindheit und Jugend definiert sind.

In diesem ersten Kapitel wird das erste von Sechs Leitprinzipien vorgestellt, die von den Autoren vorgeschlagen wurden, um Maßnahmen zum Schutz und zur Stärkung von Kindern und Jugendlichen in der digitalen Welt zu steuern: die Notwendigkeit eines entwicklungsorientierten Ansatzes in Bezug auf die Sicherheit von Kindern im Internet.

„Alle Personen unter 18 Jahren haben einen besonderen Anspruch auf Schutz und das Erleben altersgerechter Erfahrungen.“

– MIE OEHLenschLAGER,
UNABHÄNGIGE FORSCHERIN IN DEN
BEREICHEN KI, ETHIK UND POLITIK

Im Interesse einer umfassenden Untersuchung der Merkmale und der besonderen Anfälligkeiten von Minderjährigen in verschiedenen Phasen ihrer Entwicklung werden die primären Entwicklungsphasen in sekundäre Phasen unterteilt (0-2 Jahre, 3-5 Jahre, 6-9 Jahre, 10-12 Jahre, 13-15 Jahre und 16-18 Jahre), auf die in diesem Kapitel ausführlicher eingegangen wird.

Einige der für die einzelnen primären Phasen vorgelegten Empfehlungen beziehen sich nicht ausschließlich auf die Phase, unter der sie vermittelt werden, sondern gelten für die jeweils angegebenen Phasen.

0-2 Jahre: Frühe Kindheit als besonders geschützte Entwicklungsphase

Die frühe Kindheit, insbesondere das Alter von 0 bis 2 Jahren, ist eine Phase maximaler Abhängigkeit und für die Entwicklung von grundlegender Bedeutung. In dieser Zeit werden die Grundlagen für emotionale Sicherheit, soziale Bindung, Spracherwerb und Selbstregulation geschaffen.

Kernprozesse wie die Bildung emotionaler Bindungen, die Koregulierung und die Unterscheidung zwischen der eigenen Persönlichkeit des Kindes und seinem Umfeld entwickeln sich durch wiederholte Interaktionen mit ansprechbaren Betreuungspersonen. Eine Selbstregulation ist intern noch nicht ausgeprägt, sondern entwickelt sich schrittweise durch Koregulierung.

In diesem Sinne bildet eine frühzeitige Koregulierung auch die Entwicklungsgrundlage für spätere Autonomie und Selbstbestimmung. Die allmähliche Verinnerlichung von Emotionsregulation, Kommunikation und sozialer Interaktion erfolgt durch wiederholte Beziehungserfahrungen und nicht durch isolierte Exposition gegenüber digitalen Reizen.

Die Entwicklung in dieser Phase ist grundlegend relational. Die Fähigkeit zu Selbstregulation, emotionale Stabilität und frühe kognitive Strukturen werden durch externes Scaffolding (Unterstützungsstrukturen) unterstützt, bevor sie internalisiert werden.

ALTERSSPEZIFISCHE HERAUSFORDERUNGEN

Die Notwendigkeit einer direkten menschlichen Interaktion

Eine zentrale Herausforderung in dieser Phase besteht darin, sicherzustellen, dass die Kleinkinder ausreichend direkte menschliche Interaktion erhalten. Eine mangelhafte Interaktionsqualität kann sich auf spätere Bindungsprozesse auswirken, die frühe Sprachentwicklung und die grundlegenden Kommunikationsfähigkeiten beeinträchtigen und folglich unmittelbare Auswirkungen auf die gesamte weitere Entwicklung des Kindes haben.

Die Verfügbarkeit einer kohärenten, emotional abgestimmten Interaktion ist eine Grundvoraussetzung für eine sichere Entwicklung in einem zunehmend digitalisierten Umfeld. In dieser Phase sind Kleinkinder fast vollständig auf externe Regulierung angewiesen.

An der Stressregulation, der Erregungsmodulation und Schlaf-Wach-Zyklen beteiligte neurophysiologische Systeme sind noch nicht ausgereift und sehr empfindlich gegenüber Umwelteinflüssen. Dies erhöht die Anfälligkeit für Überstimulation und Störungen der Schlaf- und Stressregulierung.

Das Lernen in dieser Phase ist eher interaktions- als inhaltsbasiert. Kleine Kinder erfassen Bedeutungsinhalte durch wechselseitige körperliche Interaktion mit Eltern und Betreuungspersonen, nicht durch passive Exposition gegenüber bildschirmbasierten Darstellungen.

Frühzeitiger Spracherwerb und Kommunikationsentwicklung hängen grundlegend von wiederholter Interaktion mit Eltern und Betreuungspersonen ab. Responsives verbales Engagement, geteilte Aufmerksamkeit und emotional abgestimmte Kommunikation sind wesentliche Entwicklungsbedingungen in dieser Phase.

Risiken der Bildschirmexposition

In diesem Alter wird eine erhöhte Bildschirmexposition nachweislich mit einer kürzeren Schlafdauer, dysregulierten Stressreaktionen und einem geringeren Maß an Interaktion zwischen einer Bezugsperson und dem Kind sowie sprachlichem Input in Verbindung gebracht¹⁰. Diese Anfälligkeiten können in eine biologische, psychologische und entwicklungsbezogene Dimension unterteilt werden.

In biologischer Hinsicht sind Kleinkinder aufgrund ihrer noch nicht ausgereiften Selbstregulationssysteme sehr anfällig für Überstimulation¹¹. Die psychologische Entwicklung hängt von einer konsistenten, responsiven Interaktion ab, weshalb Kleinkinder auf Störungen in der Aufmerksamkeit und Kommunikation besonders empfindlich reagieren. Entwicklungsrisiken bestehen im Zusammenhang mit der Bindungsentwicklung und der Entwicklung der Selbstregulation.

In dieser Phase wird eine höhere Bildschirmexposition mit sozioemotionalen Schwierigkeiten, Verhaltensproblemen und Verzögerungen bei der Entwicklung der Selbstregulation¹² in Verbindung gebracht. Diese Zusammenhänge sind häufig wechselseitig, da bei Kleinkindern mit Schwierigkeiten bei der Selbstregulation auch eine stärkere Neigung zum Konsum von Bildschirminhalten bestehen kann.

Von Betreuungspersonen vermittelte digitale Exposition

Im Alter zwischen 0 und 2 Jahren wird die Exposition gegenüber sozialen Medien+ vollständig durch Betreuungspersonen vermittelt. Kleinkinder haben grundsätzlich keine Kontrolle über Zugang, Dauer und Inhalte. Die Nutzung sozialer Medien und anderer digitaler Dienste wird hauptsächlich durch die Praktiken, Routinen und situationsbezogenen Bedürfnisse von Eltern und Betreuungspersonen, beispielsweise Beruhigung oder Ablenkung, geprägt¹³.

In der frühen Kindheit ergeben sich digitale Risiken theoretisch weniger aus der direkten Interaktion mit Inhalten, sondern vielmehr aus der Art und Weise, mit der soziale Medien und andere digitale Dienste das Betreuungsumfeld umstrukturieren. Ein zentraler Begriff ist „Technoferenz“^b. In diesem Alter können selbst kurze Verschiebungen in der Aufmerksamkeit der Betreuungsperson die Responsivität, die geteilte Aufmerksamkeit und die sprachliche Interaktion verringern¹⁴.

Der gemeinsame Konsum von Bildschirminhalten durch Betreuungspersonen und Kleinkinder wird mit weniger günstigen Entwicklungsergebnissen in Verbindung gebracht. Dies ist nicht in erster Linie auf den Inhalt zurückzuführen, sondern auf die Veränderung der Eltern-Kind-Interaktion¹⁵. Somit ist das digitale Risiko in der frühen Kindheit oft relational, ehe es individuell wird.

Untersuchungen zur Beeinflussung von Familien durch Werbespots zeigen, dass Kleinkinder zunehmend zu Objekten von Visibilität, Monetarisierung und Datenextraktion werden können, lange bevor sie in der Lage sind, diese Prozesse selbst zu verstehen oder zu beeinflussen. Dies verstärkt die Notwendigkeit starker externer Schutzrahmen in der frühen Kindheit.

b. „Technoferenz“ ist definiert als Unterbrechung der Interaktionen zwischen Eltern und Kindern durch Technik. Siehe Zhang et al. (2025), [Parental Technoference and Child Problematic Media Use: Meta-Analysis](#).

Die Digitalisierung der frühen Kindheit

Eine sich neu entwickelnde und zunehmend relevante Dimension betrifft eine über die traditionellen bildschirmbasierten Interaktionen hinausgehende Digitalisierung frühkindlicher Lebenswelten. Immer mehr Spielzeuge, darunter Puppen und interaktive Spielobjekte, werden um digitale Funktionen und zunehmend auch künstliche Intelligenz (KI) erweitert.

Diese Entwicklung eines Umfelds der sozialen Medien+ ist besonders wichtig, da KI-gestütztes Spielzeug und sprachbasierte Geräte Kindern nicht nur als Objekte, sondern als responsive soziale Interaktionspartner erscheinen können. In der frühen Kindheit hängen Bindung, Koregulierung, Spracherwerb und symbolisches Spiel von regelmäßiger zwischenmenschlicher Interaktion ab.

Diese Systeme geben Anlass zu besonderen entwicklungsbezogenen Bedenken. KI-gestütztes Spielzeug und sprachbasierte Geräte können Responsivität simulieren, ohne die echte Wechselseitigkeit, emotionale Anpassung oder relationale Verantwortlichkeit zu bieten, die zwischenmenschliche Beziehungen kennzeichnen.

KI-gestütztes Spielzeug enthält häufig auch Mikrofone, Kameras sowie Funktionen zur Sprachverarbeitung oder appbasierten Personalisierung. Dies birgt Risiken für die Privatsphäre und den Datenschutz in einem Alter, in dem Kinder nicht in der Lage sind, Datenverarbeitung zu verstehen, in sie einzuwilligen oder sie anzufechten.

Verlagerung der direkten menschlichen Interaktion

Die Interaktionen von Kindern mit der digitalen Welt geben Anlass zu Bedenken hinsichtlich einer möglichen Verdrängung oder Beeinträchtigung interaktioneller Lernprozesse sowie neuer Formen von Abhängigkeit und Überstimulation. Diese Abhängigkeiten werden innerhalb der bestehenden Forschungs- oder Regulierungsrahmen noch nicht ausreichend berücksichtigt.

Die Nutzung sozialer Medien und anderer digitaler Dienste durch Eltern und Betreuungspersonen kann die Zeit verringern, die für die persönliche Interaktion mit Kindern, das freie Spiel, körperliche Aktivität und Schlaf – ausnahmslos Faktoren, die für eine frühzeitige Entwicklung von wesentlicher Bedeutung sind – aufgewendet wird¹⁶. In ihren schwerwiegendsten Formen kann die Verlagerung von Interaktionen zwischen Betreuungs- und Pflegepersonen einer „digitalen Vernachlässigung“ gleichkommen⁹.

Probleme im Zusammenhang mit der Verlagerung persönlicher Interaktionen zwischen Betreuungspersonen und Kindern gehen über die unmittelbare Überstimulation oder Ablenkung hinaus und wirken sich potenziell langfristig auf die Autonomieentwicklung, das kreative Spielen, die Kommunikation und die Entwicklung zunehmend selbstgesteuerter sozialer und emotionaler Fähigkeiten aus.

- c. Aufbauend auf etablierten Formen emotionaler und betreuungsbezogener Vernachlässigung (Dubowitz et al., 1993; Hildyard & Wolfe, 2002) dehnt der Begriff der digitalen Vernachlässigung diese Konstrukte auf digitale Umgebungen aus. Wenn Eltern in Anwesenheit ihrer Kinder extensiv Bildschirmhalte konsumieren, verringern sich die Interaktionen und die elterliche Ansprechbarkeit. Dies kann die Sprachentwicklung der Kinder beeinträchtigen. Diese Verlagerung der Interaktionen kann bei Kindern auch Gefühle der Ablehnung und emotionalen Distanz hervorrufen und ihr Risiko der Entwicklung von Depressionen, Angst und Aggression erhöhen.

Ein sehr restriktiver Ansatz in Bezug auf die Exposition gegenüber digitalen Inhalten

Trotz dieser Herausforderungen sind nicht alle Formen der Nutzung sozialer Medien und anderer digitaler Dienste in der frühen Kindheit von Natur aus schädlich. Unter bestimmten Bedingungen – insbesondere, wenn Eltern und Betreuungspersonen sicherstellen, dass die Inhalte altersgerecht (geringe Reizintensität, langsame Darstellung usw.) und in eine aktive Medienbegleitung durch Betreuungspersonen eingebettet sind – können Angebote sozialer Medien+ Aspekte des frühen Lernens unterstützen.

Es hat sich gezeigt, dass der ergänzende Einsatz sozialer Medien und anderer digitaler Dienste (Ko-Nutzung) das Lernen erleichtern kann, insbesondere wenn er mit verbaler Interaktion und Scaffolding einhergeht¹⁷. Diese Effekte scheinen jedoch begrenzt und kontextabhängig zu sein.

Die Aufrechterhaltung der zwischenmenschlichen Interaktion mit Kleinkindern ist nicht nur präventiv von Bedeutung, sondern auch, um eine gesunde sozioemotionale, sprachliche und kognitive Entwicklung zu ermöglichen. Sichere Bindung, responsive Kommunikation und Vorbildverhalten der Betreuungsperson sind zentrale Schutzfaktoren im zunehmend digitalisierten Umfeld der frühen Kindheit.

Insgesamt unterstützen diese Ergebnisse einen sehr restriktiven Ansatz in Bezug auf die Nutzung sozialer Medien und anderer digitaler Dienste in der frühen Kindheit. Ein solcher steht auch mit den Leitlinien bedeutender pädiatrischer Fachorganisationen im Einklang¹⁸. Zwar werden solche Empfehlungen möglicherweise nicht allgemein befolgt, doch bieten sie wichtige normative Leitlinien, die auf die Entwicklungsbedürfnisse dieser Altersgruppe abgestimmt sind.

Durch die Betreuungsperson vorgegebene Online-Interaktionen

In der frühen Kindheit muss die Sicherheit von Kindern im Internet grundsätzlich durch die Betreuungsperson gewährleistet werden. Da Kleinkinder keine autonomen Nutzer sind, liegt die Verantwortung für ihre Exposition gegenüber digitalen Umgebungen in erster Linie bei den Eltern und Betreuungspersonen.

Die Kapazitäten der elterlichen Medienbegleitung sind sehr unterschiedlich ausgeprägt. Der sozioökonomische Status, die psychische Gesundheit der Eltern und die Nutzung sozialer Medien+ durch die Eltern selbst haben erheblichen Einfluss auf die Expositionsmuster der Kinder [wie in Kapitel 2 ausführlicher erörtert]. Eine höhere Belastung der Eltern und ein stärkerer Konsum von Bildschirmhalten durch sie gehen mit einer längeren und weniger strukturierten Nutzung digitaler Dienste bei sehr kleinen Kindern einher¹⁹. Daher wird von einer Nutzung von Bildschirmhalten in dieser Altersgruppe dringend abgeraten.

SCHLUSSFOLGERUNGEN

Bei der Gewährleistung der Sicherheit im Internet in der frühen Kindheit geht es nicht in erster Linie um die Regulierung des Verhaltens von Kleinkindern, sondern um die Strukturierung von Betreuungsumgebungen und Interaktionskontexten. Der Schutz hängt davon ab, dass die notwendigen Voraussetzungen für Bindung, Koregulierung und die Entwicklung der Selbstregulation erhalten bleiben. Diese Bedingungen bilden die Grundlage für spätere Entwicklungsphasen.

Erkenntnisse aus etablierten Altersklassifizierungssystemen (z. B. Altersfreigaben für Filme und Spiele) können Orientierung bieten. Inhalte, die für diese Altersgruppe entwickelt werden, sollten strikt auf reizarme, langsam getaktete und nicht narrativ gestaltete Formate beschränkt sein, die Interaktionen mit Betreuungspersonen unterstützen. Dazu gehören einfache visuelle oder akustische Reize, die in Ko-Nutzungskontexte eingebettet sind.

Schnell getaktete, stark stimulierende oder emotional erregende Inhalte – einschließlich rascher Szenenwechsel, intensiver audiovisueller Effekte oder emotional aufgeladener Narrative – sollten für diese Entwicklungsphase als unangemessen angesehen werden. Die Exposition gegenüber gewalthaltigen, beängstigenden oder komplexen narrativen Inhalten ist in diesem Alter eindeutig ungeeignet.

EMPFEHLUNGEN (0 BIS 2 JAHRE)

Betreuungspersonen dafür sensibilisieren, wie wichtig direkte menschliche Interaktion ab der frühen Kindheit für die Entwicklung ist

Eltern und Betreuungspersonen sollten durch Aufklärungskampagnen und Unterstützungsprogramme mit näheren Informationen zur Bedeutung der frühen Kindheit für die Entwicklung von Kindern gestärkt werden. Betreuungspersonen sollten über die für Kleinkinder im Zusammenhang mit „Technoferenz“ bestehenden Risiken, beispielsweise aufgrund der Nutzung sozialer Medien und anderer digitaler Dienste durch diese Personen selbst, informiert werden. Betreuungspersonen sollten ermutigt werden, darüber nachzudenken, welche direkten und indirekten Auswirkungen ihre eigenen Online-Interaktionen auf Minderjährige aller Altersgruppen, insbesondere Kleinkinder, haben.

Die Risiken der „digitalen Vernachlässigung“ sollten im Rahmen des Kinderschutzes anerkannt werden. Eltern, Schulen und Sozialdienste sollten darüber informiert werden, wie sie ab der frühen Kindheit bei Kindern und Jugendlichen Anzeichen für digitale Vernachlässigung erkennen können.

Konsum von Bildschirmangeboten und sozialen Medien+ durch Kinder unter drei Jahren vermeiden

In den ersten 1 000 Lebenstagen hängen die Entwicklungsbedürfnisse der Kinder in erster Linie mit Bindung, Koregulierung, sensorischer Entwicklung und frühem Spracherwerb zusammen. Die Empfehlung, in der frühen Kindheit eine Exposition gegenüber sozialen Medien, anderen digitalen Diensten und Bildschirmangeboten zu vermeiden, impliziert jedoch kein absolutes Verbot.

Unter bestimmten Bedingungen können soziale Medien und andere digitale Dienste in begrenztem Umfang für Kleinkinder genutzt werden, z. B. im Rahmen gemeinsamer Aktivitäten (beispielsweise zum Betrachten von Familienfotos oder für die Kommunikation mit Verwandten über Videoanrufe). Die Verwendung von Bildschirmen als Mittel zur „Beruhigung“ oder Beschäftigung von Kleinkindern über längere Zeiträume hinweg sollte jedoch strikt vermieden werden.

Grundsätzlich sollten Eltern und Betreuungspersonen der direkten zwischenmenschlichen Interaktion mit Kindern und Jugendlichen (beginnend in der frühen Kindheit) Vorrang einräumen, um die gesunde kognitive, körperliche und emotionale Entwicklung der Minderjährigen zu unterstützen.

Verbreitung von Daten von Kindern über Profile in den sozialen Medien begrenzen

Die systematische Dokumentation und öffentliche Verbreitung von Daten von Kindern (einschließlich Bildern und Videos), insbesondere von Kindern unter drei Jahren, durch Profile in den sozialen Medien (z. B. durch „Sharenting“ und „Familien-Influencing“) muss in den Rechtsrahmen angegangen werden. Kinder in dieser Altersgruppe sind nicht in der Lage, in ihre digitale Darstellung einzuwilligen oder die kommerziellen Kontexte, in denen ihre Daten verwendet werden, und die künftigen Auswirkungen einer solchen Präsenz zu verstehen.

Anbieter sozialer Medien und anderer digitaler Dienste dürfen nicht durch Monetarisierungsstrukturen, algorithmische Verstärkung oder auf Nutzerinteraktion bzw. -bindung ausgerichtete Gestaltungsmerkmale Anreize für die Erstellung oder Verbreitung von Inhalten mit Kindern schaffen. Es sollten durchsetzbare Verpflichtungen in Bezug auf soziale Medien und andere digitale Dienste eingeführt werden, anstatt sich allein auf die freiwillige Verantwortung der Betreuungspersonen zu verlassen. Betreuungspersonen sollten klare Leitlinien zu den langfristigen Auswirkungen einer frühzeitigen digitalen Sichtbarkeit auf die Privatsphäre, die Würde und das Recht auf informationelle Selbstbestimmung von Kindern erhalten.

3-12 Jahre: Kindheit als Phase der beaufsichtigten Entwicklung

3-5 JAHRE: PHASE DER STRIKT BEAUFSICHTIGTEN ENTWICKLUNG

Im Alter zwischen drei und fünf Jahren erreichen Kinder eine Entwicklungsphase, die durch bewusste Aktivitäten im Rahmen einer kontinuierlichen externen Strukturierung gekennzeichnet ist. Die Kinder beginnen, bewusstes Handeln, symbolisches Denken und ein stärker kohärentes Selbstkonzept zu entwickeln.

Hinsichtlich der neurologischen Entwicklung ist diese Phase durch die fortschreitende Reifung von Systemen gekennzeichnet, die an Aufmerksamkeit, exekutiven Funktionen und Emotionsregulation beteiligt sind, jedoch weiterhin nicht vollständig ausgereift und gegenüber äußeren Reizen empfindlich sind²⁰. Belohnungsbezogene Systeme sind jedoch bereits aktiv. Kinder entwickeln zunehmend intrinsische Motivation, von Neugier getriebene Erkundungen und frühe Formen autonomen, zielorientierten Verhaltens.

Die Entwicklung in dieser Phase hängt in hohem Maße von den Möglichkeiten für fantasievolles Spiel, selbstinitiierte Aktivitäten und Beziehungserfahrungen ab, den Kompetenzerwerb unterstützen. Dazu gehört auch die Bildung eines narrativen Ichs, das beispielsweise durch Sprache und Rollenspiel zum Ausdruck kommt.

Kinder in diesem Alter können ihre Aktivitäten für begrenzte Zeiträume aufrechterhalten, aber ihre Fähigkeit, Aufmerksamkeit, Impulse und Emotionen zu regulieren, hängt nach wie vor in hohem Maße von externer Unterstützung in Form von Sprache, Nachahmung und Anleitung durch eine Betreuungsperson ab. Diese Phase kann daher als Übergang von der Koregulierung zur geführten Selbstregulation verstanden werden.

ALTERSSPEZIFISCHE HERAUSFORDERUNGEN

Sensitivität für sofortige Belohnung

Diese Kluft zwischen der laufenden Reifung der kindlichen Systeme, die an Aufmerksamkeit, exekutiven Funktionen und Emotionsregulation beteiligt sind, und den bereits aktiven Belohnungssystemen führt zu einem Ungleichgewicht. Kinder in diesem Alter reagieren intensiv auf starke Reize und unmittelbare Belohnungen, haben jedoch nur eine begrenzte inhibitorische Kontrolle und Fähigkeit zum Belohnungsaufschub.

Dadurch sind Kinder im Alter von drei bis fünf Jahren besonders anfällig für Umgebungen sozialer Medien+, die für unmittelbare und wiederholte Belohnung sowie kontinuierliche externe Stimulation optimiert sind. Experimentelle Nachweise deuten darauf hin, dass digitale Umgebungen die Entwicklung von Frustrationstoleranz, Persistenz und intrinsische Motivation beeinträchtigen können²¹.

Durch diese entwicklungsspezifische Konstellation wird ein spezifisches Vulnerabilitätsprofil geschaffen. Die Konditionierung von Belohnungssystemen durch schnelles Feedback, Wiederholungen und intermittierende Verstärkung durch Online-Interaktionen von Kindern kann die Erwartungen an eine sofortige Belohnung prägen und zu habituellen Nutzungsmustern beitragen²².

Eine übermäßige Abhängigkeit von externen Belohnungsstrukturen kann sich auch auf die Entwicklung der intrinsischen Motivation auswirken. Wenn Kinder digitale Technologien nutzen, die durch Merkmale wie kontinuierliche Verstärkung und sofortiges Feedback definiert sind, besteht das Risiko, dass sich das Verhalten in Richtung extern regulierter Verhaltensmuster verlagert, jedoch nicht auf intrinsisch motiviertes Explorationsverhalten ausgerichtet ist.

Dies ist besonders in Entwicklungsphasen von Bedeutung, in denen Autonomie und Kompetenz noch im Entstehen begriffen sind. Untersuchungen zeigen, dass diese Schwachstellen stark von kontextuellen Faktoren wie dem familiären Umfeld, elterlicher Mediation und sozioökonomischen Bedingungen beeinflusst werden²³.

Risiken der Bildschirmexposition

Eine höhere Bildschirmexposition in dieser Phase geht mit einer geringeren Selbstregulation einher, insbesondere hinsichtlich der Aufmerksamkeit und Impulssteuerung der Kinder²⁴. Wie oben dargelegt, kann die Nutzung sozialer Medien und anderer digitaler Dienste entwicklungskritische Aktivitäten wie freies Spiel, körperliche Aktivität, Schlaf und persönliche Interaktion verdrängen²⁵.

Diese Auswirkungen sind jedoch kontextabhängig und werden durch die Qualität der Inhalte, die gemeinsame Nutzung, den Zeitpunkt und Dauer der Nutzung und das soziale Umfeld mitgesteuert, sodass nicht allein Parameter wie die Bildschirmzeit ausschlaggebend sind²⁶. Es gibt Hinweise darauf, dass Online-Interaktionen in diesem Alter das Lernen unterstützen können, wenn die Inhalte interaktiv, altersgerecht und in die aktive Vermittlung durch eine Betreuungsperson eingebettet sind²⁷.

Verfügbarkeit sicherer Offline-Alternativen

Die Sicherheit von Kindern im Internet kann nicht ohne einen Blick auf die allgemeinere Ökologie des täglichen Lebens von Kindern betrachtet werden. In Kontexten, in denen die Bildungs-, Freizeit- und sozialen Angebote für Kinder begrenzt sind, insbesondere in ländlichen oder unterversorgten Gebieten, können Umgebungen sozialer Medien+ zum Schwerpunkt kindlicher Aktivität werden.

Dadurch können die Kinder geschädigt und in ihrer Entwicklung beeinträchtigt werden. Um die potenziellen schädlichen Auswirkungen der Nutzung sozialer Medien und anderer digitaler Dienste auf die Entwicklung von Kindern zu begrenzen, sollten Eltern und Betreuungspersonen ab der frühen Kindheit sichere Offline-Alternativen anbieten. Neben den Betreuungspersonen prägen strukturelle Bedingungen und das Umfeld außerhalb des digitalen Raums Expositionsmuster und die damit verbundenen Risiken. Dazu gehören der Zugang zu sicheren öffentlichen Räumen, außerschulische Aktivitäten und unterstützende soziale Infrastrukturen.

Eingeschränkte Kapazitäten zur Medienbegleitung durch Betreuungspersonen

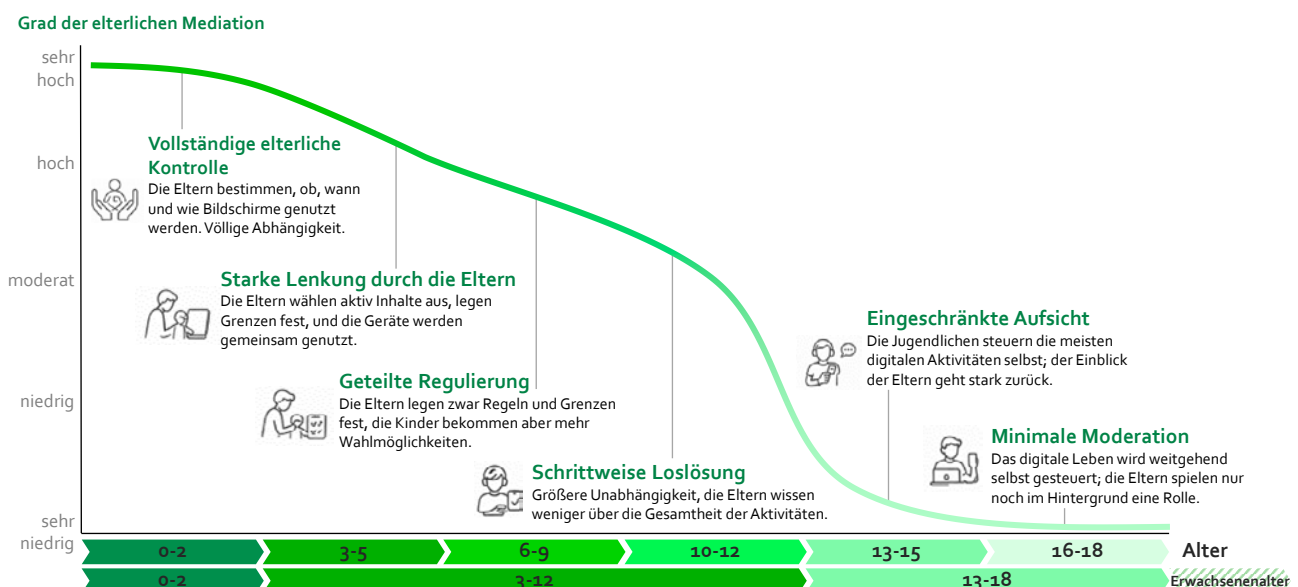
Im Alter von drei bis fünf Jahren ist die Mediation durch Betreuungspersonen nach wie vor ein zentraler Regulierungsmechanismus, der sich jedoch qualitativ verändert. Eltern und Betreuungspersonen wechseln von der direkten Kontrolle zur begleiteten Nutzung, Mitnutzung und interpretierenden Unterstützung.

Die zunehmend selbstinitiierten Aktivitäten von Kindern verringern die Wirksamkeit rein externer Kontrolle, da der elterliche Einfluss mit besonders aufmerksamkeitsbindende digitalen Systemen konkurriert. Die bestehenden Instrumente der elterlichen Kontrolle unterstützen diesen Wandel häufig nicht angemessen, was beispielsweise auf die Fragmentierung in den sozialen Medien+ und eine mangelnde Nutzbarkeit²⁸ zurückzuführen ist.

Aktive Mediation – Erörterung von Inhalten, Strukturierung der Nutzung und Bereitstellung von Erläuterungen – hat sich als hilfreich erwiesen, um das Lernen zu unterstützen und Risiken zu minimieren. Ohne ein solches Eingreifen könnten sich rein restriktive Strategien als weniger wirksam erweisen²⁹. Die Mediation durch die Betreuungsperson wird auch durch Faktoren wie digitale Kompetenz, sozioökonomische Ressourcen, Stressbelastung der Eltern und die Nutzung digitaler Dienste durch die Betreuungspersonen selbst eingeschränkt³⁰.

Abbildung 2 – Rückgang der elterlichen Mediation während der Entwicklung

Mit zunehmendem Alter der Kinder nimmt die direkte elterliche Aufsicht wie auch die digitale Abhängigkeit von elterlicher Begleitung natürlicherweise ab.



SCHLUSSFOLGERUNGEN

Diese Phase stellt einen entscheidenden Übergang für die Sicherheit von Kindern im Internet dar. Kinder sind nicht länger nur passive Rezipienten digitaler Inhalte, sondern zunehmend aktive Teilnehmer an der digitalen Welt, während es ihnen noch immer an einer stabilen Selbstregulation mangelt. Die Exposition nimmt zu, während die interne Regulierung noch nicht vollständig ausgeprägt ist.

Gleichzeitig beginnt eine Verlagerung der Verantwortung von der rein elterlichen Kontrolle zu einem stärker verteilten System, an dem Familien und Bildungseinrichtungen beteiligt sind. Aus politischer Sicht impliziert dies eine reduzierte, dennoch aber wichtige Rolle der elterlichen Aufsicht. Die größte Herausforderung in diesem Alter besteht nicht einfach darin, die Exposition zu begrenzen, sondern auch darin, die Konsolidierung schädlicher Nutzungsmuster in jungen Jahren zu verhindern.

Maßnahmen zum Online-Schutz dieser Altersgruppe müssen eine strukturierte Unterstützung durch das Umfeld und Einrichtungen umfassen. Dazu gehört auch die altersgerechte Gestaltung von Apps und digitalen Inhalten, die für Kleinkinder bestimmt sind, wobei insbesondere belohnungsbasierte und die aufmerksamkeitsbindende Mechanismen wesentlich sind.

Angesichts der in diesem Alter beginnenden, allmählich zunehmenden selbstinitiierten Aktivitäten von Kindern sollten in die frühkindliche Bildung auch digitale Erziehungsinhalte integriert werden. Zwar behalten die Betreuungspersonen ihre Aufsichtsfunktion, doch sollten die elterliche Anleitung und Praktiken der gemeinsamen Nutzung gestärkt werden, insbesondere in schutzbedürftigen Kontexten.

In den derzeitigen Rechtsrahmen bleibt diese Entwicklungsphase häufig unberücksichtigt, sodass der Schwerpunkt entweder auf sehr kleinen Kindern oder aber auf Jugendlichen liegt. Folglich wird die besondere Schutzbedürftigkeit von Kindern zwischen drei und fünf Jahren nach wie vor nicht ausreichend berücksichtigt. Schwerpunkt von Aktivitäten zur Gewährleistung der Sicherheit von Kindern im Internet dieser Altersgruppe muss es sein, Umgebungen so zu gestalten, dass sie die Entwicklung der Selbstregulation von Kindern unterstützen, anstatt sie zu untergraben, und die Betreuungspersonen in die Lage zu versetzen, die Nutzung durch Kinder zu beaufsichtigen.

6-9 JAHRE: DIE PHASE DER BEAUFSICHTIGTEN ENTWICKLUNG

Im Alter zwischen sechs und neun Jahren treten Kinder in eine Entwicklungsphase ein, die durch zunehmende kognitive Kompetenz, strukturiertes, zielorientiertes Verhalten und das Entstehen einer kompetenzbasierten Selbstbewertung gekennzeichnet ist. Kinder sind nun in der Lage, sich konsequenter an regelbasierten Aktivitäten zu beteiligen, ihre Aufmerksamkeit über längere Zeiträume hinweg aufrechtzuerhalten und festgelegte Ziele zu verfolgen.

Eine zentrale Entwicklungsaufgabe ist die Herausbildung eines kompetenzbasierten Selbstkonzept, bei dem der Selbstwert zunehmend mit Leistung und Feedback verknüpft wird. In dieser Phase gewinnt die Entwicklung von Kompetenz und Selbstwirksamkeit für eine gesunde psychologische Entwicklung zunehmend an Bedeutung. Die Kinder entwickeln eine stabilere Selbstregulation, erwerben allmählich Frustrationstoleranz und erfüllen auch anspruchsvolle Aufgaben, die eine gewisse Ausdauer erfordern.

Zudem beginnen die Kinder, Zufriedenheit aus Können und selbsterfahrener Kompetenz und nicht nur aus unmittelbaren externen Belohnungen abzuleiten. Mit dem Eintritt in die Schule werden strukturierte Bewertungssysteme und Vergleiche mit Gleichaltrigen zu einem zentralen Element und prägen die Art und Weise, in der Kinder ihre Fähigkeiten in Bezug auf externe Standards interpretieren.

Neurobiologisch ist diese Phase durch eine Steigerung der Effizienz und Spezialisierung von Gehirnetzwerken gekennzeichnet, insbesondere in Regionen, die mit exekutiven Funktionen verbunden sind. Belohnungs- und Stresssysteme bleiben jedoch sensibel und schaffen eine Konstellation, in der Kinder zunehmend besser in der Lage sind, sich selbst zu regulieren, aber immer noch auf externe Verstärkung ansprechen.

ALTERSSPEZIFISCHE HERAUSFORDERUNGEN

Erhöhte Sensibilität für externe Evaluierungen

Umgebungen der sozialen Medien+ überschneiden sich direkt mit diesen Prozessen. Soziale Medien und andere digitale Dienste, die ein quantifizierbares Feedback, einschließlich Bewertungen, Rankings und Erfolge, liefern, haben unmittelbaren Einfluss auf die kompetenzbasierte Selbstbewertung.

Dies kann Motivation und Selbstwahrnehmung prägen, indem externalisierte Erfolgsmaßstäbe³¹ anstelle von vom Erleben eigener Kompetenz, Neugier und Lernprozessen bestimmend werden. In diesem Alter reagieren die Aufmerksamkeitssysteme nach wie vor empfindlich auf hochstimulierende Umgebungen, die mit der anhaltenden Aufmerksamkeit konkurrieren können, die für das Lernen erforderlich ist³².

Risiko einer frühen Suchtentwicklung

Im Alter zwischen sechs und neun Jahren stabilisieren sich die Gewohnheiten der Kinder, da die Muster der Nutzung, Aufmerksamkeit und Motivation für den Umgang mit sozialen Medien+ im Laufe der Zeit konsistenter werden. In diesem Alter kann eine belohnungsbasierte Verstärkung, insbesondere bei Spielen, zur Herausbildung gewohnheitsmäßiger Nutzungsmuster beitragen³³. Diese Anfälligkeiten werden stark von kontextuellen Faktoren wie dem familiären Umfeld, elterlicher Mediation und sozioökonomischen Bedingungen beeinflusst³⁴.

In diesen Lebensjahren nimmt die Intensität der Nutzung sozialer Medien und anderer digitaler Dienste durch Kinder erheblich zu. Mit dem Eintritt in die Schule und der zunehmenden Interaktion zwischen Gleichaltrigen erhalten Kinder häufigeren und weniger intensiv beaufsichtigten Zugang zu sozialen Medien+. Diese Ausweitung geht mit einem allmählichen Rückgang der direkten elterlichen Kontrolle einher, auch wenn die Beaufsichtigung durch Betreuungspersonen nach wie vor wichtig ist.

In diesem Alter verlagert sich die elterliche Mediation zunehmend auf die Festlegung von Regeln, die Kontrolle ihrer Einhaltung und die Beratung. Ihre Wirksamkeit nimmt jedoch ab, da soziale Medien und andere digitale Dienste für die Kinder zunehmend unabhängig zugänglich und immer komplexer werden³⁵. Die Verantwortung für die Gestaltung des digitalen Umfelds der Kinder verteilt sich allmählich gleichmäßiger zwischen sozialen Medien und anderen Anbietern digitaler Dienste sowie Betreuungspersonen und Pädagogen.

Risiken der Bildschirmexposition

Wie in früheren Lebensphasen besteht die Gefahr, dass die Nutzung des Internets durch die Kinder entwicklungsrelevante Aktivitäten in der „realen Welt“ wie körperliche Aktivität, Schlaf und persönliche Interaktionen³⁶ verdrängt. Ein häufig diskutiertes Beispiel ist die handyfreie Grundschule als bewusstes Gegengewicht zum zunehmend digitalen Leben der Kinder. Untersuchungen deuten darauf hin, dass die Einschränkung der Nutzung von Smartphones an Schultagen nicht nur die Konzentration der Kinder und ihre schulische Leistung verbessern, sondern auch die soziale Interaktion stärken kann.

Forschungsberichte zeigen, dass smartphone-freie Umgebungen das soziale Wohlbefinden verbessern und Konflikte wie Cybermobbing verringern können³⁷. Erkenntnisse aus Interventionen auf Systemebene, beispielsweise in Ländern wie den Niederlanden, deuten auch darauf hin, dass eine Einschränkung der Smartphone-Nutzung zu einem ruhigeren und günstigeren Lernumfeld beiträgt³⁸. Studien zeigen immer wieder, dass Smartphones im Klassenzimmer ein erhebliches Ablenkungspotenzial aufweisen und die Aufmerksamkeit der Kinder beeinträchtigen können³⁹.

Unter geeigneten Bedingungen kann die Internetnutzung in diesem Alter jedoch das Lernen und das kognitive Engagement der Kinder unterstützen, insbesondere, wenn sie strukturiert und entwicklungsorientiert ist⁴⁰. Adaptive Tutoring-Systeme und Bildungs-Apps können individualisierte Lernpfade unterstützen, Themen vertiefen und die Abhängigkeit von Betreuungspersonen verringern. Auf diese Weise kann ein Beitrag zu Inklusion im Bildungsbereich geleistet werden.

SCHLUSSFOLGERUNGEN

Für die Gewährleistung der Sicherheit von Kindern im Internet ist in dieser Phase ein vielschichtiger Ansatz erforderlich. Dazu gehören klare Standards für die altersgerechte Gestaltung sozialer Medien und sonstiger digitaler Dienste, insbesondere in Bezug auf externe Feedback-Systeme und Belohnungsmechanismen, die mit dem sich entwickelnden Selbstkonzept, der Selbstregulation und der intrinsischen Motivation von Kindern interagieren. Verstärkungsschleifen und Monetarisierungsmechanismen, die die Aufmerksamkeit und die intrinsische Motivation beeinträchtigen, erfordern besondere Aufmerksamkeit.

Die digitale Bildung von Kindern sollte innerhalb der Schulsysteme gestärkt werden, wobei der Schwerpunkt nicht allein auf technischen Kompetenzen, sondern auch auf Aufmerksamkeit, Selbstregulation und kritischer Auseinandersetzung liegen sollte. Es bedarf strukturierter Rahmen für die Internetnutzung, die ein Gleichgewicht zwischen digitalem Engagement und Offline-Aktivitäten herstellen.

Die telefonfreie Grundschule kann als entwicklungsgerechtes Schutz- und Lernumfeld verstanden werden. Dadurch werden Räume geschaffen, in denen Kinder grundlegende soziale Kompetenzen entwickeln können, beispielsweise im Bereich der persönlichen Kommunikation, der Konfliktlösung und der kooperativen Interaktion. Diese Kompetenzen bilden die Grundlage für eine stärker reflektierende, verantwortungsvollere Nutzung von Online-Aktivitäten in späteren Phasen.

Solche Maßnahmen sollten nicht als Verbot digitaler Technologien konzipiert werden, sondern als pädagogisch eingebettete beaufsichtigte Nutzung des Internet, durch welche die analogen Erfahrungen von Kindern gestärkt und Kinder schrittweise auf Medienkompetenz in sozialen Medien+ vorbereitet werden. Diese Maßnahmen ersetzen nicht die Rolle von Eltern oder Betreuungspersonen, deren informierte Mediation ein zentraler Bestandteil eines wirksamen Schutzes bleibt.

10-12 JAHRE: PHASE ABNEHMENDER BEAUFSICHTIGUNG

Das Alter von 10 bis 12 Jahren ist eine kritische Phase in der Entwicklung von Kindern, die durch die Reorganisation der eigenen Persönlichkeit im Verhältnis zu anderen gekennzeichnet ist. Das Selbstbild wird differenzierter, aber auch instabiler, da Kinder ihre Identität zunehmend durch Vergleich mit Gleichaltrigen, soziale Positionierung und wahrgenommene Akzeptanz aufbauen. Parallel dazu wird externes Feedback zu einem zentralen Organisationsprinzip der Selbstbewertung.

Beziehungen zu Gleichaltrigen gewinnen erheblich an Bedeutung. Gleichaltrige fungieren zunehmend als zentrale Bezugspunkte für Normen, Werte und Verhaltensweisen. Selbstwahrnehmung und Verhalten der Kinder werden in erheblichem Maße durch Prozesse sozialer Beeinflussung, beispielsweise Konformitätsdruck, sozialer Vergleich und implizite Gruppennormen, geprägt.

Netzwerke Gleichaltriger erfüllen wichtige unterstützende Funktionen. Sie bieten emotionale Validierung, soziale Orientierung und Möglichkeiten zur gemeinsamen Bewältigung entwicklungsbedingter Herausforderungen. Die Unterstützung durch Gleichaltrige kann je nach Kontext und vorherrschenden Gruppennormen sowohl als Quelle von Resilienz als auch als Verstärker von Risikodynamik wirken.

ALTERSSPEZIFISCHE HERAUSFORDERUNGEN

Kontinuierlicher Zugang zu Online-Angeboten

Mit zunehmendem Alter verlagern sich diese unter Gleichaltrigen ablaufenden Prozesse immer häufiger in ein digitales Umfeld. Soziale Medien und andere digitale Dienste ermöglichen eine kontinuierliche, niedrighschwellige und oft grenzenlose Interaktion von Kindern mit Gleichaltrigen. Dadurch können soziale Verbundenheit und Zugehörigkeit über physische Kontexte hinaus aufgebaut und aufrechterhalten werden.

Für viele Kinder in diesem Alter wird der Zugang zu sozialen Medien und anderen digitalen Diensten bereits zu einer Voraussetzung für soziale Teilhabe. Wie in der vorhergehenden Phase kann die Nutzung sozialer Medien+ wichtige Entwicklungsaktivitäten wie körperliche Aktivität, Schlaf und Offline-Interaktion verdrängen⁴¹.

Intensiverer sozialer Vergleich

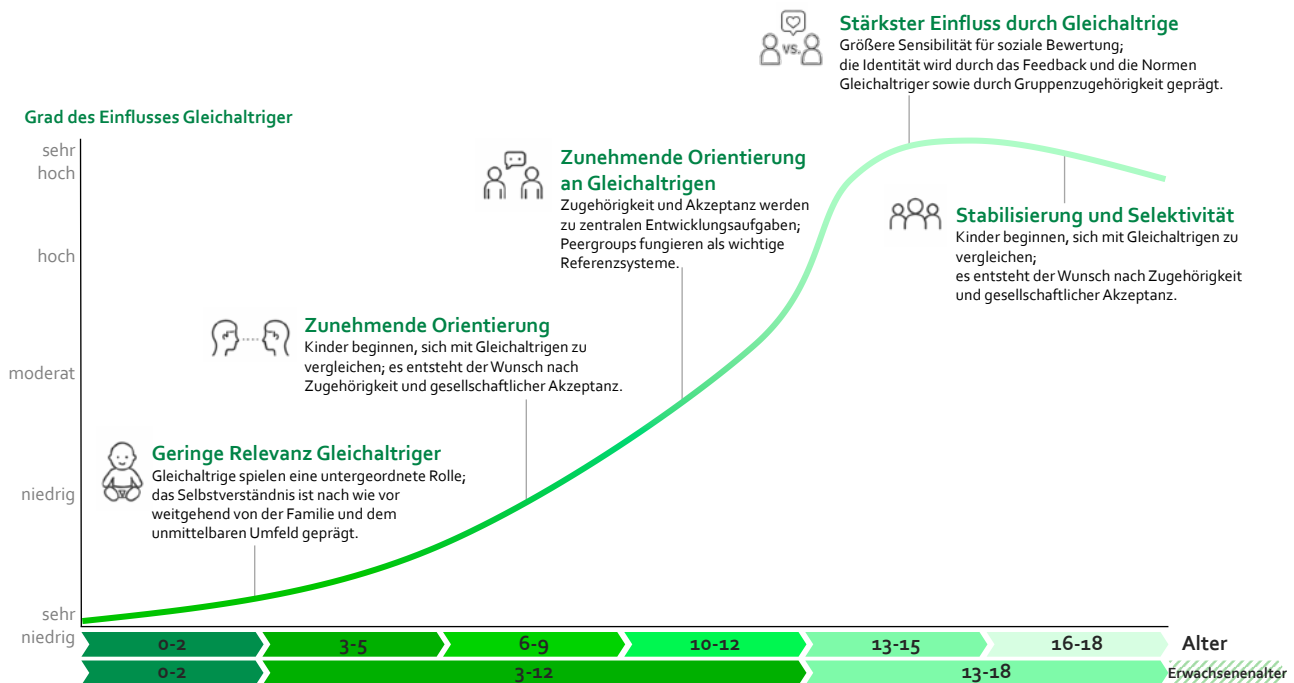
Die strukturellen Merkmale sozialer Medien und anderer digitaler Dienste, insbesondere die Persistenz, Sichtbarkeit und Skalierbarkeit von Interaktionen, verstärken die Auswirkungen des Einflusses Gleichaltriger. Algorithmisch strukturierte Umgebungen können diese Dynamik noch verstärken, indem sie emotional auffällige, mit sozialer Belohnung einhergehende oder stark aufmerksamkeitsbindende Inhalte kontinuierlich priorisieren.

In diesem Alter bewerten sich Kinder zunehmend über solche Aspekte wie das äußere Erscheinungsbild, die Beliebtheit und die soziale Kompetenz. Gleichzeitig beginnen sie mit bewusster Selbstdarstellung und Identitätsexperimentierung, insbesondere in digitalen Umgebungen.

Ein weiterer Mechanismus ist die Internalisierung von Normen und Verhaltensweisen. Die Exposition gegenüber Inhalten, die riskante Verhaltensweisen oder schädliche Normen darstellen, kann die Wahrscheinlichkeit einer Nachahmung erhöhen, insbesondere in einer Phase, in der sich die normativen Rahmen noch herausbilden⁴². Schwerwiegendere Risiken wie Nötigung oder Ausbeutung sind weniger häufig, aber potenziell schädlicher.

Abbildung 3 – Der zunehmende Einfluss Gleichaltriger während der Entwicklung

Mit zunehmendem Alter von Kindern nimmt der Einfluss Gleichaltriger zu und erreicht in der Adoleszenz einen Höhepunkt, da in dieser Phase Zugehörigkeit, soziale Bewertung und Identitätsausdruck zentrale Bedeutung erlangen



Algorithmischer Einfluss auf die Identitätsbildung

In einer Entwicklungsphase, die durch zunehmende Identitätsbildung und eine verstärkte Orientierung hin zu Gleichaltrigen gekennzeichnet ist, kann die algorithmische Verstärkung auch dazu beitragen, die Meinungsbildung, die soziale Orientierung und die Selbstbewertung in einer Weise zu gestalten, die Kinder noch nicht vollständig erkennen oder der sie nicht widerstehen können.

Plattformen sozialer Medien+ bieten Instrumente zur Gestaltung der eigenen Identität und zum Prägen von Eindrücken⁴³. Die Online-Identität wird nicht nur erfahren, sondern kontinuierlich präsentiert und bewertet, wodurch ein neuer Entwicklungskontext entsteht. Für Kinder in diesem Alter wird die Sichtbarkeit in den sozialen Medien zu einer wichtigen Dimension ihres Status unter Gleichaltrigen⁴⁴.

Kinder interagieren zunehmend mit personalisierten Informationsumgebungen, in denen Inhalte nach prognostizierte Nutzerinteraktion und nicht nach Entwicklungseignung ausgewählt werden. Dadurch können bestehende Interessen und Anfälligkeiten gestärkt und gleichzeitig die Expositionsvielfalt verringert werden, wodurch Feedback-Schleifen für Aufmerksamkeit und Verstärkung entstehen⁴⁵.

Gleichzeitig ist die Identitätsbildung nach wie vor instabil. Dies macht Kinder in diesem Alter besonders anfällig für äußere Einflüsse wie idealisierte Darstellungen und auf dem äußeren Erscheinungsbild basierenden Normen, insbesondere in visuellen Kontexten sozialer Medien+.

Risiken für die psychische Gesundheit

Da die Sensitivität für die soziale Bewertung stark zunimmt, sind das Selbstwertgefühl und das emotionale Wohlbefinden der Kinder Schwankungen unterworfen. In dieser Phase treten erstmals zwischenmenschliche Risiken von Online-Aktivitäten auf, darunter Cybermobbing, Ausgrenzung und negative Interaktionen mit Gleichaltrigen. Aufgrund der erhöhten Sensibilität für die soziale Bewertung und der Persistenz der digitalen Kommunikation können solche Erfahrungen starke emotionale Auswirkungen haben.

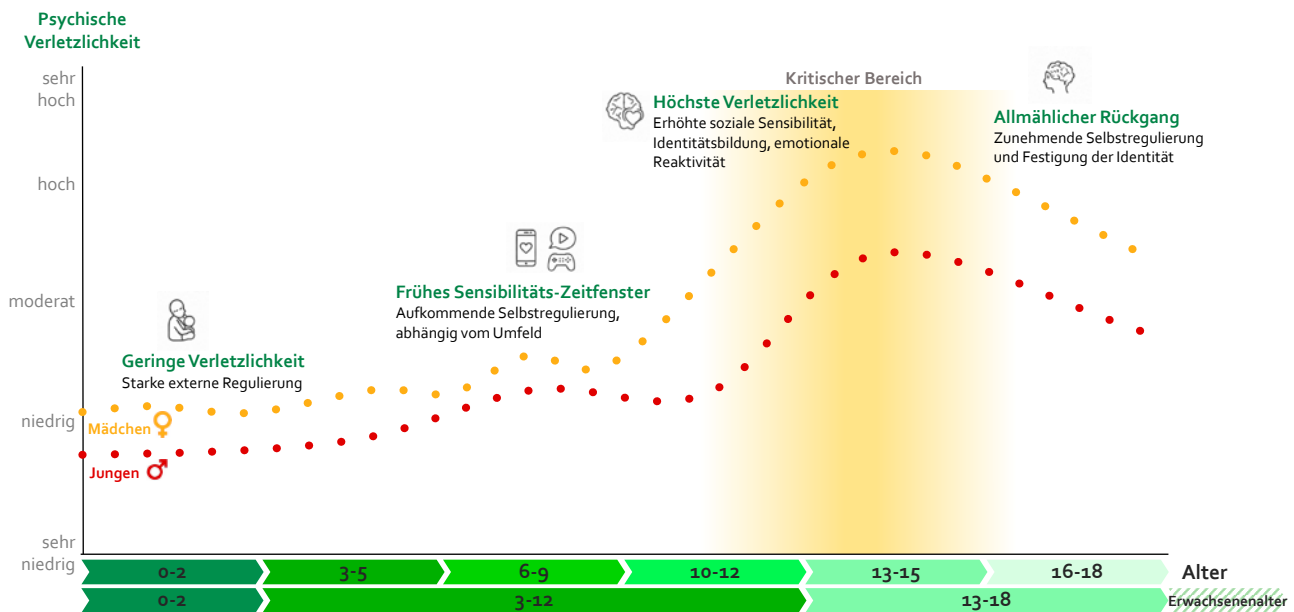
In Bezug auf die Nutzung von Smartphones deuten prospektive Längsschnittstudien darauf hin, dass der Erwerb eines Smartphones bei Kindern im Alter von 12 Jahren mit psychischen Problemen und im Alter von 13 Jahren mit Schlafmangel in Verbindung gebracht werden kann. Andererseits gibt es Anhaltspunkte dafür, dass der Erwerb eines Smartphones im Alter von 13 Jahren statistisch nicht mit dem Auftreten von Depressionen im Alter von 14 Jahren in Verbindung zu bringen ist. Diese Ergebnisse werden auch durch die Nutzungsdauer beeinflusst. Der Schluss liegt nahe, dass Kinder im Alter von 13 Jahren emotional eher bereit sind, ein Smartphone zu benutzen, soziale Medien und andere digitale Dienste zu nutzen und mit potenziell negativen Auswirkungen auf ihre psychische Gesundheit umzugehen⁴⁶.

Für viele Kinder markiert der Lebensabschnitt zwischen zehn und 12 Jahren ein frühes Stadium der Entwicklung von internalisierenden Problemen wie Angstzuständen und depressiven Symptomen. Diese Probleme werden häufig bidirektional durch die Nutzung sozialer Medien und anderer digitaler Dienste beeinflusst⁴⁷. Dabei ist die Dynamik ungleichmäßig verteilt. Es gibt Hinweise darauf, dass Mädchen besonders anfällig für auf dem äußeren Erscheinungsbild beruhende Vergleiche und plattformgestützte soziale Bewertungen sind.

Soziale Medien und andere Architekturen digitaler Dienste prägen die Risikoexposition weiter. Konkret wird die Exposition gegenüber idealisierten und auf das äußere Erscheinungsbild ausgerichteten Inhalten mit Unzufriedenheit mit dem eigenen Körper und negativer Selbstwahrnehmung, insbesondere bei Mädchen, in Verbindung gebracht⁴⁸. In diesem Alter besteht ein komplexerer Zusammenhang zwischen individuellen Anfälligkeiten wie ADHS, Angstzuständen oder sozialen Schwierigkeiten einerseits sowie Umgebungen sozialer Medien+ andererseits, wodurch problematische Nutzungsmuster häufig verstärkt werden⁴⁹. Die Auswirkungen von Umgebungen der sozialen Medien+ auf die psychische und körperliche Gesundheit von Kindern sowie soziale und individuelle Risikofaktoren werden in Kapitel 2 näher untersucht.

Abbildung 4 – Psychologische Anfälligkeit während der Entwicklung

Sensibilität für psychische Gesundheitsprobleme und digitale Risiken



SCHLUSSFOLGERUNGEN

Das Alter zwischen zehn und 12 Jahren ist eine kritische Phase, die durch entwicklungsbedingte Anfälligkeiten, eine abnehmende Beaufsichtigung durch Eltern und Betreuungspersonen sowie die zunehmende Nutzung digitaler Dienste gekennzeichnet ist. Digitale Risiken ergeben sich aus der Wechselwirkung zwischen diesen Faktoren und nicht allein aus der individuellen Nutzung digitaler Medien. Diese Phase stellt somit einen wichtigen Wendepunkt für die Sicherheit von Kindern im Internet dar. Die größte Herausforderung besteht in der Konvergenz von entwicklungsbedingten Anfälligkeiten und Verstärkungsmechanismen, die das Risiko eines instabilen Selbstwertgefühls und eines problematischen Nutzungsverhaltens im Umgang mit digitalen Medien erhöhen.

Dies erfordert einen Übergang von elternzentrierten Ansätzen zu einer strukturorientierten, an die Entwicklung angepassten Regulierung. Der Zugang zu digitalen Geräten sollte in dieser Phase sorgfältig geregelt werden. Die Nutzung sollte in erster Linie entweder mit Zustimmung und unter Aufsicht der Eltern oder in strukturierten Bildungskontexten (beispielsweise mithilfe von geführten schulischen Lernanwendungen) und nicht auf der Grundlage von uneingeschränktem persönlichem Besitz von Geräten erfolgen. Dieser Ansatz trägt dazu bei, eine frühe digitale Teilhabe mit der Festlegung der erforderlichen Schutzgrenzen in Einklang zu bringen.

Institutionelle Reaktionen, insbesondere in Schulen, sollten digitale Fähigkeiten und Kompetenzen, emotionale Resilienz und kritische Auseinandersetzung fördern. Betreuungspersonen bleiben wichtig, insbesondere im Zusammenhang mit dem Nutzungsverhalten in der Freizeit. Ihr Einfluss wird jedoch zunehmend durch die sich entwickelnde Autonomie der Kinder und die Komplexität der sozialen Medien und weiterer digitaler Dienste eingeschränkt.

EMPFEHLUNGEN (3-12 JAHRE)

Nutzung altersgerechter sozialer Medien+ und Endgeräte unter Aufsicht sicherstellen

Ab einem Alter von drei Jahren sollten die Online-Interaktionen von Kindern begrenzt und überwacht sowie schrittweise und strukturiert an die sich entwickelnden Fähigkeiten der Kinder angepasst werden. Die Verwendung von Endgeräten ohne Zustimmung und Aufsicht durch die Eltern sollte vermieden werden. Betreuungspersonen sollten persönlichen Interaktionen und Offline-Aktivitäten weiterhin Priorität einräumen und sicherstellen, dass die Kinder ausreichend schlafen. In Bildungseinrichtungen sollte die Nutzung der von den Schulen bereitgestellten Endgeräte durch Kinder und Jugendliche einem festgelegten pädagogischen Zweck dienen. Grundschulen sollten weitgehend frei von solchen Endgeräten sein, um die Entwicklung, die sozialen Interaktionen und das Lernen der Kinder zu schützen.

Kindern und ihrem Umfeld hochwertige Bildungsinhalte für den Erwerb digitaler Kompetenzen und für Wohlbefinden bereitstellen

Kinder und Jugendliche sollten bereits ab einem frühen Alter und während der gesamten Schulzeit Zugang zu hochwertiger digitaler Bildung und Medienkompetenz (einschließlich KI-Kompetenz) haben. Bei der Konzeption der Bildung in den Bereichen Digitales und Medienkompetenz könnten Minderjährige konsultiert werden. Im Rahmen der Bildung sollten Kindern und Jugendlichen das Wissen und die Fähigkeiten vermittelt werden, die sie benötigen, um die Risiken zu verstehen und sich online sicher zurechtzufinden.

Selbstregulationskompetenzen sollten bereits in den ersten Lebensjahren als Priorität hervorgehoben werden, nicht nur für Kinder im schulpflichtigen Alter. Schulen sollten sicherstellen, dass Kinder und Jugendliche Informationen über Wohlbefinden und hochwertige Bildung im Bereich der psychischen Gesundheit erhalten. Es sollten einschlägige Ressourcen und Fachkräfte zur Verfügung gestellt werden, um Kinder sowie Betreuungspersonen und Pädagogen (das Umfeld) in ihrer Aufsichtsfunktion zu unterstützen. Das Umfeld der Kinder muss in der Lage sein, frühe Anzeichen für digitale Vernachlässigung, schädliche Nutzung und Missbrauch online zu erkennen, und es muss wissen, wo Unterstützung verfügbar ist.

13-18 Jahre: Jugend als Phase der sich entwickelnden Autonomie

13-15 JAHRE: DIE ERSTE PHASE DER SICH

ENTWICKELNDEN AUTONOMIE

Die Jugend im Alter von 13 bis 15 Jahren ist die zentrale Phase der Identitätsbildung von Minderjährigen. Sie ist durch einen verstärkten Wissensdrang, Instabilität und das Streben nach Kohärenz über verschiedene soziale Kontexte hinweg gekennzeichnet. Beziehungen zu Gleichaltrigen werden zum wichtigsten Bezugspunkt für Selbstbewertung und Zugehörigkeit. Die kognitiven Fähigkeiten werden erweitert und ermöglichen fortgeschrittenes abstraktes Denken, die Einnahme unterschiedlicher Perspektiven und Selbstreflexion.

Entscheidungsfindung und Selbstregulation verbessern sich ebenfalls, bleiben aber kontextabhängig, insbesondere in emotional oder sozial belasteten Situationen. Die Identitätsentwicklung verläuft zunehmend in digital vermittelten Umgebungen, in denen Selbstdarstellung, Feedback und soziale Bewertung kontinuierlich, sichtbar und skalierbar sind⁵⁰.

Neurobiologisch ist die Jugend durch ein Ungleichgewicht zwischen hochaktiven emotionalen und Belohnungssystemen und der Entwicklung von Systemen der kognitiven Kontrolle gekennzeichnet. Während limbische Prozesse ^d die emotionale Reaktivität und die Sensibilität für soziales Feedback erhöhen, reift der präfrontale Kortex (der für Impulskontrolle und Selbstregulation verantwortlich ist) langsamer. Hormonelle Veränderungen verstärken die emotionale Erfahrung weiter.

Dies führt zu einer Entwicklungskonfiguration, in der Jugendliche reaktiver und anfälliger für soziale Bewertungen sind sowie eine größere Risikobereitschaft aufweisen, insbesondere unter Gleichaltrigen. Obwohl sich die Selbstregulationsfähigkeiten verbessern, können sie mit der Intensität sozioemotionaler Verarbeitungsprozesse häufig nicht Schritt halten⁵¹.

Psychologisch ist diese Phase durch eine intensivere Gestaltung von Identitätsarbeit, emotionale Variabilität und die Abhängigkeit von externer Validierung bestimmt. Das Selbstwertgefühl wird instabil und hängt von sozialem Feedback ab, während sich Jugendliche zunehmend bewusst selbst präsentieren. Umgebungen der sozialen Medien+ bieten Vorteile wie Editierbarkeit, Sichtbarkeit und quantifizierbares Feedback, die diese Prozesse erleichtern⁵².

ALTERSSPEZIFISCHE HERAUSFORDERUNGEN

Risiken für die psychische Gesundheit

In dieser Phase werden soziale Medien und andere digitale Dienste für die Emotionsregulation und -bewältigung genutzt, was kurzfristige Vorteile bieten, aber auch die Abhängigkeit von externer Regulierung verstärken kann⁵³. Die Nutzung sozialer Medien+ durch Jugendliche als Strategie zur Stimmungsregulierung kann mit einem häufigeren Auftreten depressiver Symptome in Verbindung gebracht werden⁵⁴.

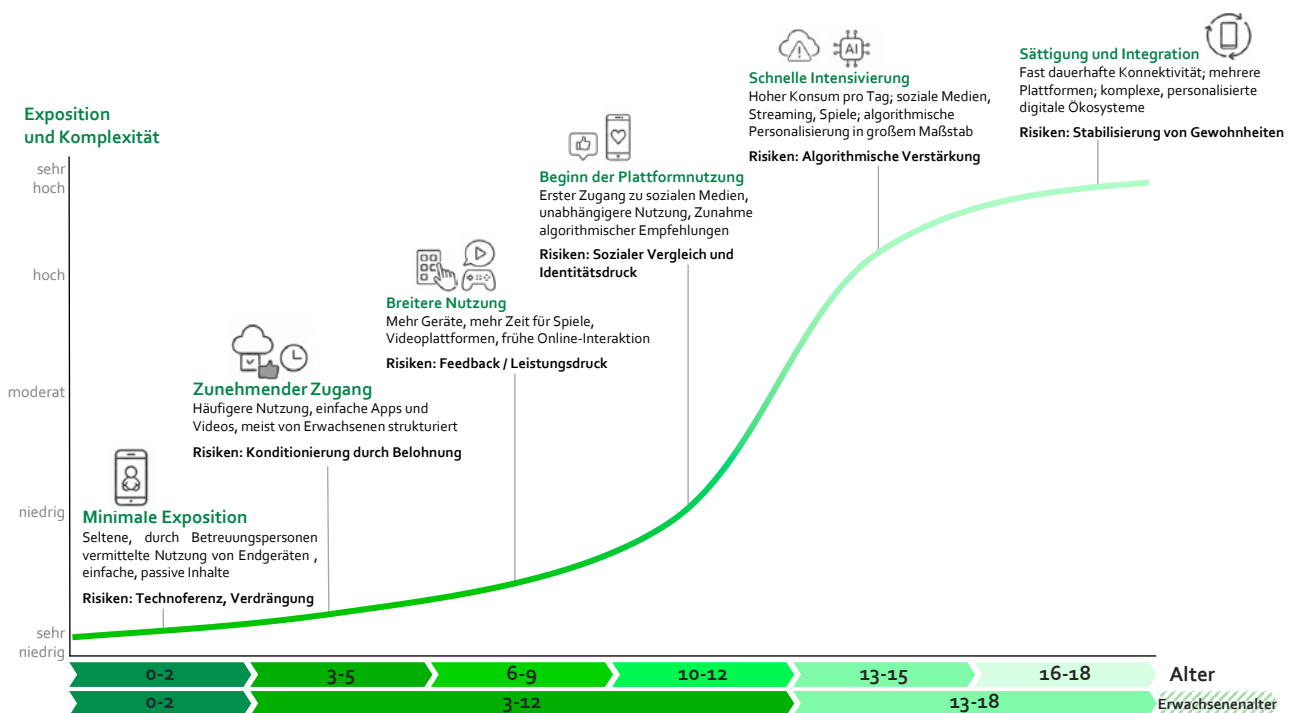
Die Zeit der Jugend zwischen 13 und 15 Jahren stellt den Höhepunkt der Anfälligkeit für psychische Gesundheitsprobleme dar, was durch die Wechselwirkung von entwicklungsbedingten Veränderungen

^{d.} Das limbische System besteht aus einer Reihe von Gehirnstrukturen, die an Prozessen der Verarbeitung von Emotionen, der Motivation und der Belohnung beteiligt sind.

und Umwelteinflüssen noch verstärkt wird. Diese Phase steht im Zusammenhang mit einem erhöhten Auftreten internalisierender Störungen wie Depressionen und Angstzustände⁵⁵. Eine erhöhte Sensitivität für sozialen Vergleich, Feedback und Ausgrenzung führt zu einer spezifischen Anfälligkeit in Umgebungen der sozialen Medien+. Belastungen im Zusammenhang mit Selbstdarstellung und einer instabilen eigenen Identität können zu einer geringeren Klarheit des Selbstbildes beitragen.

Risikobehaftete Verhaltensweisen erreichen ihren Höhepunkt und sind stark von der Dynamik unter Gleichaltrigen (Peer-Dynamiken) geprägt. Dies kann durch Sichtbarkeit und Feedback im digitalen Raum noch verstärkt werden. Individuelle und kontextuelle Faktoren wie psychische Vorerkrankungen und familiärer Stress interagieren mit Umgebungen der sozialen Medien+, was die Anfälligkeiten im Laufe der Zeit häufig verstärkt⁵⁶. Längsschnittdaten deuten darauf hin, dass diese Risiken uneinheitlich sind. Besonders starke und anhaltende negative Auswirkungen sind bei heranwachsenden Mädchen zu beobachten.

Abbildung 5 – Digitale Exposition und Komplexität während der gesamten Entwicklung
Zugänglichkeit, Intensität und Komplexität von Umgebungen der sozialen Medien+ nehmen zu



Risiken im Zusammenhang mit KI, sozialen Medien und anderen digitalen Diensten

Digitale Risiken im Jugendalter werden durch die Konvergenz von autonomer Nutzung, entwicklungsbedingten Anfälligkeiten und algorithmisch strukturierten Umgebungen verstärkt. Ein besonders wichtiges KI-spezifisches Risiko in dieser Phase betrifft Konversationsagenten und sogenannte „KI-Gefährten“. Jugendliche können solche Systeme nicht nur für Unterhaltungs- oder Informationssuche nutzen, sondern auch für persönliche, emotionale oder krisenbezogene Gespräche.

Diese Interaktionen sind oft so konzipiert, dass sie bestätigend, konfliktarm und dauerhaft verfügbar sind. Dies mag zwar eine Form der niedrigschwelligen Unterstützung bieten, birgt aber auch das Risiko einseitiger Bindung und emotionaler Abhängigkeit. Dies kann durch eine geringere Exposition gegenüber Mehrdeutigkeit, Widerspruch und wechselseitiger Verantwortung, die zwischenmenschliche Beziehungen kennzeichnen, erreicht werden.

Wenn solche Systeme ohne zuverlässige Altersüberprüfung oder angemessene Schutzvorkehrungen zugänglich sind, entstehen zusätzliche Risiken im Zusammenhang mit sexualisierter Kommunikation, Manipulation, Grooming und krisenbezogenen Inhalten. KI-Gefährten stellen nicht nur eine andere Form digitaler Inhalte dar, sondern eine neue Art des sozioemotionalen Umfelds, das eine spezielle entwicklungsorientierte und regulatorische Aufmerksamkeit erfordert.

Ein zentraler Mechanismus ist die algorithmische Verstärkung. Empfehlungssysteme priorisieren Inhalte, die Nutzerbindung maximieren und häufig emotional auffälliges und identitätsrelevantes Material übergewichten. Dies kann die Wahrnehmung und das Verhalten im Laufe der Zeit beeinflussen, indem bestehende Vulnerabilitäten verstärkt werden⁵⁷. Viele soziale Medien und andere digitale Dienste fördern eine kontinuierliche soziale Bewertung und setzen Jugendliche anhaltendem Feedback und Vergleichen aus. Dies kann die emotionale Instabilität und Abhängigkeit von externer Validierung erhöhen.

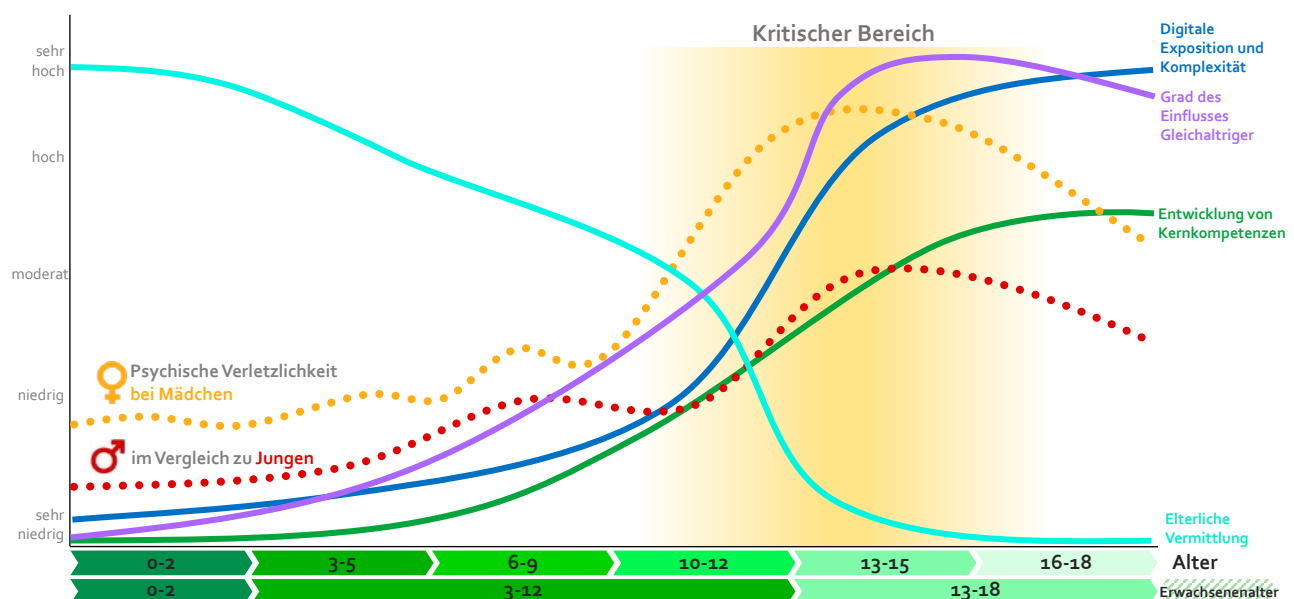
Risiko problematischer Nutzung und Suchtverhalten

Gestaltungsmerkmale wie variable Belohnungen, unendliches Scrollen (infinite scrolling) und ständige Verfügbarkeit tragen zu einer problematischen oder zwanghaften Nutzung bei und interagieren mit der erhöhten Empfänglichkeit Jugendlicher für Belohnungen⁵⁸. Die Nutzung sozialer Medien und anderer digitaler Dienste geht auch mit Schlafstörungen, vermindertem Wohlbefinden und emotionaler Belastung einher, obwohl die Auswirkungen im Allgemeinen gering sind und durch den Kontext abgeschwächt werden⁵⁹.

Wichtig ist, dass diese Risiken nicht für alle Dienste einheitlich oder bestimmend sind. Sie ergeben sich aus der Wechselwirkung zwischen entwicklungsbedingten Vulnerabilitäten und digitalen Merkmalen und machen deutlich, dass über vereinfachte Modelle für die Auswirkungen digitaler Dienste hinausgegangen werden muss⁶⁰.

Abbildung 6 – Missverhältnis zwischen digitaler Exposition, Anfälligkeit und Regulierungskapazität im Laufe der Entwicklung

Die kombinierten Entwicklungswege veranschaulichen, dass die digitale Exposition rasch zunimmt, während die Mediation durch die Eltern abnimmt und sich die Regulierungskompetenzen langsamer entwickeln. Dieser Trend fällt mit einem maximalen Niveau der psychologischen Vulnerabilität in der Jugend zusammen.



SCHLUSSFOLGERUNGEN

Ab dem Alter von 13 Jahren wechseln Jugendliche von einer beaufsichtigten zu begleiteter Online-Nutzung. Jugendliche haben mehr Freiheit zur Erschließung der Möglichkeiten, die die Online-Welt bietet, um Kontakte zu knüpfen, zu lernen und ihre Kreativität zu entfalten. Soziale Medien und andere digitale Dienste bieten Jugendlichen die Möglichkeit, ihre Leidenschaften und Interessen zu entwickeln und sie mit anderen zu teilen.

Eine zunehmende Eigenständigkeit gehört heutzutage nicht nur offline, sondern auch in der Online-Welt zum Aufwachsen dazu. Es geht nicht darum, Jugendliche in diesem Übergangsprozess zurückzuhalten, sondern vielmehr darum, dafür zu sorgen, dass sie in einer Phase besonders hoher entwicklungsbedingter Vulnerabilität weniger Gefahren ausgesetzt sind. Diese Vulnerabilität ist gekennzeichnet durch die Konvergenz der Identitätsbildung, eine erhöhte sozioemotionale Sensitivität und algorithmisch strukturierte Umgebungen.

Digitale Risiken ergeben sich nicht allein aus der Exposition, sondern aus ihrer Intensität und Struktur innerhalb der sozialen Medien+, die darauf ausgelegt sind, die Nutzungsinteraktion der Jugendlichen in einem Lebensabschnitt erhöhter Anfälligkeit zu maximieren. Aufgrund dieser Faktoren ist die Jugend sowohl für die Forschung als auch für die Gesetzgebung von zentraler Bedeutung.

In diesem Alter werden traditionelle Formen der Beaufsichtigung durch Betreuungspersonen und Pädagogen immer ineffizienter und schwieriger umzusetzen. Die Risiken werden zunehmend durch soziale Medien und andere digitale Dienste und nicht mehr nur durch individuelles Verhalten geprägt. Eine zentrale Herausforderung besteht im Umgang mit algorithmischen Systemen, die Exposition strukturieren und das Verhalten beeinflussen, gleichzeitig aber nur begrenzt transparent sind.

Bei Regulierungsansätzen muss ein Ausgleich zwischen dem Schutz der Jugendlichen und ihrem Streben nach Autonomie und Teilhabe im Online-Bereich gefunden werden. Für einen wirksamen Schutz ist ein entwicklungsorientierter, vielschichtiger Ansatz erforderlich, bei dem die Regulierung sozialer Medien+, Bildungsmaßnahmen sowie Unterstützung zur Selbstregulation und kritischen Nutzung digitaler Dienste ineinandergreifen.

Jüngste Untersuchungen deuten darauf hin, dass pauschale Verbote der Nutzung sozialer Medien+ möglicherweise weniger wirksam sind als häufig angenommen. Während solche Maßnahmen darauf abzielen, die Exposition und die damit verbundenen Risiken zu verringern, sind die Nachweise ihrer Wirksamkeit, insbesondere bei Jugendlichen, derzeit begrenzt. Übermäßig restriktive Ansätze können umgangen werden oder Risiken auf weniger stark regulierte Umgebungen verlagern.

Vor diesem Hintergrund wurde als entwicklungssensiblere Alternative ein altersdifferenziertes Modell der regulierten Teilhabe vorgeschlagen, bei dem eine Altersüberprüfung unter Einhaltung der Datenschutzbestimmungen, Safety by Design und Medienbildung kombiniert werden. Mit diesem Ansatz werden Schutzmaßnahmen an die sich entwickelnden Fähigkeiten der Kinder angepasst, wobei ein Gleichgewicht zwischen Sicherheit, Teilhabe und Kinderrechten innerhalb eines integrierten Rahmens für die Sicherheit von Kindern im Internet hergestellt wird.

16-18 JAHRE: DIE ZWEITE PHASE DER SICH ENTWICKELNDEN AUTONOMIE

Die späte Adoleszenz markiert eine Phase zunehmender Identitätskonsolidierung und wachsender Autonomie. Zuvor ausprobierte Rollen, Werte und Selbstkonzepte beginnen sich zu stabilisieren, was zu kohärenteren und intern integrierten Selbstrepräsentationen führt. Unterdessen haben die kognitiven Fähigkeiten einen höheren Entwicklungsstand erreicht. Dazu gehören abstraktes Denken, langfristige Planung und reflektierte Entscheidungsfindung.

Diese Entwicklungen unterstützen eine stärker autonome Teilhabe an Sozial-, Bildungs- und Wirtschaftssystemen. Soziale Medien und andere digitale Dienste sind nicht länger Räume zum Ausprobieren, sondern vollständig in das tägliche Leben eingebettet und prägen Kommunikation, Teilhabe und den Ausdruck der eigenen Persönlichkeit⁶¹. Neurobiologisch nähert sich das Gehirn der funktionellen Reife, insbesondere im präfrontalen Kortex. Dies führt zu einer verbesserten Selbstkontrolle, Planung und Entscheidungsfindung.

Emotionale und kognitive Systeme werden stärker integriert, was eine stabilere Emotionsregulation und eine bessere Antizipation langfristiger Folgen ermöglicht. Die Entwicklung ist jedoch noch nicht abgeschlossen, da die Reifung bis ins frühe Erwachsenenalter andauert⁶². Dies führt zu einem Profil erhöhter Stabilität in Verbindung mit einer anhaltenden Empfindlichkeit gegenüber stark anregenden Umgebungen.

ALTERSSPEZIFISCHE HERAUSFORDERUNGEN

Pfadabhängigkeit

Trotz der zunehmenden Reife in diesem Alter bestehen nach wie vor Anfälligkeiten. Frühere Probleme im Bereich der psychischen Gesundheit können fortbestehen, insbesondere wenn die zugrunde liegenden Mechanismen nicht angegangen werden⁶³. Dies unterstreicht die Notwendigkeit, Minderjährige nicht erst in der Jugend, sondern bereits ab der frühesten Kindheit vor potenziellen Schäden zu schützen.

Die Selbstregulation ist zwar verbessert, hängt aber nach wie vor vom Kontext ab und kann durch stark aufmerksamkeitsbindende digitale Umgebungen herausgefordert werden. Darüber hinaus führt die Konsolidierung von Verhaltensmustern zu einer Pfadabhängigkeit, wodurch etablierte Gewohnheiten widerstandsfähiger gegenüber Veränderungen werden. Digitale Risiken in diesem Alter betreffen weniger das Entstehen als vielmehr die Stabilisierung und Verstärkung.

Risiken einer problematischen Nutzung

Etablierte Nutzungsmuster, einschließlich problematischer und übermäßiger Nutzung oder Abhängigkeit, werden durch Funktionen in sozialen Medien und anderen digitalen Diensten (beispielsweise personalisierte Empfehlungen, kontinuierliche Inhaltsströme und auf Belohnung basierendes Nutzerverhalten) aufrechterhalten und gestärkt⁶⁴. Algorithmische Systeme prägen Exposition und Verhalten nach wie vor, oft unterbewusst⁶⁵. Schließlich werden Anfälligkeiten nach wie vor durch strukturelle Ungleichheiten wie das familiäre Umfeld und den Zugang zu Ressourcen geprägt⁶⁶.

Die Nutzung sozialer Medien+ bleibt mit Folgen wie Schlafstörungen, emotionalem Stress und sozialem Vergleich verbunden. Die Auswirkungen werden jedoch zunehmend von langfristigen Mustern und nicht

von akuten entwicklungsbedingten Sensitivitäten bestimmt⁹⁷. Risiken im Zusammenhang mit der Datenverwertung, dem kommerziellen Einfluss und der Teilhabe an der digitalen Wirtschaft gewinnen an Bedeutung, da Jugendliche aktiver mit den sozialen Medien+ arbeiten.

SCHLUSSFOLGERUNGEN

Die späte Adoleszenz stellt eine Herausforderung für die Sicherheit von Kindern im Internet dar und markiert den Übergang von der geschützten Lebensphase der Kindheit und Jugend zur Volljährigkeit. Die größte Herausforderung in diesem Alter besteht darin, ein Gleichgewicht zwischen der zunehmenden Autonomie Jugendlicher und fortgesetzten entwicklungsbedingter Vulnerabilität zu schaffen.

Ein weiteres wichtiges Thema ist das Entstehen einer Diskrepanz. Personen im Alter von 16 bis 18 Jahren werden trotz ihrer noch nicht abgeschlossenen Persönlichkeitsentwicklung häufig als vollständig autonome Nutzer behandelt. Dies macht deutlich, dass Regulierungsansätze erforderlich sind, die über starre Altersgrenzen hinausgehen und allmählichen Entwicklungsübergängen Rechnung tragen.

Für einen wirksamen Schutz in dieser Phase müssen nicht nur der Zugang und die Inhalte berücksichtigt werden, sondern auch die strukturellen Rahmenbedingungen, die das langfristige Verhalten prägen, einschließlich der Gestaltung sozialer Medien und anderer digitaler Dienste, algorithmischer Systeme und Datenpraktiken. Jugendliche sollten in dieser Phase der zunehmenden Autonomie bei der Entwicklung nachhaltiger und reflektierender Verfahren für die Nutzung sozialer Medien+, einschließlich Selbstregulation und kritischem Bewusstsein für das digitale Umfeld, unterstützt werden.

Die Risiken sind zunehmend kumulativ und werden eher von etablierten Gewohnheiten und strukturellen Einflüssen als von unmittelbaren entwicklungsbedingten Anfälligkeiten geprägt. Daher müssen Maßnahmen zum Schutz von Kindern im Internet auch auf diese Phase ausgedehnt werden, um den Übergang zur autonomen Teilhabe zu begleiten und gleichzeitig den anhaltenden entwicklungsbedingten Anfälligkeiten Rechnung zu tragen. Die Maßnahmen sollten die Entwicklung nachhaltiger Nutzungspraktiken fördern, die Jugendliche ins Erwachsenenalter führen.

EMPFEHLUNGEN (13-18 JAHRE)

Zunehmend eigenständige Nutzung altersgerechter sozialer Medien+ gewährleisten

Ab dem Alter von 13 Jahren können Jugendliche allmählich von der beaufsichtigten zu einer autonomen Nutzung sozialer Medien+ übergehen. Eltern und Betreuungspersonen, Lehrkräfte und Pädagogen spielen weiterhin eine wichtige Rolle bei der Begleitung der Online-Interaktionen Jugendlicher. Das Umfeld der Jugendlichen sollte weiterhin persönliche Interaktionen und Aktivitäten offline fördern, einschließlich eines ausreichenden Schlafs. In Bildungseinrichtungen sollte die Verwendung von Endgeräten einem festgelegten pädagogischen Zweck dienen.

Schlussfolgerung

In diesem Kapitel wurden die grundlegenden Merkmale und Risiken im Zusammenhang mit der Nutzung des Internets durch Kinder in drei Hauptphasen ihrer Entwicklung untersucht: in der frühen Kindheit (0-2 Jahre), der Kindheit (3-12 Jahre) und der Jugend (13-18 Jahre). Es wurden übergreifende Empfehlungen vorgelegt, um soziale Medien und andere Anbieter digitaler Dienste, Regulierungsbehörden, Betreuungspersonen und Pädagogen bei der Umsetzung eines altersgerechten Ansatzes zur Gewährleistung der Sicherheit von Kindern im Internet im Einklang mit ihren jeweiligen Befugnissen und Zuständigkeiten zu unterstützen.

Auf der Grundlage einer Analyse der verfügbaren Erkenntnisse über die Risiken für die Gesundheit und das Wohlbefinden von Minderjährigen in diesen Entwicklungsphasen wurde ein abgestufter Ansatz zur Steuerung der Online-Interaktionen von Kindern und Jugendlichen in drei Hauptphasen skizziert:

- // 0-2 Jahre: frühe Kindheit als besonders geschützte Entwicklungsphase,
- // 3-12 Jahre: Kindheit als beaufsichtigte Entwicklungsphase,
- // 13-18 Jahre: Jugend als Phase der sich entwickelnden Autonomie.

Die bestehenden Rahmen und Instrumente zur Sicherheit von Kindern im Internet werden in Kapitel 3 eingehender untersucht. In Kapitel 4 werden Maßnahmen vorgestellt, mit denen Minderjährige im digitalen Raum befähigt und ihr Umfeld in die Lage versetzt werden sollen, die Nutzung sozialer Medien+ durch Kinder und Jugendliche zu lenken. Im nächsten Kapitel werden die Online-Risiken für Kinder in verschiedenen Phasen ihrer Entwicklung eingehender untersucht, auch in Bezug auf verschiedene soziale und individuelle Faktoren.

02

Forschung zu Risiken, denen Minderjährige online ausgesetzt sind

Wie in Kapitel 1 angedeutet, kann die Sicherheit von Kindern im Internet nicht allein aus einer entwicklungsorientierten Perspektive betrachtet werden. Faktoren wie der sozioökonomische Hintergrund und das Geschlecht haben einen wichtigen Einfluss auf die Muster der Nutzung von Online-Angeboten durch Kinder und Jugendliche und ihre Vulnerabilität für damit verbundene Risiken⁶⁸. Auch Aspekte wie Sexualität, ethnische Herkunft, Religion, Migrationshintergrund und sonderpädagogische Bedürfnisse wirken sich auf die potenzielle Gefährdung Minderjähriger aus.

In diesem Kapitel wird das zweite der Sechs Leitprinzipien untersucht, die von den Ko-Vorsitzenden als Gerüst für die Steuerung von Maßnahmen vorgeschlagen wurden: Gleichstellung und Diversität. Es wird dargelegt, wie sich Ungleichheiten bei den Risiken und bei der Exposition gegenüber Online-Gefahren in verschiedenen Altersgruppen und sozioökonomischen Gruppen mit den Bedürfnissen Minderjähriger im Verlauf ihrer Entwicklung überschneiden. Außerdem wird eingeschätzt, inwieweit Minderjährige verschiedenen Online-Risiken (beispielsweise illegale Inhalte und schädliche Gestaltungsmerkmale sozialer Medien und anderer digitaler Dienste), die sich auf ihre körperliche und psychische Gesundheit auswirken, ausgesetzt sind.

Derzeit **gibt es deutlich mehr Evidenz (beispielsweise mit Schwerpunkt auf Cybermobbing und schädlichen Inhalten) für einen möglichen negativen Zusammenhang zwischen sozialen Medien und psychischer Gesundheit** als auf entsprechende positive Auswirkungen. Viele Anhaltspunkte für das Potenzial sozialer Medien, die Gesundheit und das Wohlbefinden von Minderjährigen zu schädigen, sind korrelativ und lassen keine kausalen Schlussfolgerungen zu. Sie reichen jedoch aus, um Maßnahmen zur Sicherheit von Minderjährigen im Internet zu rechtfertigen.

Trotz der Verfügbarkeit von Belegen in bestimmten Bereichen behindern einige Datenlücken eine umfassende Analyse, bei der soziale und individuelle Risikofaktoren aus entwicklungsorientierter Sicht berücksichtigt werden können. Ganz allgemein behindern mangelnde Transparenz und mangelnder Zugang zu Daten sozialer Medien die Erforschung der positiven und negativen Auswirkungen der Nutzung sozialer Medien durch Minderjährige⁶⁹.

Weitere Längsschnittstudien und europaweite Datensätze könnten dazu beitragen, die Folgen der Risiken, denen Kinder und Jugendliche in verschiedenen sozialen Medien+ ausgesetzt sind, besser zu verstehen. Alle eingehenden Untersuchungen zu Minderjährigen erfordern Sorgfalt in Bezug auf die Forschungsethik⁷⁰.

Zudem haben einige Aspekte in der öffentlichen Debatte zu Missverständnissen geführt. Ein Beispiel sind in sozialen Medien verbreitete Behauptungen zum „Brainrot“, die darauf hindeuten, dass eine übermäßige Nutzung sozialer Medien die Masse der „grauen Substanz“ im menschlichen Gehirn verringern kann⁷¹. Solche Aussagen sind zu stark verkürzt und medizinisch nicht belegt.

Das vorliegende Kapitel dient der Darstellung und Verdeutlichung der aktuellen Evidenzgrundlage. **Solide Erkenntnisse darüber, wie Risiken und Schäden mit verschiedenen digitalen Diensten – und nicht nur sozialen Medien – zusammenhängen, sind unerlässlich, um geeignete Maßnahmen** zum Schutz und zur Stärkung Minderjähriger online ergreifen zu können. Die Chancen für Kinder und Jugendliche in der digitalen Welt werden in Kapitel 4 untersucht.

Soziale und individuelle Risikofaktoren

GESCHLECHT UND SEXUALITÄT

Risiken für Mädchen und Jungen

Junge Frauen und Mädchen sind online in besonderem Maße einer ganzen Reihe geschlechtsspezifischer Gefahren ausgesetzt. Dazu gehören sexistisches und misogynes Mobbing und eine unverhältnismäßige Exposition gegenüber sexuellen Gefahren⁷², wie die nicht einvernehmliche Weitergabe intimer Bilder und sexuell expliziter Deepfakes online⁷³.

Ganz allgemein deuten Untersuchungen darauf hin, dass Mädchen häufiger Opfer von Cybermobbing werden als Jungen⁷⁴. Gemäß einer Studie haben 63 % der Mädchen in Europa in den sozialen Medien bereits eine Form von Belästigung online erlebt⁷⁵.

Es gibt Belege dafür, dass **sich die Schäden, denen junge Frauen und Mädchen online ausgesetzt sind, mit zunehmendem Alter weiterentwickeln**. Bei Mädchen im Alter von 13 bis 15 Jahren ist die Wahrscheinlichkeit größer, dass sie soziale Ausgrenzung in Form von Ausschluss aus Gruppenchats, Bodyshaming, Gerüchten und öffentlicher Demütigung erleben⁷⁶. Junge Frauen im Alter von 11 bis 18 Jahren könnten hingegen häufiger Opfer von sexualisiertem oder kontrollierendem Missbrauch, einschließlich Nötigung, Deepfakes und Grooming, werden. Zwar sind Mädchen in diesem Alter besonders gefährdet, doch auch Jungen sind diesen Gefahren ausgesetzt.

Die zunehmende Verbreitung künstlicher Intelligenz (KI) und ihre Integration in Online-Anwendungen und -Dienste verstärkt die Risiken⁷⁷. Beispielsweise können Deepfakes als Mittel zum Cybermobbing eingesetzt werden⁷⁸. Die Schaffung von Deepfakes, die auch für sexuellen Missbrauch online genutzt werden können, hat zugenommen⁷⁹. Deepfakes haben eine neue Dimension der Schädigung eingeführt, durch die nicht nur der Ruf einer Person geschädigt wird, sondern die, wie andere Cybermobbing-Handlungen auch, zu psychischen Traumata führen könnte.

Mädchen sind möglicherweise in stärkerem Maße Gefahren durch soziale Vergleiche online ausgesetzt und in stärkerem Maße gefährdet, ein negatives Bild ihres eigenen Körpers zu entwickeln⁸⁰. Untersuchungen deuten darauf hin, dass der von Gleichaltrigen ausgehende Gruppendruck in Bezug auf ein ideales Körperbild durch Online-Nutzung noch verstärkt werden könnte⁸¹.

Bei Mädchen ist die Gefahr des Anschlusses an eine Online-Gemeinschaft, die Essstörungen fördert, oder der Unterstützung einer solchen Gemeinschaft höher⁸². Belege zeigen einen Zusammenhang zwischen den Online-Interaktionen junger Mädchen zur Selbstdarstellung, einschließlich der Nutzung

sozialer Medien, und negativen Auswirkungen auf ihre psychische Gesundheit, darunter Depressionen und Angststörungen⁸³. Mädchen zwischen 10 und 12 Jahren können besonders gefährdet sein.

Im Allgemeinen verbringen Mädchen mehr Zeit in sozialen Medien und nutzen Online-Chat-Funktionen häufiger als Jungen⁸⁴. In einigen Studien wurde eine mäßige bis starke Nutzung digitaler Dienste bei Mädchen mit einer höheren Prävalenz psychischer Probleme und einem geringeren Wohlbefinden in Verbindung gebracht⁸⁵.

Jungen verbringen dagegen tendenziell mehr Zeit mit Online-Gaming. Eine Reihe von Studien hat gezeigt, dass Online-Gaming mit psychischen Problemen wie Depressionen und Angstzuständen in Verbindung stehen. Es kann jedoch ein stärkerer Zusammenhang zwischen der Nutzung sozialer Medien und psychischen Problemen bestehen als zwischen Online-Gaming und psychischen Problemen⁸⁶. Das Risiko sexueller Übergriffe ist für Jungen online höher als in der realen Welt. Ihre Anfälligkeit in diesen Umgebungen wird häufig unterschätzt⁸⁷.

Schließlich können Mädchen und Jungen auf unterschiedliche Weise mit Online-Gefahren konfrontiert sein. Im Falle von Cybermobbing nutzen junge Männer möglicherweise eher vermeidende Bewältigungsstrategien, da Normen junge Männer dazu ermutigen, Probleme selbst zu bewältigen, anstatt Hilfe durch ihr Umfeld zu suchen⁸⁸. Sowohl bei Mädchen als auch bei Jungen wird in Studien eine stärkere Nutzung sozialer Medien mit einer schlechteren psychischen Gesundheit und einem schlechteren psychischen Wohlbefinden in Verbindung gebracht⁸⁹.

LGBTIQ+-Gemeinschaften

Sexuell diverse Kinder und Jugendliche sind online häufiger Opfer von Hass⁹⁰ und Gewalt, einschließlich Cybermobbing⁹¹ und sexueller Belästigung⁹². Digitale Dienste können auch die Erfahrungen junger LGBTIQ+-Nutzer mit Grooming, sexuellen Übergriffen und dem Risiko, ohne ihre Zustimmung „geoutet“ zu werden, verstärken⁹³.

Auf der Bevölkerungsebene geben 63 % der Menschen, die LGBTIQ+-Gemeinschaften angehören, an, online bereits mit gewalttätigen Inhalten und Desinformationen, die sich gegen LGBTIQ+-Gemeinschaften richten, konfrontiert gewesen zu sein⁹⁴. Es gibt Hinweise darauf, dass Jugendliche, die LGBTIQ+-Gemeinschaften angehören, möglicherweise mit größerer Wahrscheinlichkeit Online-Räume nutzen, um online ihre Sexualität und Identität zu erkunden, nach Informationen über die sexuelle Gesundheit zu suchen oder Unterstützung und Vernetzung Gleichaltriger zu suchen, ohne sich „persönlichen“ Risiken auszusetzen⁹⁵.

Dies kann online für LGBTIQ+-Kinder und -Jugendliche die Exposition gegenüber Risiken und Gefahren erhöhen. Trotz vieler Argumente für das Potenzial von Online-Räumen, sexuell diversen Kindern und Jugendlichen die Möglichkeit zu bieten, sich zu vernetzen und Unterstützung durch Gleichaltrige zu erhalten, gibt es Hinweise darauf, dass persönliche Interaktionen als Angebot von Unterstützung nach wie vor wirksamer sein können als Online-Interaktionen⁹⁶.

SOZIOÖKONOMISCHER HINTERGRUND

Bei Jugendlichen aus benachteiligten sozioökonomischen Verhältnissen ist die Wahrscheinlichkeit höher, online mit negativen Erfahrungen konfrontiert zu werden, darunter Cybermobbing⁹⁷, übermäßige Nutzung von Technik, Social-Media-Sucht⁹⁸ und problematische Nutzung⁹⁹. Auch sozioökonomische Faktoren, einschließlich eines geringeren Familieneinkommens, können die Prävalenz schädlicher Online-Erfahrungen bei Kindern und Jugendlichen erhöhen¹⁰⁰.

Der familiäre Hintergrund hat erheblichen Einfluss darauf, inwieweit Minderjährige Online-Gefahren ausgesetzt sind. Kinder und Jugendliche, deren Eltern über geringe digitale Medienkompetenz verfügen, können online größeren Gefahren ausgesetzt sein¹⁰¹. Es gibt Hinweise darauf, dass Minderjährige aus benachteiligten sozioökonomischen Verhältnissen tendenziell über ein geringeres Maß an digitalen Kompetenzen verfügen, die es ihnen ermöglichen würden, sich online sicher zurechtzufinden, und online möglicherweise ein riskanteres Verhalten zeigen¹⁰².

Wohlhabendere Familien hingegen verfügen möglicherweise über bessere Mittel und Ressourcen, um den Umgang ihrer Kinder und Jugendlichen mit digitalen Technologien positiv zu gestalten¹⁰³ und negative Auswirkungen anzugehen. Auf diese Weise kann die problematische Nutzung digitaler Dienste, einschließlich sozialer Medien, bestehende Ungleichheiten hinsichtlich der Gesundheit von Jugendlichen und jungen Erwachsenen, ihrer Teilhabe an Bildungsangeboten und ihren Leistungen verstärken.

Zwar hat das Leben in einem städtischen oder ländlichen Gebiet möglicherweise keinen direkten Einfluss auf die Exposition Minderjähriger gegenüber Online-Gefahren, doch ist es bei in ländlichen Gebieten lebenden Kindern und Jugendlichen möglicherweise wahrscheinlicher, dass sie vermeidende Bewältigungsstrategien einsetzen, die enger mit negativen Auswirkungen auf die psychische Gesundheit verbunden sind. Dies macht deutlich, dass Programme entwickelt werden müssen, mit denen soziale Ungleichheiten, auch in ländlichen und unterversorgten Gebieten, angegangen werden, um die Wahrscheinlichkeit zu verringern, dass Minderjährige online Schaden erleiden¹⁰⁴.

ETHNISCHE HERKUNFT, RELIGION UND MIGRATIONSHINTERGRUND

Bei Jugendlichen, die ethnischen Minderheiten angehören, ist die Wahrscheinlichkeit höher, dass sie Online-Gefahren wie Cybermobbing, rassistische Diskriminierung und Belästigung erleben¹⁰⁵. In Europa erhobene Belege zeigen, dass Hetze im Internet häufig gegen Menschen aufgrund ihrer ethnischen Herkunft, Religion, Staatsangehörigkeit oder ihres Migrationshintergrunds gerichtet ist, wobei Schwarze, Roma, Juden und Muslime zu den am häufigsten betroffenen Gruppen gehören¹⁰⁶. Darüber hinaus gehören Rassismus, religiöser Hass, Hass aufgrund der sexuellen Orientierung und Sexismus zu den häufigsten Formen von Hassrede, die online zu finden sind¹⁰⁷.

Hinweise aus der Europäischen Union deuten ferner darauf hin, dass diese Online-Erfahrungen umfassendere Diskriminierungsmuster widerspiegeln, von denen Minderheitengemeinschaften betroffen sind. Nach Angaben der Agentur der Europäischen Union für Grundrechte (FRA) gab fast die Hälfte (47 %) der in 13 EU-Mitgliedstaaten befragten Muslime an, in den letzten fünf Jahren rassistische Diskriminierung erfahren zu haben. Dazu gehören Belästigung und Diskriminierung in den Bereichen Bildung, Beschäftigung und öffentlicher Raum. Viele berichteten auch, online antimuslimischer Feindseligkeit ausgesetzt zu sein¹⁰⁸. Parallel dazu ergab die Umfrage der FRA unter Menschen afrikanischer Abstammung, dass fast die Hälfte der Befragten rassistische Diskriminierung erfahren hatte, wobei Online-Umgebungen als wichtiges Umfeld genannt wurden, in dem rassistische Übergriffe stattfinden¹⁰⁹.

Es scheint eine zunehmende Normalisierung und Verharmlosung von Hassrede im Internet zu geben. Die Europäische Kommission gegen Rassismus und Intoleranz (ECRI) des Europarats hat auf eine Zunahme von Hassrede in ganz Europa hingewiesen. Sie stellt fest, dass ethnische Herkunft und Religion zu den häufigsten Risikofaktoren für Hass online gehören, und warnt, dass sich fremdenfeindliche, antimuslimische, antisemitische und gegen Schwarze gerichtete Rhetorik in digitalen Räumen zunehmend normalisiert hat¹¹⁰.

Darüber hinaus gibt es auf der Bevölkerungsebene Hinweise dafür, dass Menschen, die Minderheiten angehören, unverhältnismäßig stark von Beschränkungen und Entfernungmaßnahmen in Systemen zur

Moderation von Inhalten betroffen sein könnten, was auf Verzerrungen in den in diesen Systemen verwendeten Algorithmen zurückzuführen ist¹¹¹. Dies spiegelt allgemeinere Bedenken hinsichtlich ethnischer und geschlechtsspezifischer Verzerrungen in Spracherkennungs- und Vorhersagemodellen wider, die von Anbietern digitaler Dienste zum automatischen Scannen auf schädliche Online-Inhalte verwendet werden¹¹².

KINDER MIT SONDERPÄDAGOGISCHEM FÖRDERBEDARF

Es gibt Hinweise darauf, dass junge Menschen mit sonderpädagogischem Förderbedarf und Behinderungen mit höherer Wahrscheinlichkeit online eine Schädigung erfahren¹¹³, beispielsweise durch Hetze, Cybermobbing, Cyberbedrohungen, Belästigung, Exposition gegenüber sexuellen Inhalten und Online-Grooming¹¹⁴.

Faktoren wie Kommunikationshindernisse und emotionale Kompetenz können die bestehende Anfälligkeit von Kindern und Jugendlichen mit Behinderungen in Online-Räumen verstärken¹¹⁵. Soziale Isolation und das Gefühl der Verletzlichkeit von Minderjährigen mit Behinderungen erhöhen das Risiko einer Viktimisierung erheblich¹¹⁶.

Es gibt Hinweise darauf, dass sich Kinder und Jugendliche mit Behinderungen möglicherweise wohler fühlen, wenn sie sich in Online-Räumen ausdrücken¹¹⁷. Darüber hinaus sind Minderjährige mit Behinderungen häufiger online, um ihre Interessen und Hobbys zu teilen, mit anderen zu spielen und nach Gesundheitsinformationen und emotionaler Unterstützung zu suchen, obwohl sie stärker gefährdet sind, online Schaden zu erleiden¹¹⁸.

Ebenso deuten Untersuchungen darauf hin, dass Kinder und Jugendliche mit neurologischen Entwicklungsstörungen, einschließlich Aufmerksamkeitsdefizit-/Hyperaktivitätsstörung (ADHS), in stärkerem Maße einer problematischen Online-Nutzung ausgesetzt sind¹¹⁹. Darüber hinaus werden Minderjährige mit den Merkmalen einer Autismus-Spektrum-Störung, einer intellektuellen oder entwicklungsbezogenen Störung mit zunehmender Wahrscheinlichkeit Ziel von Online-Mobbing¹²⁰. Eine längere Bildschirmzeit kann auch mit erhöhten ADHS-Symptomen einhergehen¹²¹.

Es sei darauf hingewiesen, dass sich online soziale und individuelle Risikofaktoren für Kinder und Jugendliche überschneiden. So kann es beispielsweise bei Minderjährigen mit Behinderungen wahrscheinlicher sein, dass sie Hassrede im Internet erleben, die sich auf ihr Geschlecht, ihre Sexualität, ihre ethnische Herkunft oder ihre Religion bezieht¹²². Dies zeigt, dass bei der Gestaltung von Maßnahmen zur Förderung der Sicherheit von Kindern im Internet das Zusammenspiel verschiedener sozialer und individueller Faktoren und die davon ausgehende erhöhte Gefährdung bestimmter sozialer Gruppen berücksichtigt werden muss.

RISIKEN FÜR DIE PSYCHISCHE GESUNDHEIT

Daten der Weltgesundheitsorganisation zufolge leidet weltweit jeder Siebte im Alter zwischen 10 und 19 Jahren an einer psychischen Erkrankung¹²³. Auf europäischer Ebene ergab die Eurobarometer-Umfrage 2023 zur psychischen Gesundheit, dass 59 % der jungen Menschen ein emotionales oder psychosoziales Problem hatten, beispielsweise das Empfinden einer Depression oder Angststörung¹²⁴.

Bei Jugendlichen gehören Depressionen, Ängste und Verhaltensstörungen zu den häufigsten Krankheitsursachen¹²⁵. Weltweit ist Suizid eine der häufigsten Todesursachen bei jungen Menschen¹²⁶ (siehe unten: Vorsätzliche Selbstverletzung und Suizidalität). Auf der Ebene der Bevölkerung sind schutzbedürftige

Gruppen, darunter Menschen, die LGBTQ+-Gemeinschaften angehören, und Menschen mit Migrations- oder Fluchthintergrund am stärksten gefährdet¹²⁷.

Es gibt Hinweise darauf, dass Mädchen besonders anfällig sind, beispielsweise für einen auf dem äußeren Erscheinungsbild beruhenden Vergleich und eine plattformgestützte soziale Bewertung. Für viele Minderjährige stellt das Alter von 10 bis 12 Jahren eine frühe Phase internalisierender Probleme dar, beispielsweise in Form von Angstsymptomen und depressiven Symptomen. Psychische Probleme können bis ins Jugendalter hinein andauern, in dem die Vulnerabilität ihren Höhepunkt erreicht, wenn die zugrunde liegenden Mechanismen nicht angegangen werden.

Psychische Probleme haben nicht nur schwerwiegende direkte Folgen für das Wohlbefinden und die Entwicklung von Kindern und Jugendlichen, sie wirken sich auch auf den Schulbesuch und die schulischen Leistungen von Minderjährigen und im späteren Leben auf ihre Beschäftigungsfähigkeit aus¹²⁸. Die Daten deuten auf weitreichende Auswirkungen der Nutzung digitaler Dienste, insbesondere sozialer Medien, auf die Gesundheit und Entwicklung von Kindern und Jugendlichen hin.

In einer Studie wurde darauf hingewiesen, dass eine übermäßige Nutzung sozialer Medien über mehr als drei Stunden pro Tag mit negativen Folgen für die psychische Gesundheit, insbesondere Depressionen und Ängsten, in Verbindung gebracht werden kann¹²⁹. Ebenso zeigten die Ergebnisse der PISA-Studie 2022, die 22 EU-Mitgliedstaaten abdeckte, dass die geschätzte Wahrscheinlichkeit, dass 15-Jährige eine beeinträchtigte psychische Gesundheit aufweisen, mit der Dauer, die sie online verbringen, zunimmt¹³⁰.

HINWEISE AUF EINEN BIDIREKTIONALEN ZUSAMMENHANG ZWISCHEN PSYCHISCHEN PROBLEMEN UND DER NUTZUNG DIGITALER DIENSTE

Der Zusammenhang zwischen der Interaktion von Kindern und Jugendlichen mit der Welt der sozialen Medien+ und psychischen Problemen ist komplex. Was die sozialen Medien betrifft, so deuten Hinweise auf einen bidirektionalen Zusammenhang zwischen den Online-Interaktionen Minderjähriger und der Prävalenz psychischer Probleme hin¹³¹. Dies bedeutet, dass die Interaktionen von Kindern und Jugendlichen mit Online-Räumen psychische Probleme, einschließlich Depressionen, verursachen, sie aber auch verstärken können¹³².

Die vorliegenden Hinweise stützen die Annahme, dass negative Online-Erfahrungen bei Jugendlichen, die bereits mit psychischen Problemen zu kämpfen haben, weit verbreitet sind¹³³. Jugendliche mit sozialen Ängsten sind möglicherweise besonders geneigt, mehr Zeit in den sozialen Medien zu verbringen oder problematische Nutzungsmuster zu entwickeln¹³⁴. Sozial ängstliche Personen wenden sich mitunter sozialen Medien zu, um positive Online-Beziehungen aufzubauen, die Ängste vor persönlichen Interaktionen verringern, wodurch jedoch Vermeidungsverhalten gefördert werden.

Ebenso dürfte die Exposition Minderjähriger gegenüber für ihr Alter ungeeigneten Inhalten, einschließlich Inhalten, die körperliche Selbstverletzung, Essstörungen und Suizid darstellen oder fördern, bereits bestehende Erkrankungen verschärfen.

Für Jugendliche in sozialen Medien kann die Qualität von Offline-Netzwerken und Persönlichkeitsmerkmalen, einschließlich Introversion oder Extroversion, als Schutz- oder Risikofaktor wirken. Untersuchungen deuten darauf hin, dass die Nutzung sozialer Medien durch extrovertierte Jugendliche mit gutem Selbstwertgefühl und hochwertigen Offline-Freundschaften die Offline-Beziehungen stärken und die Unterstützung online erhöhen kann.

Introvertierte Jugendliche mit geringem Selbstwertgefühl und schwächeren sozialen Offline-Netzwerken könnten hingegen eher geneigt sein, online neue Freunde zu suchen. Dies kann das potenzielle Risiko einer Exposition gegenüber unerwünschtem Kontakt oder unerwünschten Inhalten erhöhen¹³⁵.

Die jüngsten technologischen Fortschritte haben den Einsatz von generativer KI, Chatbots auf Basis großer Sprachmodelle und „KI-Begleiter“ durch Kinder und Jugendliche beschleunigt. Dieser Wandel geht mit wachsender Besorgnis über die Auswirkungen dieser Technologien auf die psychische Gesundheit und das Wohlbefinden von Minderjährigen einher. Aus diesem Grund haben sich die Ko-Vorsitzenden in diesem Bericht für den weit gefassten Begriff „soziale Medien+“ entschieden.

Im Gegensatz zu älteren digitalen Tools im Bereich der psychischen Gesundheit, darunter Apps und virtuelle Realität, die oftmals eher sporadisch genutzt wurden, werden KI-Chatbots bereits von Millionen Kindern und Jugendlichen eingesetzt, um Informationen (auch zu Fragen der psychischen Gesundheit), Interaktion und emotionale Unterstützung zu suchen. Einige erste Hinweise deuten auf Vorteile hin, z. B. das Potenzial von KI-Gesprächsagenten, zur Verringerung der Symptome von Depressionen beizutragen¹³⁶.

Forschungsergebnisse deuten zudem auf den potenziellen Nutzen KI-gestützter Oberflächen für die inklusive Bildung von Schülerinnen und Schülern mit Sehstörungen oder körperlichen und kognitiven Behinderungen hin¹³⁷. Die Auswirkungen von KI-Instrumenten auf die Bildung und Kompetenzentwicklung von Minderjährigen müssen jedoch umfassender analysiert werden, um die potenziellen Vorteile und Risiken zu verstehen¹³⁸.

„Die verschiedenen Technologien müssen umfassender und genauer betrachtet werden. ... Die ausschließliche Konzentration auf soziale Medien ist viel zu eng, da andere Technologien wie generative KI ein vergleichbares, wenn nicht sogar höheres Risiko für Minderjährige darstellen.“

– JUDITH SIMON,

PROFESSORIN FÜR ETHIK IN DER
INFORMATIONSTECHNOLOGIE,
UNIVERSITÄT HAMBURG

KI-TOOLS UND KI-BEGLEITER IN DEN SOZIALEN MEDIEN+

Hinsichtlich der Signale werden in der Medienberichterstattung und in der frühen Forschung zu den Möglichkeiten von KI-assoziierten „psychotischen“ Symptomen parasoziale Bindung, Abhängigkeitsmuster¹³⁹ und Anstiftung zu Suizid¹⁴⁰ genannt. Es gibt Hinweise darauf, dass Minderjährige „KI-Begleiter“ oft als menschenähnlich wahrnehmen¹⁴¹. Sie können jedoch keine echte empathische Unterstützung bieten und stellen möglicherweise ein Risiko für die psychische Gesundheit von Minderjährigen dar¹⁴².

Kleinkinder können besonders anfällig für den Aufbau emotionaler Bindungen zu KI-Begleitern sein, weil sie diese möglicherweise als mitfühlende Begleiter verstehen. Jugendliche, die diese Tools für den persönlichen und emotionalen Austausch nutzen, sind ebenfalls Risiken wie dem Aufbau einer Bindung und Abhängigkeit ausgesetzt.

Aus einer aktuellen europäischen Studie geht hervor, dass mehr als 86 % der irischen, französischen, deutschen und schwedischen Teenager KI-Tools nutzen. Mehr als die Hälfte von ihnen nutzt KI-Tools, um intime Themen zu erörtern und persönliche Probleme zu lösen¹⁴³. Diese Studie ergab auch, dass Jugendliche, die KI-Tools nutzen, eher an Angstsymptomen leiden.

KI-Systeme können die Anfälligkeit Minderjähriger ausnutzen, indem sie ihre natürliche Neugier, ihren Wunsch nach Belohnung, ihre Anfälligkeit für sozialen Druck und ihre Neigung zur sofortigen Gratifikation missbrauchen. Sie können auch die Auswirkungen manipulativer Gestaltungstechniken wie der Verhaltensbeeinflussung („Nudging“) verschärfen ¹⁴⁴.

Algorithmische und gesellschaftliche Verzerrungen (Biases), die in KI-Trainingsdaten eingebettet sind, können auch Desinformation, Fehlinformationen und Stereotype fördern, die Minderjährige ab einem frühen Alter verinnerlichen können¹⁴⁵. Die Folgen einer KI-gestützten Instrumentalisierung können für Kinder und Jugendliche schwerwiegend und langanhaltend sein, darunter Suchtverhalten, eine Verschlechterung des Konzentrationsvermögens und der kognitiven Fähigkeiten, schlechte schulische Leistungen und soziale Schwierigkeiten.

Kinder im Alter von 6 bis 12 Jahren können in besonderem Maße der Entwicklung eines frühen Suchtverhaltens ausgesetzt sein, das bis ins frühe Jugendalter und darüber hinaus andauern kann. Es sind weitere Forschungsarbeiten erforderlich, nicht nur zu den Möglichkeiten, die KI-Tools Kindern und Jugendlichen bieten, sondern auch, um zu verstehen, wie Schäden erkannt werden können und wie sichergestellt werden kann, dass die menschliche Aufsicht ein wesentlicher Bestandteil der KI-vermittelten Unterstützung bleibt.

Darüber hinaus sind KI-gestützte Funktionen (z. B. in Spielumgebungen, einschließlich KI-gestützter Charaktere, personalisierter Erstellung von Inhalten und In-Game-Chatbots) im bestehenden Rechtsrahmen nicht ausreichend berücksichtigt, um einen adäquaten Schutz Minderjähriger im Internet sicherstellen zu können¹⁴⁶.

EINSAMKEIT ALS URSACHE ODER FOLGE DER NUTZUNG SOZIALER MEDIEN

Bei Kindern und Jugendlichen kann Einsamkeit eine Ursache oder Folge der Nutzung sozialer Medien sein¹⁴⁷. In Fällen, in denen Einsamkeit als Ursache angesehen werden kann, kann das Gefühl der Isolation dazu beitragen, dass zum Aufbau neuer Freundschaften verstärkt soziale Medien¹⁴⁸ genutzt werden. Das Empfinden von Einsamkeit im realen Leben kann auch Verhaltensweisen wie unrealistische Selbstdarstellungen online stärken, die wiederum das Empfinden von Einsamkeit verschärfen können¹⁴⁹.

Generell kann das Erleben von Online-Gefahren Minderjährige dazu veranlassen, sich von sozialen Aktivitäten und aus dem Schulbetrieb zurückzuziehen, das Vertrauen in andere zu verlieren und zögerlicher zu sein, wenn es um die Aufnahme von Online-Aktivitäten zur Förderung des Wohlbefindens (z. B. die Pflege von Kontakten zu Freunden oder die Nutzung von Diensten) geht¹⁵⁰. Es ist wichtig anzuerkennen, dass sich Online-Gefahren, einschließlich Cybermobbing, häufig mit Schäden in der physischen Welt überschneiden.

PASSIVE UND AKTIVE NUTZUNG

Die Gestaltung sozialer Medien+ hat ebenfalls großen Einfluss darauf, wie sich diese Dienste auf die psychische Gesundheit von Kindern und Jugendlichen auswirken. Automatisierte Pfade, die für kommerzielle Ziele optimiert sind, können dazu führen, dass Minderjährige anscheinend endlos mit schädlichen Inhalten versorgt werden, von expliziten Darstellungen von Selbstverletzungen, Essstörungen bis hin zu sexuellen Bilddarstellungen¹⁵¹.

Untersuchungen zeigen, dass die Art und Weise des Umgangs von Kindern und Jugendlichen mit sozialen Medien deren mögliche Auswirkungen auf ihre psychische Gesundheit und ihr Wohlbefinden beeinflusst. Die passive Nutzung wie Browsen und Scrollen kann mit einem höheren Maß an depressiven Symptomen, Einsamkeit und Stress in Verbindung gebracht werden¹⁵².

Unterdessen korreliert eine aktive Nutzung wie das Posten, das Veröffentlichen von Kommentaren, Messaging und Liken tendenziell mit einem höheren Wohlbefinden, einer höheren Lebenszufriedenheit (insbesondere bei Mädchen) und einer verstärkten Wahrnehmung sozialer Unterstützung. Einige Ergebnisse bieten jedoch ein gemischtes Bild in Bezug auf die aktive und passive Nutzung und die Häufigkeit von Depressionen¹⁵³.

KÖRPERBILDPROBLEME UND ESSVERHALTEN

Plattformen der sozialen Medien öffnen Kindern und Jugendlichen den Zugang zu einem breiten Spektrum von Inhalten im Zusammenhang mit Essverhalten, die sowohl gesunde als auch ungesunde Praktiken umfassen. Kanäle, die Essstörungen fördern, geben Anlass zu großer Sorge und haben das Potenzial, dysfunktionales Essverhalten zu fördern, die die Genesung behindern¹⁵⁴.

Solche Kanäle können dynamische Hashtags verwenden, damit sie durch Plattformen der sozialen Medien nicht erkannt und blockiert werden, und beispielsweise Dünnsein, ein geringes Selbstwertgefühl oder Perfektionismus propagieren. Diese Phänomene stehen im Zusammenhang mit Essstörungen, von denen insbesondere weibliche Teenager¹⁵⁵ ab dem Alter von 10 Jahren betroffen sind.

Die weite Verbreitung und Normalisierung von bildlichen Darstellungen „perfekter Körper“ und eines „Schlankheitsideals“, häufig durch fotozentrische Aktivitäten in sozialen Medien, kann weiter zur Unzufriedenheit von Kindern und Jugendlichen mit ihrem körperlichen Erscheinungsbild und zu Bodyshaming beitragen.

Diese Exposition kann zu erhöhter Selbstobjektivierung, Bedenken hinsichtlich des Körperbildes und sogar dem Wunsch nach kosmetischer Chirurgie führen. Jugendliche, insbesondere Mädchen im Teenageralter, sind einem besonderen Risiko ausgesetzt, eine negative Wahrnehmung ihres Körperbildes zu entwickeln, die durch die Darstellung idealisierter Körperstandards in den sozialen Medien verfestigt wird¹⁵⁶.

DESINFORMATION UND FEHLINFORMATIONEN (etc.)

Minderjährige neigen dazu, soziale Medien und Online-Plattformen als Nachrichten- und Informationsquellen gegenüber traditionellen Medien zu bevorzugen¹⁵⁷. Dieses Nutzungsverhalten setzt sie online einem breiten Spektrum von Desinformation und Fehlinformation aus.

Etwa die Hälfte der Achtjährigen gibt an, wöchentlich auf Fehlinformation zu stoßen¹⁵⁸. Je älter die Kinder sind, desto häufiger berichten sie davon, mit Fehlinformation konfrontiert worden zu sein¹⁵⁹. Eine Umfrage in den Vereinigten Staaten ergab, dass mehr als ein Drittel der Jugendlichen durch gefälschte Online-Inhalte irreführt wurde¹⁶⁰.

Kinder und Jugendliche kennen die Begriffe „Desinformation“ und „Fehlinformation“ möglicherweise gar nicht, was dazu führt, dass sie zu selten von entsprechenden Fällen berichten und es ihnen an Bewusstsein für die damit verbundenen Risiken mangelt. Dies verdeutlicht die Kluft zwischen den kognitiven und emotionalen Fähigkeiten von Kindern und den Risiken, denen sie online ausgesetzt sind. Etwa 70 % der jungen Menschen in der EU gaben an, dass sie Desinformation im Internet zuverlässig erkennen könnten¹⁶¹, doch sind ihre Antworten von ihrem Verständnis des Begriffs „Desinformation“ und von anderen Faktoren (z. B. Geschlecht, sozioökonomischer Hintergrund usw.) beeinflusst.

Mit dem Aufkommen immer ausgefeilterer Technologien, die in der Lage sind, Fehlinformation und Desinformation zu erzeugen und zu verbreiten, einschließlich KI-Tools¹⁶², wird es für Nutzer, insbesondere Minderjährige, immer schwieriger, unzuverlässige von zuverlässigen Informationen zu unterscheiden.

Minderjährige können nicht nur durch Fehlinformation und Desinformation unmittelbar geschädigt werden, sondern sie können diese auch unter ihren Altersgenossen¹⁶³ verbreiten, um beispielsweise Beliebtheit zu erlangen oder Bestätigung zu erfahren¹⁶⁴. Ein besonders besorgniserregender Trend ist die zunehmende Nutzung sozialer Medien durch Jugendliche, um nach Informationen über persönliche und (psychische) Gesundheitsprobleme zu suchen, obwohl Falschinformationen zu diesen Themen online weitverbreitet sind¹⁶⁵.

Eine Medienuntersuchung im Jahr 2021 ergab, dass in den ersten 35 Minuten der Nutzung einer Plattform der sozialen Medien fast 90 % der Nutzerinnen und Nutzer Fehlinformationen über COVID-19-Impfstoffe angezeigt wurden¹⁶⁶. Diese Ergebnisse unterstreichen die Notwendigkeit von Schutzmaßnahmen zur Begrenzung der Verbreitung von Fehlinformationen und Desinformation online.

In den Risikobewertungs- und Risikominderungszyklen sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen im Rahmen des Gesetzes über digitale Dienste der EU wiesen sowohl Anbieter als auch die Zivilgesellschaft auf systemische Risiken für die öffentliche

Gesundheit hin, die sich aus der großflächigen Verbreitung von Desinformation und Fehlinformationen zu medizinischen Themen ergeben. Anbieter von Online-Marktplätzen wiesen zudem auf systemische Risiken hin, die mit dem Verkauf legaler, aber schädlicher Stoffe und illegaler, nicht konformer oder unregulierter Medizinprodukte auf ihren Marktplätzen zusammenhängen. Auch Inhalte im Zusammenhang mit Selbstverletzung, Essstörungen und gesundheitlich riskanten Praktiken geben Anlass zur Sorge.

Dies unterstreicht, wie wichtig es ist, Kindern und Jugendlichen, aber auch Betreuungspersonen und Pädagogen frühzeitig digitale Fähigkeiten und Kompetenzen zu vermitteln. Öffentliche Dienste, einschließlich im Gesundheitswesen, sollten darüber nachdenken, wie Kindern, Jugendlichen und Betreuungspersonen online genaue und altersgerechte Informationen und Hinweise zu psychischen, körperlichen, sexuellen und anderen Gesundheitsfragen zugänglich¹⁶⁷ gemacht werden können.

VORSÄTZLICHE SELBSTVERLETZUNG UND SUIZIDALITÄT

Die Prävalenz von selbstverletzendem Verhalten bei Jugendlichen ist aufgrund begrenzter Daten über Krankenhausaufenthalte schwer zu ermitteln, es gibt jedoch Hinweise auf eine Zunahme entsprechender Fälle¹⁶⁸. Die Weltgesundheitsorganisation (WHO) nennt Suizid als dritthäufigste Todesursache bei 15- bis 29-Jährigen weltweit im Jahr 2021, wobei Frauen in dieser Altersgruppe besonders gefährdet sind¹⁶⁹.

Die Nutzung sozialer Medien+ für den Zugang zu und die Weitergabe von Inhalten über selbstverletzendes Verhalten ist ein gesellschaftliches Problem. Solche Aktivitäten tragen zur Normalisierung und Desensibilisierung für Verhaltensweisen der Selbstverletzung bei. Untersuchungen deuten darauf hin, dass die Exposition gegenüber Inhalten mit Selbstverletzungs- oder Suizidbezug in sozialen Medien zu sogenannten „Ansteckungseffekten“ oder „Werther-Effekten“ führen kann¹⁷⁰. Die Auseinandersetzung mit Inhalten in sozialen Medien, in denen Suizid und Selbstverletzung thematisiert werden, kann durch algorithmische Verstärkung auch die Wahrscheinlichkeit erhöhen, dass zukünftig verwandte Inhalte angesehen werden¹⁷¹.

Jugendliche können Selbstverletzungsinhalte in sozialen Medien posten, um ein Zugehörigkeitsgefühl zu entwickeln oder um Validierung oder Unterstützung zu erlangen. Allerdings können die Rückmeldungen, die sie erhalten, schwer zu verarbeiten sein. Sie könnten zwar positive Unterstützung erhalten, aber auch unbeabsichtigt selbstverletzende oder suizidale Verhaltensweisen verstärken¹⁷². Der Zusammenhang zwischen dem Einfluss sozialer Medien und Suizidalität ist komplex und umfasst indirekte und vielschichtige Zusammenhänge [siehe Kasten zum Fall „White Tiger“].

Die Online-Viktimisierung, einschließlich Cybermobbing, und ihr Potenzial, das Gefühl der Isolation bei Kindern und Jugendlichen zu verstärken, werden mit einem zunehmenden Auftreten von Fällen vorsätzlicher Selbstverletzung und Suizidgedanken in Verbindung gebracht¹⁷³. In diesem Zusammenhang muss die Rolle der sozialen Medien+ sorgfältig abgewogen werden, um negative Auswirkungen zu mindern und schutzbedürftige Kinder und Jugendliche sowie deren unterstützendes Umfeld wirksam zu fördern.

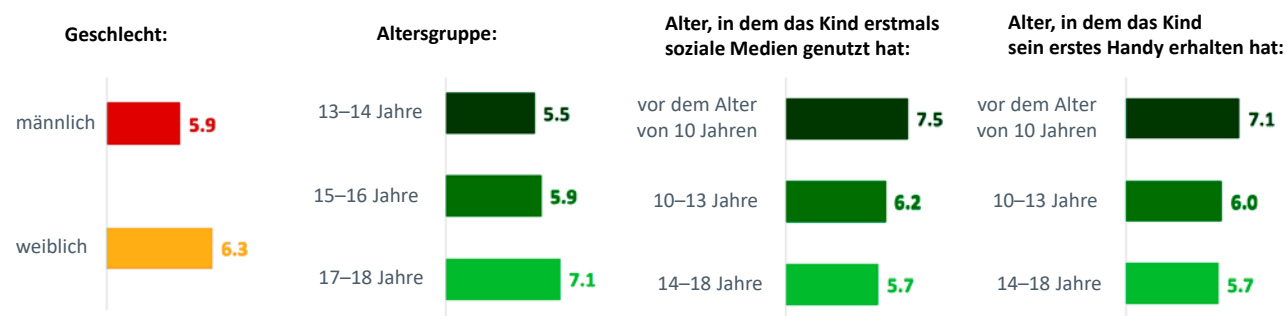
Risiken für die körperliche Gesundheit

Die meisten körperlichen Auswirkungen sozialer Medien und anderer digitaler Dienste auf die Gesundheit hängen mit der Bildschirmnutzung durch Minderjährige im Allgemeinen und nicht mit bestimmten Arten der Nutzung, beispielsweise von sozialen Medien, zusammen. Ähnlich wie die sozialen Medien hat auch Bildschirmzeit nicht unbedingt nur negative Auswirkungen, was jedoch stark von der konkreten Aktivität abhängt. Zu den wichtigsten Forschungsthemen in diesem Bereich gehören die Auswirkungen der Bildschirmzeit auf das Sehvermögen von Kindern und Jugendlichen, die Entwicklung des Gehirns, Alkoholkonsum und Schlaf ¹⁷⁴.

Aus Eurobarometer-Daten zu den Auswirkungen übermäßiger Bildschirmzeit und übermäßiger Aktivitäten in sozialen Medien auf die psychische Gesundheit junger Menschen geht hervor, dass 13- bis 18-Jährige an einem typischen Schultag durchschnittlich 4,5 Stunden vor Bildschirmen verbringen. An Wochenenden steigt dieser Wert auf durchschnittlich 6,1 Stunden pro Tag, wobei fast die Hälfte der Jugendlichen (46 %) mehr als sechs Stunden vor dem Bildschirm verbringt. 14 % der Jugendlichen verbringen an Wochenenden mehr als 10 Stunden täglich vor dem Bildschirm.

Abbildung 1: Erhöhte Bildschirmnutzung durch Jugendliche am Wochenende

Frage: Wie viel Zeit verbringst du insgesamt vor einem Bildschirm (Smartphone, Computer, Tablet, Fernsehen, Spielkonsole)?^a



Quelle: Europäische Kommission (2026), Auswirkungen übermäßiger Bildschirmzeit und sozialer Medien auf die psychische Gesundheit junger Menschen – Juni 2026 – Eurobarometer-Umfrage.

a. Anmerkung: Die Zahlen geben die durchschnittliche Dauer der Bildschirmnutzung pro Tag (in Stunden am Wochenende) an..

SEHVERMÖGEN UND

KÖRPERLICHE GESUNDHEIT

Eine längere Bildschirmnutzung erhöht anerkanntermaßen das Risiko von Rückenschmerzen, Kopfschmerzen¹⁷⁵ und digitaler Überbeanspruchung der Augen (auch als „Computer-Vision-Syndrom“ bezeichnet). Das Risiko, an diesen Symptomen zu erkranken, steigt mit langer Bildschirmzeit, unkorrigiertem Sehvermögen, kleiner Schrift, geringer Auflösung, ungünstiger Bildschirmhöhe oder -entfernung und unzureichender Beleuchtung¹⁷⁶.

Kinder sind besonders anfällig für Sehstörungen, die durch längere Bildschirmzeit verursacht werden, da viele von ihnen nicht diagnostizierte Sehstörungen haben oder ihre Augen nicht fachgerecht untersucht werden¹⁷⁷.

Wenn Kinder und Jugendliche übermäßig viel Zeit in den sozialen Medien+ verbringen, kann dies auch zu Opportunitätskosten führen, weil sie dann nicht in der Lage sind, sich an Offline-Aktivitäten, einschließlich körperlicher Aktivität und Offline-Spielen, zu beteiligen, die für ihre Entwicklung und Gesundheit von entscheidender Bedeutung sind.

SCHLAF

Weitere häufige physische Gesundheitsrisiken bei der Nutzung sozialer Medien sind eine verminderte körperliche Aktivität, weniger im Freien verbrachte Zeit und reduzierter Schlaf¹⁷⁸. Ein angemessener Schlaf ist für die Entwicklung von Kindern und Jugendlichen, die Emotionsregulation, die Gedächtniskonsolidierung, die Reifung des Gehirns und die Freisetzung von Wachstumshormonen von entscheidender Bedeutung¹⁷⁹. Dennoch hält sich ein großer Teil der Jugendlichen nicht an die für ihr Alter geltenden Schlafempfehlungen¹⁸⁰.

Es gibt Hinweise darauf, dass die Bildschirmnutzung durch Kinder und Jugendliche zu einem verringerten und schlechteren Schlaf, zu weniger Schlaf, zu psychologischer Stimulation und zur Unterdrückung der Melatoninproduktion (insbesondere durch die Emission von blauem Licht) beitragen kann¹⁸¹. Zudem kann Bildschirmzeit im Freien verbrachte Zeit ersetzen, was sich negativ auf den Schlaf¹⁸² und die körperliche und psychische Gesundheit Minderjähriger insgesamt auswirkt.

Umfragen zeigen starke nächtliche Aktivitäten bei Jugendlichen. Altersspezifische Muster belegen, dass Kinder unter fünf Jahren durch die elterliche Kontrolle weitgehend geschützt sind. Sechs- bis 12-Jährige weisen hingegen eine längere Schlafatenz und eine schlechtere Schlafqualität auf, während 13- bis 15-Jährige von Einschlafproblemen, verminderter Schlafqualität und kognitiver Erregung vor dem Einschlafen berichten¹⁸³.

**„Die meisten der
im Rahmen des
Sonderausschusses
für die Online-
Sicherheit von Kindern
erörterten Risiken,
einschließlich
übermäßiger
Bildschirmzeit und
der Nutzung von KI-
Gefährten, sind
nicht nur für Kinder
und junge Menschen
relevant, sondern
für Menschen aller
Altersgruppen.“**

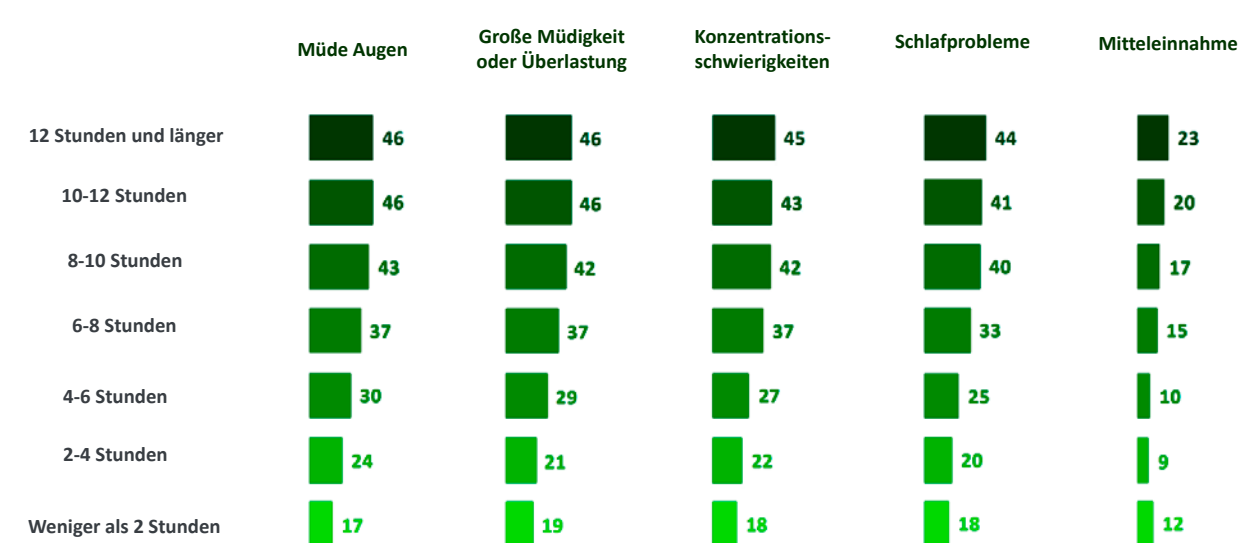
— ALBERTO MONGE ROFFARELLO,

ASSISTENZPROFESSOR FÜR DIGITALES
WOHLBEFINDEN UND ETHISCHES
KI-DESIGN, POLITECNICO DI TORINO

Allgemeine Maßnahmen zur Verkürzung der Bildschirmzeit (z. B. eine Reduzierung der Bildschirmnutzung vor dem Schlafen, also nach 21.00 Uhr) wirken sich nachweislich positiv auf die Schlafdauer¹⁸⁴ und die Vigilanz am nächsten Tag aus¹⁸⁵. Forschungsarbeiten, in denen die Auswirkungen einer hohen Bildschirmexposition auf die Gehirnentwicklung von Minderjährigen untersucht werden, sind weitgehend korrelativ; darin kann kein ursächlicher Zusammenhang hergestellt werden.

Abbildung 2: Zunehmende Symptome bei Jugendlichen aufgrund der vor Bildschirmen verbrachten Zeit

Frage: Welche der folgenden Situationen haben Sie ggf. in den letzten 30 Tagen erlebt?^b



Quelle: Europäische Kommission (2026). Auswirkungen übermäßiger Bildschirmzeit und sozialer Medien auf die psychische Gesundheit junger Menschen – Juni 2026 – Eurobarometer-Umfrage.

b. Anmerkung: Die Zahlen geben den prozentualen Anteil (%) der Befragten an, die von Problemen aufgrund der am Wochenende vor Bildschirmen verbrachten Zeit berichten.

SUCHTERZEUGENDE GESTALTUNG UND „DARK PATTERNS“

Nach Erkenntnissen der WHO gab mehr als ein Drittel der Jugendlichen an, online in ständigem Kontakt mit Freunden zu stehen. Jeder zehnte Jugendliche zeigt Anzeichen für ein problematisches Nutzungsverhalten in den sozialen Medien, das durch suchtmännliche Symptome gekennzeichnet ist¹⁸⁶.

In jüngster Zeit hat sich der Forschungsschwerpunkt in der Suchtmedizin von individuellen Faktoren, die zu suchtmännlicher Nutzung von Sozialen Medien führen oder dieses kennzeichnen, verlagert, um auch die Gestaltung sozialer Medien und anderer digitaler Dienste zu untersuchen, die entsprechende Verhaltensweisen fördern.

Kinder zwischen sechs und 12 Jahren können einem besonderen Risiko ausgesetzt sein, bei der Nutzung sozialer Medien+ frühzeitig ein Suchtverhalten zu entwickeln. Diese Risiken bestehen später fort, insbesondere in der frühen Jugend.

Suchterzeugende Designmerkmale und „Dark Patterns“¹⁸⁷, die in einigen sozialen Medien+ (absichtlich oder unbeabsichtigt) verfügbar sind, verzerren oder beeinträchtigen die Fähigkeit der Nutzer, autonome und fundierte Entscheidungen zu treffen. Suchterzeugende Funktionen umfassen Autoplay-Inhalte, unendliches Scrollen, Gamification und „Pull-to-Refresh“-Funktionen. Beispiele für „Dark Patterns“ sind gefälschte Countdown-Zähler, Web-Oberflächen, die Verbraucher zu Käufen, Abonnements oder anderen Entscheidungen veranlassen sollen, sowie versteckte Informationen¹⁸⁸.

Untersuchungen deuten darauf hin, dass auch andere Merkmale, darunter „Likes“ und „Push-Benachrichtigungen“, zu zwanghafter Nutzung anregen können¹⁸⁹. Studien haben auch gezeigt, dass Plattformen zur Maximierung von Nutzerinteraktionen auf Jugendliche überwiegend negative Auswirkungen haben¹⁹⁰. Jugendliche sind aufgrund ihrer Entwicklungsmerkmale und der Bedeutung der Akzeptanz unter Gleichaltrigen für die Identitätsbildung besonders anfällig für auf Beeinflussung zielende Designmerkmale¹⁹¹. Junge Erwachsene und Erwachsene mit ohnehin bereits beeinträchtigten Wohlbefinden sind ebenfalls besonders gefährdet¹⁹².

Die Eignungsprüfung der Europäischen Kommission zur digitalen Fairness von 2024¹⁹³ ergab, dass Merkmale wie manipulative Benutzeroberflächen („Dark Patterns“) von Menschen online sehr häufig angetroffen werden. Es wurde festgestellt, dass bei bis zu 97 % der unter Verbrauchern in der EU beliebtesten Websites und Anwendungen mindestens ein Dark Pattern zum Einsatz kommt. Außerdem wurde festgestellt, dass 31 % der Verbraucher aufgrund suchterzeugender Gestaltungselemente mehr Zeit online verbrachten und dort auch mehr Geld ausgaben.

Um einen systemischen Wandel zu erreichen, muss der Schwerpunkt von der individuellen Verantwortung auf den Umgang mit den umfassenderen Auswirkungen von Strategien zur Gestaltung der sozialen Medien+ verlagert werden. Forscher untersuchen die datengesteuerten Geschäftsmodelle von Social-Media-Plattformen, bei denen gewinnorientierte Nutzerinteraktion im Vordergrund steht, und erörtern alternative Modelle, deren Schwerpunkt eine ethische Gestaltung ist¹⁹⁴.

Dies wird im weiteren Sinne dadurch erreicht, dass gefordert wird, dass das Wohl der Kinder bei der Gestaltung und Betreuung digitaler Umgebungen¹⁹⁵ vorrangig berücksichtigt wird, um ihr digitales Wohlergehen zu unterstützen.

ALKOHOL- ODER SUBSTANZMISSBRAUCH

In den letzten zehn Jahren hat die Forschung den Zusammenhang zwischen der Nutzung sozialer Medien und Alkoholkonsum bei Jugendlichen ermittelt und untersucht¹⁹⁶. Alkohol ist in den sozialen Medien sehr präsent, doch bestehen zwischen den digitalen Diensten erhebliche Unterschiede in Bezug auf seine Verbreitung und Darstellung¹⁹⁷. Positive Darstellungen von Alkohol in den sozialen Medien prägen Einstellungen und wahrgenommene Normen¹⁹⁸. Die Exposition gegenüber alkoholbezogenen Inhalten und deren Weiterverbreitung ist mit einem höheren Alkoholkonsum verbunden, wodurch eine bidirektionale Verstärkungsschleife entsteht¹⁹⁹.

Individuelle Unterschiede, wie Dispositionsmerkmale, der soziale Kontext und das Entwicklungsstadium, schwächen diesen Zusammenhang ab. Familiäre Umgebungen können diese Auswirkungen abfedern, wobei eine negative alkoholbezogene Sozialisation durch Eltern und Gleichaltrige den Einfluss alkoholbezogener Online-Inhalte abschwächen kann²⁰⁰. Zu den künftigen Forschungsprioritäten gehören die Ausweitung von Studien über WEIRD-Stichproben^e hinaus, die Klärung der zeitlichen Dynamik und die Untersuchung, wie unterschiedliche Inhaltsarten (positive Darstellungen, Werbe- und Präventionsbotschaften) mit dem Trinkverhalten von Jugendlichen interagieren.

Hinsichtlich des Substanzmissbrauchs ist festzustellen, dass Inhalte, die die Offenheit gegenüber dem Substanzkonsum fördern oder deren Verwendung aktiv darstellen, in den sozialen Medien weithin verfügbar sind. Dies kann die Einstellungen, Verhaltensweisen und Risikowahrnehmungen in Bezug auf den Drogenkonsum beeinflussen, insbesondere bei Kindern und Jugendlichen²⁰¹. Ähnlich wie bei Alkohol deuten Untersuchungen darauf hin, dass Inhalte in sozialen Medien im Zusammenhang mit Drogen mit einer höheren Wahrscheinlichkeit des Konsums von Cannabis und eines Konsums mehrerer Substanzen in Verbindung gebracht werden²⁰².

GEFÄHRDUNG DURCH KRIMINALITÄT UND ILLEGALE ONLINE-INHALTE

Nach Angaben von Europol sind Kinder und Jugendliche online einer Reihe von Straftaten ausgesetzt, darunter Grooming, sexueller Missbrauch von Kindern, Radikalisierung oder Anwerbung zu Gewalttaten und Terrorismus²⁰³. Diese Risiken werden durch Aktivitäten Minderjähriger in Online-Räumen²⁰⁴ sowie durch die Exposition gegenüber schädlichen oder missbräuchlichen Inhalten, einschließlich des Zugangs zu Pornografie ab einem sehr jungen Alter, noch erhöht²⁰⁵.

In Deutschland gibt es Hinweise darauf, dass die mit sexuellen Absichten getätigte Kontaktaufnahme zu Kindern und der sexuelle Missbrauch von Kindern unter den jüngeren Generationen zuletzt deutlich zugenommen haben. Dies könnte auf die zunehmende Exposition gegenüber digitalen Umgebungen in Verbindung mit der Verbreitung sozialer Medien in den letzten Jahrzehnten zurückzuführen sein. Diese Ergebnisse machen deutlich, dass gezielte Präventionsmaßnahmen dringend erforderlich sind, um Online-Risiken für Kinder und Jugendliche zu begegnen²⁰⁶.

c. Demografische Stichprobe, die den Kriterien „westlich“ (Western), „gebildet“ (educated), industrialisiert (industrialized), „reich“ (rich) und „demokratisch“ (democratic) – WEIRD – entspricht.

DARSTELLUNGEN VON SEXUELLEM MISSBRAUCH VON KINDERN

In den letzten Jahrzehnten sind soziale Medien+ zu einem zentralen Element bei der Verbreitung von Darstellungen des sexuellen Missbrauchs von Kindern sowie dessen Produktion, Verbreitung und Konsum geworden. Im Jahr 2025 wurden 63 % aller von der Internet Watch Foundation gefundenen Webseiten mit Darstellungen des sexuellen Missbrauchs von Kindern in EU-Mitgliedstaaten gehostet.

Nach Daten des National Centre for Missing and Exploited Children (NCMEC) der Vereinigten Staaten aus dem Jahr 2025 nimmt das Online-Grooming mit alarmierender Geschwindigkeit zu, wobei entsprechende Anzeigen in den letzten drei Jahren um 158 % gestiegen sind. Täter nutzen systematisch soziale Medien, Messaging-Anwendungen und Spielplattformen, um Kontakt zu Minderjährigen herzustellen und Grooming-Aktivitäten durchzuführen. Diese Online-Interaktionen führen häufig zu sexueller Ausbeutung außerhalb des digitalen Raum, was zeigt, dass ein enger Zusammenhang zwischen Online-Grooming und der Begehung damit zusammenhängender Straftaten außerhalb des Internets besteht.

Technologische Entwicklungen, einschließlich generativer KI, verstärken die Risiken und beschleunigen das Ausmaß möglichen Missbrauchs. Die Verbreitung von KI hat zu einem exponentiellen Anstieg von KI-generiertem Material mit Darstellungen des sexuellen Missbrauchs von Kindern geführt, wobei die Anzahl der Anzeigen sprunghaft von 5 000 im Jahr 2023 auf 1,3 Millionen im Jahr 2025 gestiegen ist²⁰⁷.

Allein zwischen 2024 und 2025 haben KI-generierte Videos mit Darstellungen des sexuellen Missbrauchs von Kindern um mehr als das 26-fache zugenommen. 65 % wurden als Material der Kategorie A, der schwerwiegendsten Form des Missbrauchs, eingeschätzt. Diese Erkenntnisse verdeutlichen die Bedrohung, die von sozialen Medien+ und generativer KI ausgeht, wenn es darum geht, die rasche Verbreitung von Material mit Darstellungen des sexuellen Missbrauchs von Kindern zu ermöglichen.

Der Konsum realitätsnaher KI-generierter Inhalte kann bestehende sexuelle Neigungen verstärken. Einer Umfrage von Protect Children Finland aus dem Jahr 2021 zufolge gaben 44 % von 5 171 Befragten an, durch die Betrachtung von Material mit Darstellungen des sexuellen Missbrauchs von Kindern dazu veranlasst worden zu sein, über die Suche nach Kontakten zu Minderjährigen nachzudenken, wobei 37 % angaben, Kontakt gesucht zu haben²⁰⁸.

Mädchen sind möglicherweise besonders gefährdet. Im Jahr 2025 zeigten 97 % der von der Internet Watch Foundation ermittelten KI-generierten Darstellungen des sexuellen Missbrauchs von Kindern Mädchen²⁰⁹. Junge Mädchen im Alter zwischen 12 und 18 Jahren sind möglicherweise besonders gefährdet.

Sexuelle Ausbeutung online steht auch in engem Zusammenhang mit Menschenhandel. Digitale Dienste können die Anwerbung, Kontrolle und Monetarisierung von Opfern erleichtern, auch bei in großem Maßstab durchgeführtem Live-Streaming-Missbrauch. Diese Form der Ausbeutung ist aufgrund ihrer Anonymität eine der weltweit am schnellsten wachsenden. Die Schädigung der Opfer ist schwerwiegend und langanhaltend.

Opfer berichten über langfristige psychische Folgen, darunter Angst, Scham und die permanente Furcht davor, erkannt zu werden²¹⁰. Durch die kontinuierliche Online-Zirkulation des Materials wird die Viktimisierung auf unbestimmte Zeit verlängert, was bedeutet, dass der Schaden mit der Beendigung des ursprünglichen Missbrauchs nicht endet.

In einer internen Studie der Gemeinsamen Forschungsstelle (JRC) der Europäischen Kommission wurde festgestellt, dass Plattformen der sozialen Medien zwar nicht die primären Hosts von Material mit Darstellungen des sexuellen Missbrauchs von Kindern sind, aber genutzt werden können, um dieses Material zu verbreiten, häufig über Links zu externen Websites oder verschlüsselte Kanäle.

Algorithmische Systeme, die in Plattformen der sozialen Medien integriert sind, können Inhalte im Zusammenhang mit Material mit Darstellung des sexuellen Missbrauchs von Kindern verstärken und sie für Nutzer, einschließlich Täter und Minderjährige, leichter auffindbar und zugänglich machen.

Andere Inhalte mit Darstellungen Minderjähriger auf Plattformen der sozialen Medien sind zwar nicht notwendigerweise Darstellungen des sexuellen Missbrauchs von Kindern, können aber von Straftätern ausgenutzt werden und die Risiken für Kinder und Jugendliche erhöhen. Zu den Risiken für Minderjährige, die durch die Exposition gegenüber Darstellungen des sexuellen Missbrauchs von Kindern verursacht werden, gehören emotionale und psychische Schäden, Angstsymptome, Depressionen und Traumata.

Bei Kindern und Jugendlichen, die bereits sexuellen Missbrauch erfahren haben, können Online-Umgebungen zum Risiko einer Reviktimisierung beitragen²¹¹. Die kontinuierliche Verfügbarkeit und Verbreitung von Material mit Darstellungen des sexuellen Missbrauchs von Kindern bedeutet, dass der Missbrauch noch lange nach Beendigung der ursprünglichen Straftat wiederholt erneut erlebt werden kann²¹². Im Gegensatz zu vielen Formen der Offline-Viktimisierung kann digitales Material unbegrenzt kopiert, weiterverbreitet und zugänglich gemacht werden, was für die Opfer, die oft wissen, dass Bilder oder Videos ihres Missbrauchs weiterhin verbreitet werden, eine anhaltende Quelle von psychischer Belastung und Unsicherheit ist.

Darüber hinaus gibt es Hinweise darauf, dass Überlebende von sexuellem Missbrauch im Kindesalter besonders anfällig für schädliche Online-Erfahrungen sein können²¹³. Sexueller Missbrauch im Kindesalter wird mit einer verstärkten Neigung zu hochriskantem Online-Verhalten, einer stärkeren Exposition gegenüber sexuellen Online-Inhalten, einem höheren Anteil an Cybermobbing-Viktimisierung und einem erhöhten Risiko einer durch das Internet initiierten Reviktimisierung in Verbindung gebracht²¹⁴. Diese Anfälligkeiten können die langfristigen Auswirkungen von Traumata auf die psychosoziale Entwicklung und das sexuelle Selbstbild stärker widerspiegeln als das individuelle Verhalten allein²¹⁵.

Eine wiederholte Online-Exposition gegenüber sexualisiertem oder ausbeuterischem Material kann daher traumabezogene Symptome verstärken, die Genesung beeinträchtigen und die Wahrscheinlichkeit einer weiteren Viktimisierung erhöhen. Gleichzeitig kann die Exposition gegenüber Darstellungen des sexuellen Missbrauchs von Kindern zur Normalisierung ausbeuterischer sexueller Verhaltensweisen unter Minderjährigen beitragen, wodurch sich das Risiko erhöht, dass anfällige Kinder zur Zielscheibe weiteren Missbrauchs oder weiterer Nötigung werden. Die Verhinderung der Verbreitung von Material mit Darstellungen des sexuellen Missbrauchs von Kindern ist nicht nur von entscheidender Bedeutung, um den anhaltenden Missbrauch zu unterbinden, sondern auch, um das Risiko einer wiederholten Viktimisierung zu verringern und die langfristige Genesung der betroffenen Kinder und Jugendlichen zu unterstützen²¹⁶.

Minderjährige, die in den sozialen Medien+ diesem Material oder Grooming ausgesetzt sind, sind in stärkerem Maße gefährdet, selbst ausgebeutet oder missbraucht zu werden. Die wiederholte Exposition gegenüber Material mit Darstellungen des sexuellen Missbrauchs von Kindern kann Minderjährige gegenüber dessen schädlichen Auswirkungen desensibilisieren und möglicherweise zu einer Normalisierung ausbeuterischer Verhaltensweisen führen.

Kinder und Jugendliche, die bereits sexuellen Missbrauch erlebt haben, unterliegen einem erhöhten Risiko einer Online-Reviktimisierung. Es gibt Hinweise darauf, dass der sexuelle Missbrauch eines Kindes in der Vergangenheit mit einer erhöhten Anfälligkeit gegenüber technologiegestützter sexueller Kontaktaufnahme und sexuellen Missbrauch verbunden ist, was die Notwendigkeit gezielter Schutzmaßnahmen für diese Gruppe unterstreicht²¹⁷.

Abbildung 3: Je mehr Zeit Jugendliche vor Bildschirmen verbringen, desto häufiger werden sie mit unerwünschten und illegalen Inhalten konfrontiert.

Frage: Haben Sie in den letzten drei Monaten bei der Nutzung sozialer Medien eine der nachfolgend beschriebenen Situationen gesehen oder erlebt?^d



Quelle: Europäische Kommission (2026). Auswirkungen übermäßiger Bildschirmzeit und sozialer Medien auf die psychische Gesundheit junger Menschen – Juni 2026 – Eurobarometer-Umfrage.

RADIKALISIERUNG UND ANWERBUNG FÜR GEWALTSTATEN

UND TERRORISMUS

Umgebungen sozialer Medien+ spielen eine wichtige Rolle bei der Radikalisierung und Anwerbung Minderjähriger für terroristische Handlungen und gewalttätigen Extremismus. Soziale Medien, verschlüsselte Messaging-Dienste und Online-Gemeinschaften werden genutzt, um Propaganda zu verbreiten, Netzwerke zu schaffen und direkt mit Minderjährigen in Kontakt zu treten.

Aus dem European Union Terrorism Situation and Trend Report von 2025 geht hervor, dass fast ein Drittel der Verdächtigen, die 2024 in der EU wegen Straftaten im Zusammenhang mit Terrorismus festgenommen wurden, Minderjährige oder junge Erwachsene waren²¹⁸. Von den 133 angezeigten jungen Verdächtigen waren 70 jünger als 18 Jahre. Die meisten jungen Verdächtigen standen im Zusammenhang mit dschihadistischem Terrorismus, gefolgt von rechtsextremistischem Terrorismus und gewalttätigem Extremismus.

Die Rekrutierung kann in einem sehr jungen Alter beginnen, wobei es dokumentierte Fälle gibt, an die Kinder im Alter von acht oder neun Jahren betreffen. Kinder und Jugendliche sind besonders anfällig für Online-Rekrutierungsstrategien der organisierten Kriminalität und terroristischer Gruppen, die häufig Gaming-Umgebungen und Online-Foren nutzen, um Minderjährige für diese Aktivitäten anzulocken.

Es hat sich gezeigt, dass Minderjährige, die in der EU terroristischer Straftaten schuldig befunden wurden, online möglicherweise einen Prozess der Selbstradikalisierung durchlaufen, wobei algorithmengesteuerte Inhalte eine Schlüsselrolle bei der Verstärkung radikaler Vorstellungen spielen. Die regelmäßige Online-Exposition gegenüber Gewaltinhalten kann zu einer gefährlichen Normalisierung und allgemeinen Desensibilisierung gegenüber menschlichem Leid führen²¹⁹.

d. Anmerkung: Die Zahlen geben den prozentualen Anteil (%) der Befragten an, die von Risiken aufgrund der am Wochenende vor Bildschirmen verbrachten Zeit berichten.

Der Fall „White Tiger“ [siehe Kasten unten] veranschaulicht, wie Online-Plattformen kriminellen Netzwerken und Einzelpersonen ermöglichen können, Minderjährige in Online-Missbrauchsnetzwerke zu locken, wodurch Ausbeutung, Grooming und psychischer Missbrauch erleichtert werden.

DER FALL „WHITE TIGER“

Im Mittelpunkt des Falles „White Tiger“ steht ein Verdächtiger, der im Sommer 2025 in Deutschland festgenommen und mutmaßlich als wichtige Persönlichkeit innerhalb der nihilistischen, gewaltbereiten Online-Extremistengruppe „764“ identifiziert wurde. Dem Verdächtigen, der unter dem Pseudonym „White Tiger“ auftrat, werden über 200 Straftaten gegen mehr als 30 Kinder und Jugendliche zur Last gelegt^e. Der Verdächtige war 16 bzw. 19 Jahre alt, als er die ihm zur Last gelegten Straftaten begangen hat.

Zu den mutmaßlichen Straftaten gehört die Anstiftung eines 13-jährigen Jungen aus den Vereinigten Staaten zum Suizid, der 2022 live im Internet übertragen wurde. Weitere Fälle sind das „Grooming“ von 11- bis 15-Jährigen, die veranlasst wurden, sich online vor Zuschauern zu verletzen, und die Herstellung von Material mit Darstellungen des sexuellen Missbrauchs von Kindern. Opfer wurden in mehreren Ländern ermittelt, vor allem in Deutschland, den Vereinigten Staaten, dem Vereinigten Königreich und in Kanada. Dem Verdächtigen wird vorgeworfen, online gezielt nach vulnerablen, isolierten oder emotional belasteten Kindern und Jugendlichen gesucht zu haben, einschließlich Personen, die ihre LGBTIQ+-Identität erkunden.

Durch Rapid-Grooming-Techniken hat der Verdächtige angeblich starke emotionale Abhängigkeiten geschaffen und die Opfer schrittweise von ihren Unterstützungssystemen in der realen Welt abgeschnitten. Nach der Isolierung der Opfer wurde das Grooming in eine heimtückische Form der Radikalisierung im Sinne gewaltbereiter extremistischer Ideologien und psychischer Folter überführt. Das Verfahren gegen den Verdächtigen begann 2026 in Deutschland. Die Staatsanwaltschaft sieht sich aufgrund der transnationalen und virtuellen Dimension des Falls mit Schwierigkeiten konfrontiert.

Das 764-Netzwerk arbeitet mit Mitteln wie schwerer Erpressung, Doxing-Drohungen und Gaslighting, um bei ihren Opfern das Erleben der eigenen Selbstwirksamkeit auszuhöhlen. Die Täter setzten systematisch gängige digitale Dienste, die bei Minderjährigen beliebt sind, als Waffe ein. Jugendliche wurden auch gezwungen, immer gefährlichere Befehle auszuführen, erniedrigende Handlungen zu filmen und die nihilistische Ideologie der Gruppe als verzerrte Form der Bestätigung zu übernehmen.

Ein wesentliches Merkmal ist, dass die Opfer häufig dazu erpresst werden, selbst Täter zu werden, und vom Netzwerk gezwungen werden, andere Minderjährige ins Visier zu nehmen, zu groomen und auszubeuten. Diese Dynamik veranschaulicht die Überschneidung zwischen der Viktimisierung von Kindern und der Verübung von Straftaten durch Kinder, bei denen Minderjährige genötigt werden, Straftaten gegen andere Kinder zu begehen oder sie zur Selbstverletzung zu ermutigen. Die ideologische Fluidität, die Vermischung von Online-Gefahren und die allmählich zunehmende Intensität von Selbstverletzung und Gewalt in Verbindung mit privaten Online-Räumen behindern die Bemühungen, gewalttätige extremistische Online-Netzwerke aufzudecken und vor Gericht zu bringen.

^e. Dieses Gerichtsverfahren ist noch anhängig. Bei den genannten Straftaten handelt es sich um Behauptungen, die dem Ausgang des Gerichtsverfahrens in keiner Weise vorgreifen.

DIE (MISSBRÄUCLICHE) VERWENDUNG VON DATEN MINDERJÄHRIGER

Kinder und Jugendliche sind bei der Nutzung sozialer Medien⁺ hinsichtlich der Art und Weise der Erhebung und Nutzung ihrer personenbezogenen Daten mehreren Risiken ausgesetzt. Ein wichtiges Problem ist das Profiling Minderjähriger. Das Verhalten von Nutzern in sozialen Medien und anderen digitalen Diensten wird für die unterschiedlichsten Zwecke in der Regel mithilfe von Cookies und ähnlichen Tracking-Technologien verfolgt. Der am stärksten in die Privatsphäre eingreifende Zweck eines solchen Trackings ist das websiteübergreifende Tracking für personalisierte Werbung. Viele Plattformen der sozialen Medien erheben personenbezogene Daten nicht nur über lokal auf dem Endgerät abgelegte Cookies, sondern auch über ihre Server in einem Umfang, der in die Privatsphäre von Minderjährigen eingreifen kann. In bestimmten Fällen können Anbieter digitaler Dienste und Werbetreibende Daten aus verschiedenen Quellen erheben^f.

Solche Praktiken ermöglichen es den Anbietern, ein umfassendes Bild des Verhaltens, der Vorlieben, Interessen, Bewegungen und Online-Aktivitäten Minderjähriger zu zeichnen^g. Sie können auch private Aspekte des Lebensstils oder der Überzeugungen eines Kindes oder Jugendlichen offenlegen, selbst wenn Minderjährige diese Informationen nicht direkt zur Verfügung gestellt haben. Eine allgegenwärtige Datenerhebung kann die Kontrolle Minderjähriger über ihre Daten verringern und sie unvorhergesehenen Risiken aussetzen, einschließlich des Drucks, In-App-Käufe zu tätigen oder zusätzliche Dienstleistungen zu erwerben.

Kinder können sich zwar auf das bedingungslose Recht auf Vergessenwerden gemäß der DSGVO²²⁰ berufen, doch müssen sie dieses Recht geltend machen, nachdem die Verarbeitung bereits stattgefunden hat. Dies setzt natürlich auch voraus, dass Kinder in der Lage sind, dieses Recht und die Art und Weise seiner Durchsetzung zu verstehen.

In diesem Zusammenhang sind Minderjährige Risiken ausgesetzt, die sich aus der Nutzung sozialer Medien und digitaler Dienste durch sie ergeben, in die Empfehlungssysteme und Algorithmen integriert sein können. Diese Systeme stützen sich häufig auf verhaltensbezogene Daten und Suchaktivitäten, um personalisierte Inhaltsfeeds und Werbung zu generieren. Sie können Minderjährige auch zu schädlichen oder unangemessenen Inhalten führen, die dazu bestimmt sind, eine längere Nutzung zu fördern. Diese Praktiken erhöhen die Risikoexposition von Kindern und Jugendlichen und die Möglichkeit, ein zwanghaftes oder Suchtverhalten zu entwickeln.

In beiden Fällen verstehen Minderjährige möglicherweise nicht, dass und in welchem Umfang ihre personenbezogenen Daten erhoben und wofür sie verwendet werden. Solche Praktiken erschweren die Feststellung, ob die Einwilligung von Kindern „freiwillig erteilt“ wurde, was ein zentraler Grundsatz dessen ist, was unter Einwilligung im Sinne der DSGVO zu verstehen ist.

Ein weiteres Problem ist die Nutzung der Geolokalisierungsdaten von Minderjährigen, die von gängigen Alltagsanwendungen wie Mobilitäts- und Wetter-Apps aufgezeichnet werden können und häufig von globalen Datenbrokern gehandelt werden. Wenn der Aufenthaltsort eines Kindes oder Jugendlichen nachverfolgt oder ermittelt werden kann, besteht die Gefahr, dass seine personenbezogenen Daten missbraucht werden könnten, was sich sowohl online als auch offline negativ auf seine körperliche

^f. Siehe beispielsweise Meta Platforms Inc./Bundeskartellamt (C-252/21).

^g. Meta Platforms Inc./Bundeskartellamt (C-252/21).

Sicherheit und sein Wohlergehen auswirken könnte. Zwar bedarf die Nutzung von Geolokalisierungsdaten in der Regel einer Einwilligung^h, doch ist es möglich, dass Minderjährige unbeaufsichtigt einwilligen, z. B. bei der Einrichtung einer auf ihr Telefon heruntergeladenen App, ohne dass ihre Einwilligung durch die Überprüfung Altersverifikation wirksam wurde.

Schließlich können Datenschutzverletzungen eine Reihe nachteiliger Auswirkungen auf Minderjährige haben, die zu einem physischen, materiellen oder immateriellen Schaden führen können²²¹. Dies kann den Verlust der Kontrolle von Kindern über ihre personenbezogenen Daten, die Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste und die unbefugte Aufhebung der Pseudonymisierung umfassen. Zudem besteht die Gefahr erheblicher weiterer wirtschaftlicher oder sozialer Nachteile.

- h.** Für Geolokalisierungsdaten, die im Rahmen herkömmlicher Telefondienste erzeugt werden (Daten des Ortes, von dem aus ein Mobiltelefongespräch geführt oder eine SMS versendet wurde); dies ergibt sich dies aus Artikel 9 der Datenschutzrichtlinie für elektronische Kommunikation. Geolokalisierungsdaten, die auf anderem Wege erhoben werden (in der Regel die GPS-Ortungsfunktion des mobilen Geräts), würden der DSGVO unterliegen und könnten auf unterschiedlichen Rechtsgrundlagen beruhen. Angesichts des in die Privatsphäre eingreifenden Charakters von Geolokalisierungsdaten halten die ehemalige Artikel-29-Datenschutzgruppe und der EDSA jedoch eine Einwilligung für erforderlich.

VIDEOSPIELE

Videospiele bieten Kindern und Jugendlichen nicht nur Unterhaltung, sondern auch soziale Räume, in denen sie online mit Anderen in Kontakt treten und kommunizieren können. Einige Hinweise deuten darauf hin, dass Videospiele Vorteile in Form von prosozialem Verhalten²²², Aufbau von Gemeinschaften und Eskapismus bieten können²²³. Aktuelle Schätzungen gehen davon aus, dass 80 % der Minderjährigen (zwischen zwei und 18 Jahren) 30 % ihrer Freizeit mit Spielen verbringen²²⁴.

Videospiele gibt es in sehr unterschiedlichen Formen und sie bergen verschiedene Risiken für Minderjährige. Einige der meistgespielten Spiele weisen plattformähnliche Merkmale auf. Eine offene Kommunikation über diese Dienste kann Minderjährige Risiken aussetzen, darunter Cybermobbing, Grooming und Radikalisierung²²⁵, und ihnen einen Zugang zu schädlichen oder nicht altersgerechten Inhalten ermöglichen. So ermöglichen beispielsweise „intermediäre Videospiele“ es den Nutzern, eigene Inhalte oder Spiele zu spielen und zu entwickeln. Nutzergenerierte Inhalte erhöhen das Risiko, dass Minderjährige nicht altersgerechten Inhalten ausgesetzt werden.

Bestimmte Plattformen vertreiben auch Spiele. Sowohl Videospiele als auch solche Plattformen können Geschäftspraktiken wie Lootboxen, Pay-to-advance, In-App-Käufe und virtuelle Währungen einsetzen, die manipulativ sein oder unerwünschte Ausgaben, zwanghafte Verhaltensweisen oder Suchtverhalten verursachen können²²⁶. Im Jahr 2018ⁱ wurde die Glücksspielerkrankung in die 11. Revision der Internationalen Klassifikation der Krankheiten (ICD-11) aufgenommen. Offenbar tritt sie bei Jugendlichen und jungen Männern zwischen 12 und 20 Jahren am häufigsten auf.

Eine Umfrage ergab, dass 12 % der Jugendlichen als von problematischem Gaming-Verhalten bedroht eingestuft wurden²²⁷. Diese Ergebnisse deuten auch darauf hin, dass Jungen zwischen 11 und 15 Jahren im Vergleich zu Mädchen einem erhöhten Risiko einer problematischen Nutzung ausgesetzt sind. Bei Jugendlichen wird eine Computerspielerkrankung mit einem erhöhten Maß an Externalisierung (beispielsweise unsoziales Verhalten und Wutprobleme) und Internalisierung (beispielsweise emotionale Belastung und geringeres Selbstwertgefühl) in Verbindung gebracht. Jugendliche, die an einer Computerspielerkrankung leiden, können einem höheren Risiko von schulischen Leistungsschwächen, Schulabbruch, psychosozialen Problemen und Schlafproblemen ausgesetzt sein.

Im Juni 2026 wurde das europäische System für die Alterseinstufung von Computer- und Videospielen (PEGI) um neue Kategorien seiner Einstufungskriterien ergänzt, um Risiken der Online-Interaktion bei Videospielen zu begegnen. Neu eingereichte Spiele werden nun nach umfassenderen Kriterien klassifiziert, die sowohl den Inhalt als auch die Funktionen betreffen. Dazu gehören Käufe von In-Game-Inhalten, kostenpflichtige Zufallsartikel, Kommunikationsfunktionen und solche, die Anreize für kontinuierliches Spielen schaffen. Einige dieser Merkmale sind nun an bestimmte Altersgruppen gebunden, sodass beurteilt werden kann, ob ein Videospiel eine höhere Alterseinstufung benötigt.

Einem Vertreter der deutschen „Unterhaltungssoftware Selbstkontrolle“ (USK) zufolge wurde mindestens eines der neuen USK-Kriterien auf rund 30 % aller Spiele angewandt, die seit der Aktualisierung des Systems eingereicht wurden. Davon hat etwa jedes dritte eine höhere Alterseinstufung erhalten ²²⁸.

- i. „Computerspielerkrankung“ ist als ein Muster des Verhaltens beim Spielen definiert, das sich dadurch auszeichnet, dass Spieler „die Kontrolle über ihr Spielverhalten verlieren, dass dem Spielen Vorrang vor anderen Aktivitäten eingeräumt wird, bis schließlich das Spielen Vorrang vor anderen Interessen und alltäglichen Aktivitäten hat, und dass das Spielen trotz des Auftretens negativer Folgen fortgesetzt wird oder eskaliert“. Siehe Weltgesundheitsorganisation (2020), Addictive behaviours: Gaming disorder.

GEMEINSAME MERKMALE DER SOZIALEN MEDIEN+ UND IHRE RISIKEN

Soziale Medien und andere digitale Dienste unterscheiden sich stark, weisen jedoch eine Reihe gemeinsamer Merkmale auf. Die OECD²²⁹ und Forschende haben unterschiedliche Einstufungen der Risiken entwickelt, denen Kinder und Jugendliche online ausgesetzt sein können. Die 5-C-Klassifikation unterstützt Anbieter sozialer Medien und anderer digitaler Dienste, Hochschulen und politische Entscheidungsträger dabei, die online bestehenden Risiken für Minderjährige besser zu verstehen und zu bewerten²³⁰.

Die 5-C-Klassifikation umfasst fünf Kategorien:

- // Verhaltensrisiken (Conduct risks): Risiken für Minderjährige, sich an Fehlverhalten zu beteiligen oder Zeuge oder Opfer eines solchen Verhaltens zu werden,
- // Kontaktrisiken (Contact risks): Risiken für Minderjährige, online mit böswilligen Akteuren konfrontiert oder von ihnen ins Visier genommen zu werden,
- // Inhaltsrisiken (Content risks): Risiken, mit schädlichen Inhalten konfrontiert zu werden,
- // Vertragsrisiken (Contract risks): Risiken für Minderjährige, einen potenziell schädlichen Vertrag abzuschließen,
- // bereichsübergreifende Risiken (Cross-cutting risks; in der nachstehenden Tabelle mit „CC“ abgekürzt): Risiken für die Gesundheit, die Privatsphäre und die faire Behandlung von Minderjährigen (Nichtdiskriminierung).

Das Europäische Zentrum für die Transparenz der Algorithmen (ECAT)²³¹ hat in einer Matrix zum Online-Schutz von Minderjährigen gemeinsame Merkmale mit Risiken der 5-C-Klassifikation verknüpft, die in der nachstehenden Tabelle dargestellt sind. Es sei darauf hingewiesen, dass Minderjährige unterschiedlichen Alters durch diese Merkmale unterschiedlich stark gefährdet sind²³².

HÄUFIGE ONLINE-FUNKTIONEN UND DAMIT VERBUNDENE 5-C-RISIKEN

Merkmale	Beschreibung	5-C-Risiken
Werbung	Werbeinhalte, die Nutzenden angezeigt werden, meist zur Bewerbung von Produkten oder Dienstleistungen.	Inhalt, Verhalten, Vertrag, CC-Gesundheit, CC-Privatsphäre, CC-Diskriminierung
Altersfeststellung/-verifikation	Methoden zur Bestätigung des Alters der Nutzer, um sicherzustellen, dass sie die Altersanforderungen der Plattform erfüllen.	Inhalt, CC-Gesundheit, CC-Privatsphäre, CC-Diskriminierung
KI-Chatbots	Automatisierte Systeme, die eine Konversation mit Nutzern unter Verwendung künstlicher Intelligenz simulieren.	Inhalt, CC-Gesundheit
Schönheitsfilter	Tools, die das Erscheinungsbild einer Nutzerin oder eines Nutzers auf Fotos oder in Videos verbessern oder verändern.	CC-Gesundheit
Kommentare/Meinungsäußerungen	Feedback oder Gedanken zu Inhalten oder Posts.	Inhalt, Verhalten, Vertrag, CC-Gesundheit, CC-Privatsphäre
Geschäftspraktiken	Strategien und Aktivitäten sozialer Medien+ zur Förderung und zum Verkauf von Produkten oder Dienstleistungen.	Verhalten
Kontakt-Empfehlungen	Vorschläge für Nutzer, mit anderen Nutzerinnen und Nutzern in sozialen Medien+ Kontakt aufzunehmen.	Kontakt, CC-Gesundheit, CC-Privatsphäre
Inhaltliche Empfehlungen	Vorschläge für Inhalte, die Nutzenden angezeigt bzw. empfohlen werden.	Inhalt, CC-Gesundheit, CC-Privatsphäre, CC-Diskriminierung
Standardeinstellungen	Anfangskonfigurationen sozialer Medien+, die vorhanden sind, wenn ein Nutzer erstmalig darauf zugreift	Inhalt, CC-Datenschutz
Redaktionelle Inhalte	Inhalte, die von professionellen Autoren oder Redakteuren für eine Online-Plattform erstellt werden.	Inhalt
Generative KI	Generative künstliche Intelligenz, die neue Inhalte oder Daten erzeugt	Verhalten, Inhalt, CC-Gesundheit, CC-Privatsphäre
Geolokalisierung	Verwendung von Daten zur Bestimmung des physischen Standorts eines Nutzers	CC-Gesundheit, CC-Privatsphäre
Lootboxen	Virtuelle Artikel, die Zufallsprämien enthalten und häufig mit echtem Geld gekauft werden.	Verhalten, CC-Gesundheit
Marktplätze	Soziale Medien+, in denen Nutzer Waren oder Dienstleistungen kaufen und verkaufen können.	Inhalt, Verhalten, Vertrag, CC-Gesundheit
Benachrichtigungen	Warnungen oder Nachrichten, die die Nutzer über Aktivitäten oder Aktualisierungen auf der Plattform informieren.	CC-Gesundheit
Online-Oberfläche	Layout und Funktionen sozialer Medien+.	CC-Gesundheit
Elterliche Kontrolle	Tools, mit denen Betreuungspersonen Online-Aktivitäten Minderjähriger überwachen und beeinflussen können.	CC-Gesundheit, CC-Privatsphäre
Private Nachrichten	Individuelle Mitteilungen zwischen Nutzern, die nicht öffentlich sichtbar ist.	Kontakt, Vertrag
Melde- und Abhilfemechanismen	Mechanismen für Nutzerinnen und Nutzer, um Probleme auf einer Plattform zu melden und zu beheben.	Verhalten, Inhalt, CC-Privatsphäre, CC-Diskriminierung
Allgemeine Geschäftsbedingungen	-	Vertrag
Vom Nutzenden generierte Inhalte	Jede Form von Inhalten – wie Text, Videos, Bilder, Bewertungen oder Kommentare –, die von Nutzerinnen und Nutzern in sozialen Medien+ erstellt und geteilt werden.	Verhalten, Inhalt, CC-Gesundheit, CC-Privatsphäre

Quelle: MANOLIOS, S., *Online Minor Protection Matrix*, CHAUDRON, S., SALA, A. und GOMEZ, E. (Herausgeber), Amt für Veröffentlichungen der Europäischen Union, Luxemburg, 2026, JRC147657.

Empfehlungen

Trotz der damit verbundenen Herausforderungen müssen Maßnahmen zur Förderung der Sicherheit von Kindern im Internet bedarfsorientiert und entwicklungsorientiert gestaltet werden, wobei den komplexen und heterogenen sozialen und individuellen Situationen und Hintergründen von Kindern und Jugendlichen Rechnung zu tragen ist. In einer zunehmend digitalisierten Welt sind Minderjährige, unabhängig davon, ob sie als „aktive Nutzer“ gelten oder nicht, bereits in den allerersten Lebenstagen häufig über ihre primären Betreuungspersonen passiven Kontakten mit sozialen Medien+ ausgesetzt.

Die Herausforderung für die politischen Entscheidungsträger besteht darin, dieser Komplexität durch gezielte politische Maßnahmen Rechnung zu tragen und gleichzeitig eine wirksame Umsetzung und Bewertung sicherzustellen. Solide Erkenntnisse darüber, wie Risiken und Schäden mit verschiedenen sozialen Medien und anderen digitalen Diensten zusammenhängen, sind unerlässlich, um geeignete Maßnahmen zum Schutz und zur Stärkung Minderjähriger in der Online-Umgebung ergreifen zu können. Spezifische Merkmale, Funktionen oder Formate, die in sozialen Medien+ implementiert werden, können je nach den sozialen und persönlichen Umständen eines Kindes oder Jugendlichen in unterschiedlichem Maße schädlich sein.

Minderjährige, die ethnischen und religiösen Minderheiten angehören, einen Migrationshintergrund haben, Teil der LGBTIQ+-Gemeinschaft sind oder sonderpädagogischen Förderbedarf und Behinderungen oder bereits bestehende psychische Erkrankungen haben, können in besonderem Maße Gefahren im digitalen Raum ausgesetzt sein. Diese Exposition wird durch digitale Dienste verstärkt, die schädliche, manipulative oder suchtfördernde Inhalte oder Konzepte umfassen. Die Forschungsarbeit und die Sammlung von Erkenntnissen sollten in jedem Fall mit der Weiterentwicklung dieser Merkmale Schritt halten.

Damit diese Forschungsarbeit zum Tragen kommt, gibt es eine zentrale Voraussetzung: zuverlässige Daten, die direkt von der Quelle – den Anbietern selbst – stammen. Nur durch den Zugang zu einschlägigen Daten können Forschende, Pädagogen und politische Entscheidungsträger systemische Risiken verstehen, neu auftretende Bedrohungen überwachen und geeignete Schutzmaßnahmen konzipieren.

Die EU hat erhebliche Schritte unternommen, um sicherzustellen, dass die Forschung durch einen sinnvollen, verhältnismäßigen und wirksamen Zugang zu Daten von Online-Plattformen erleichtert wird, insbesondere im Rahmen des Gesetzes über digitale Dienste (Digital Services Act (DSA)), das sowohl den Zugang zu öffentlichen als auch zu nicht öffentlichen Daten erleichtert, um systemische Risiken zu untersuchen, von denen Minderjährige online betroffen sind. Aufbauend auf diesem bestehenden Rahmen und den Maßnahmen, die die Anbieter ergreifen sollten [\[siehe auch die Empfehlungen in Kapitel 4\]](#), könnten die folgenden Empfehlungen in Betracht gezogen werden:

„Empfehlungen zur Nutzung sozialer Medien durch Kinder und Jugendliche sollten evidenzbasiert sein und auf den besten verfügbaren wissenschaftlichen Studien beruhen.“

– PROF. CHRISTOPH PIEH,

LEITER DES DEPARTMENTS FÜR
PSYCHOSOMATISCHE MEDIZIN UND
PSYCHOTHERAPIE, UNIVERSITÄT FÜR
WEITERBILDUNG KREMS

EMPFEHLUNG 1**Evidenzbasierte Politik stärken, indem Evidenz in wenig erforschten Bereichen erarbeitet wird**

Forschende sollten sich weiter auf Erkenntnisse über die Risiken und Chancen im Zusammenhang mit der Nutzung sozialer Medien+ durch Kinder und Jugendliche in wenig erforschten Bereichen stützen. Zu den Schlüsselbereichen, die gestärkt werden müssen, gehören die heterogenen Auswirkungen der Nutzung sozialer Medien+ durch Minderjährige während der gesamten Entwicklung, der Umgang Minderjähriger mit Geld im digitalen Raum (auch auf Online-Marktplätzen), KI-Tools (einschließlich KI-Gefährten) und die ethische Gestaltung sozialer Medien+. Kontrollierte Nutzerstudien in bestimmten sozialen Medien und digitalen Diensten sind wichtig, um die Auswirkungen bestimmter Gestaltungsmerkmale oder einer Gruppe dieser Merkmale zu untersuchen. Um die kausalen Auswirkungen bestimmter Merkmale klarer darzustellen, sollten randomisierte kontrollierte Studien durchgeführt werden. Die Anbieter tragen eine wichtige Verantwortung für die Unterstützung dieser Studien, indem sie unabhängigen Forschenden Zugang gewähren.

Die potenziellen positiven Auswirkungen der Nutzung sozialer Medien+, beispielsweise in strukturierten Betreuungs- oder Bildungskontexten, sind ein weiterer Bereich, der näher untersucht werden sollte. Soziale und individuelle Faktoren, die die Auswirkungen der Nutzung sozialer Medien+ auf die Entwicklung von Minderjährigen beeinflussen, sowie das Zusammenspiel zwischen diesen Faktoren sollten ebenfalls näher beleuchtet werden. Diese Erkenntnisse werden benötigt, um eine evidenzbasierte Politik zur Förderung der Sicherheit und Stärkung der Handlungskompetenz von Kindern online zu unterstützen und zu stärken.

EMPFEHLUNG 2**Anbieter sollten unabhängige wissenschaftliche Expertise aktiv in die Gestaltung von Risikominderungsstrategien und -instrumenten einbeziehen**

Über die Einhaltung der geltenden Vorschriften hinaus sollten soziale Medien und andere Anbieter digitaler Dienste aktiv unabhängige Sachverständige und Minderjährige in die Gestaltung ihrer Risikominderungsstrategien und -instrumente sowie in die Entwicklung spezifischer Funktionen und Dienste für Minderjährige im Internet einbeziehen. Dabei sollten Sachverständige aus einem breiten Spektrum von Disziplinen, die unter Anwendung unterschiedlicher Methoden arbeiten, vertreten sein, um solide und fundierte Erkenntnisse zu gewährleisten.

EMPFEHLUNG 3**Langfristige Finanzierung für groß angelegte europäische Langzeitstudien bereitstellen und randomisierte kontrollierte Studien weiter fördern**

Groß angelegte europäische Langzeitstudien zur Sicherheit von Kindern im Internet könnten sich beispielsweise an der nordamerikanischen Langzeitstudie zur Gehirnentwicklung und Gesundheit von Kindern (Adolescent Brain Cognitive Development; ABCD-Studie) orientieren. Um bei Fragen der Sicherheit von Kindern im Internet einen entwicklungsorientierten und neurobiologischen Ansatz verfolgen zu können, braucht es umfassende europäische Langzeitdaten (die einen Zeitraum von zehn Jahren oder

mehr abdecken). So könnten Lücken in den weitgehend korrelierenden Forschungsergebnissen im europäischen Kontext zu den Auswirkungen der Nutzung sozialer Medien auf die Entwicklung, die körperliche und psychische Gesundheit von Minderjährigen und Online-Gefahren geschlossen werden.

Auch randomisierte kontrollierte Studien sind wichtige Werkzeuge, um die Evidenzbasis für politische Entscheidungen zu stärken. Die Forschungsförderung sollte ausdrücklich entwicklungsorientierte und psychopathologische Ansätze zur Untersuchung der Anfälligkeiten von Minderjährigen für Risiken im Internet unterstützen, wobei auch soziale und individuelle Faktoren in Kindheit und Jugend berücksichtigt werden sollten.

EMPFEHLUNG 4

In eine geschützte, gemeinsame europäische Forschungsinfrastruktur investieren, um sicheren Zugang zu den Daten von Minderjährigen zu ermöglichen

Die Europäische Union und ihre Mitgliedstaaten sollten in eine geschützte, gemeinsame europäische Forschungsinfrastruktur investieren, die auf den FAIR-Prinzipien [siehe unten] beruht und es Forschenden und politischen Entscheidungsträgern ermöglicht, unter uneingeschränkter Achtung der geltenden Rechtsvorschriften zum Schutz der Privatsphäre und zum Datenschutz auch auf sensible, nicht öffentliche Daten über den Schutz Minderjähriger im Internet zuzugreifen.

Gemeinsame Infrastrukturen sollten gemäß den FAIR-Prinzipien für das Forschungsdatenmanagement (FAIR: Findability, Accessibility, Interoperability, and Reusability – Auffindbarkeit, Zugänglichkeit, Interoperabilität und Wiederverwendbarkeit)^j arbeiten, um die Robustheit, Zuverlässigkeit und Wiederverwendbarkeit von Daten und Forschung zu gewährleisten. Es sollte mit der Forschungsgemeinschaft zusammengearbeitet werden, um eine kontinuierliche Verbesserung und Verfügbarkeit von Daten und den Einsatz methodischer Innovationen zu gewährleisten.

Soziale Medien und andere Anbieter digitaler Dienste sollten ermutigt werden, zur Entwicklung einer gemeinsamen Forschungsinfrastruktur beizutragen, um die Evidenzbasis für Maßnahmen zum Schutz Minderjähriger im Internet zu stärken.

EMPFEHLUNG 5

Vorschriften über den Zugang der Forschung zu Daten und über die Kontrolle stärker durchsetzen

Mit der delegierten Verordnung über Datenzugang nach Artikel 40 des Gesetzes über digitale Dienste vom Juli 2025 wurde zugelassenen Forschenden grundsätzlich ein neuer Weg eröffnet, Zugang zu Daten von Online-Plattformen zu erhalten. Diese Daten können für Forschungsarbeiten verwendet werden, die dabei helfen werden, systemimmanente Risiken zu erkennen, festzustellen und zu verstehen sowie Risikominderungsmaßnahmen zur Förderung der Sicherheit von Kindern online zu bewerten.

^j. Die FAIR-Prinzipien für das Forschungsdatenmanagement wurden erstmals 2016 in einem Artikel in der Zeitschrift *Scientific Data* vorgestellt. Ziel ist es, die Infrastruktur für die Nachnutzung von Forschungsdaten zu verbessern, indem Maschinen und Menschen das Auffinden und Nutzen von Daten erleichtert wird. Siehe Wilkinson, M. D. et al., [The FAIR Guiding Principles for scientific data management and stewardship](#), *Scientific Data*, 3, 2016.

Ob die verfolgten Ziele erreicht werden, hängt davon ab, ob die Vorschriften von den Anbietern sozialer Medien und anderer digitaler Dienste eingehalten und von den Regulierungsbehörden wirksam durchgesetzt werden. Der Erfolg ist auch von der Bandbreite der abgedeckten Dienste und von der Qualität und der Kontinuität der zur Verfügung gestellten Daten abhängig. Die Kommission sollte die praktische Wirksamkeit des Artikels 40 über Datenzugang und Kontrolle unter Berücksichtigung der ersten Erfahrungen von Forschenden mit der delegierten Verordnung prüfen. Nur so kann sichergestellt werden, dass Online-Plattformen Anträgen auf Datenzugang aus Compliance-Gründen, für Risikobewertungen und zu Forschungszwecken nachkommen.

Die Verpflichtungen zur Datenauskunft sind nicht nur ein zentraler Bestandteil der Transparenzvorschriften des DSA, sondern fallen auch unter die umfassendere Verantwortung der Anbieter sozialer Medien und anderer digitaler Dienste für Risikominderung. Angesichts der Risiken, die kleinere Plattformen für Minderjährige darstellen, und der Rolle einer unabhängigen Kontrolle bei der Bewältigung dieser Risiken sollten auch diese Plattformen ermutigt werden, der Forschung Zugang zu Daten zu gewähren. Bei der Umsetzung von Artikel 40 sollten standardmäßig die FAIR-Prinzipien für das Forschungsdatenmanagement angewandt werden.

03

Minderjährige in der sich rasch wandelnden Welt der sozialen Medien+ schützen

Im vorhergehenden Kapitel wurden die vielfältigen Risiken untersucht, denen Kinder und Jugendliche durch die Nutzung sozialer Medien und anderer digitaler Dienste in Bezug auf ihre körperliche und psychische Gesundheit und ihr Wohlbefinden ausgesetzt sind, und es wurde untersucht, wie sich diese Risiken mit sozialen und individuellen Faktoren überschneiden, die die Gefährdung Minderjähriger erhöhen.

In diesem Kapitel wird untersucht, wie diesen Risiken mit den bestehenden Rechtsvorschriften und Instrumenten, die der EU und ihren Mitgliedstaaten derzeit zur Verfügung stehen, begegnet und die Sicherheit von Kindern im Internet gestärkt wird.

Diese Analyse stützt sich auf die Säulen 3 und 4 der Sechs Leitprinzipien, die von den Ko-Vorsitzenden vorgelegt wurden, um die Bemühungen zur Verbesserung der Sicherheit von Kindern im Internet zu steuern: Kinderschutz, Rechenschaftspflicht der Anbieter sozialer Medien und anderer digitaler Dienste sowie Verbraucherrechte. In diesem Kapitel werden zunächst die wichtigsten Rechtsinstrumente und Tools untersucht, die der EU und den Mitgliedstaaten zur Verfügung stehen, und Beispiele für ihre bisherige erfolgreiche Durchsetzung hervorgehoben.

Diese wichtigsten Rechtsinstrumente der EU im Bereich der Sicherheit von Kindern im Internet gehörten zu den wichtigsten Ausgangspunkten für die Überlegungen der Ko-Vorsitzenden hinsichtlich der Stärkung des Online-Schutzes Minderjähriger. Die Erfassung des Inhalts und des Anwendungsbereichs der leistungsstärksten Instrumente auf EU-Ebene und die Ermittlung von Lücken in den Rechtsvorschriften und/oder bei der Durchsetzung gehörten ebenfalls zu den wichtigsten Themen, die in den Sitzungen des Sonderausschusses erörtert wurden.

Es wird allgemein anerkannt, dass die EU einen leistungsstarken Rechtsrahmen geschaffen hat – doch Technologien entwickeln sich schnell, Geschäftsmodelle werden angepasst, neue Funktionen kommen auf und die Regulierungsbehörden müssen sich entsprechend anpassen, sei es bei der Durchsetzung bestehender Vorschriften oder bei der Schließung von Lücken. Der Schutz Minderjähriger in einem sich rasch verändernden Umfeld der sozialen Medien+ erfordert eine kontinuierliche Bewertung und Aufmerksamkeit, um mit dem Entwicklungstempo Schritt zu halten.

Im Abschnitt „Unerledigte Angelegenheiten“ werden mehrere Bereiche genannt, in denen die bestehenden Instrumente und Werkzeuge gestärkt werden müssen. Das Kapitel schließt mit einer Reihe von Empfehlungen zur besseren Durchsetzung dieser bestehenden Instrumente, zur wirkungsvolleren Bekämpfung schädlicher Praktiken sowie Merkmalen und Funktionen, die von sozialen Medien und anderen digitalen Diensten zur Stärkung der Sicherheit von Kindern im Internet eingesetzt werden.

Die Notwendigkeit eines altersgerechten Schutzes von Kindern im Internet

Wie in Kapitel 1 dargelegt, muss ein wirksamer Ansatz für die Sicherheit von Kindern im Internet auf dem Verständnis beruhen, dass die Entwicklung von Kindern und Jugendlichen in Phasen erfolgt. Auf ihrem Weg ins Erwachsenenalter sind Minderjährige zu verschiedenen Zeitpunkten besonderen Risiken ausgesetzt. Inwiefern Kinder und Jugendliche für die Bewältigung dieser Risiken gerüstet sind, wird teilweise auch durch ihre sich entwickelnden Fähigkeiten bestimmt.

Ausgangspunkt dieser Analyse sind die auf internationaler und auf EU-Ebene bestehenden Rechtsrahmen zur Gewährleistung der Rechte des Kindes^a. Maßnahmen zur Förderung der Sicherheit von Kindern im Internet müssen auf der Anerkennung ihrer Rechte beruhen. Die sich verändernden Rollen von Betreuungspersonen und Pädagogen bei der Beaufsichtigung der Nutzung sozialer Medien und anderer digitaler Dienste durch Minderjährige müssen sich auch in den Instrumenten zum Schutz von Kindern besser widerspiegeln.

Die zunehmende politische Dynamik, den Zugang von Kindern und Jugendlichen zu potenziell schädlichen sozialen Medien und anderen digitalen Diensten sowie deren Nutzung einzuschränken, ist ein Schritt in die richtige Richtung hin zu einem entwicklungssensibleren Ansatz für die Sicherheit von Kindern im Internet. Erste Ergebnisse aus Ländern, die pauschale Altersbeschränkungen für den Zugang zu sozialen Medien eingeführt haben (beispielsweise Australien), zeigen, dass die meisten Minderjährigen einen Weg finden, diese Maßnahmen zu umgehen²³³.

Andererseits haben sich einige Minderjährige aus riskanten sozialen Medien⁺ zurückgezogen und haben nun mehr Zeit für Offline-Aktivitäten (wie Sport und persönliche Begegnungen). Dies zeigt, dass ein progressiver Wandel bei den Normen für die Nutzung sozialer Medien⁺ und anderer digitaler Dienste durch Minderjährige möglich ist und anerkannt werden muss.

Es bestehen jedoch nach wie vor mehrere Herausforderungen bei der erfolgreichen Einführung von Altersbeschränkungen, um den Schutz von Minderjährigen im Internet zu verstärken und es ihnen zu ermöglichen, die in der digitalen Welt bestehenden Möglichkeiten zu nutzen. Auf diese Herausforderungen wird an späterer Stelle in diesem Kapitel im Abschnitt „Unerledigte Angelegenheiten“ eingegangen.

a. Insbesondere das Übereinkommen der Vereinten Nationen über die Rechte des Kindes und die Allgemeinen Bemerkungen des Ausschusses für die Rechte des Kindes, die Charta der Grundrechte der Europäischen Union und die EU-Kinderrechtsstrategie.

Gewährleistung sicherer Gestaltungsmerkmale von Online-Angeboten

Es gibt immer mehr Belege für die potenziell schädlichen Auswirkungen der Nutzung sozialer Medien und anderer digitaler Dienste durch Minderjährige, wie in Kapitel 2 untersucht. Die Risiken, denen Kinder und Jugendliche in sozialen Medien+ ausgesetzt sind, entstehen nicht zufällig. In vielen Fällen sind sie das Ergebnis bewusster Entscheidungen von Anbietern sozialer Medien und anderer digitaler Dienste, die darauf abzielen, den Grad der Interaktion der Nutzerinnen und Nutzer zu maximieren, darunter auch für Minderjährige, die leicht auf diese Angebote zugreifen können. Die kontinuierliche Weiterentwicklung der sozialen Medien+ mit dem Ziel, die Interaktion der Nutzerinnen und Nutzer zu erfassen und aufrechtzuerhalten, ist Teil der Kerngeschäftsmodelle vieler Anbieter geworden.

Inzwischen wird zunehmend gefordert, dass die Regulierungsbehörden einen risikobasierten Ansatz verfolgen und inhärente Risiken, die bestimmte Merkmale und Funktionen für Kinder und Jugendliche mit sich bringen, einschließlich süchtigmachender oder zwanghafter Nutzung, in Angriff nehmen, um sicherzustellen, dass soziale Medien und andere digitale Dienste „safe by design“ sind. Trotz vieler Beispiele für eine erfolgreiche Durchsetzung bei der Bewältigung solcher Probleme befinden sich die Regulierungsbehörden häufig in der Defensive.

Derzeit müssen sie in der Regel nachweisen, dass bestimmte Merkmale und Funktionen schädlich sind, nachdem sie auf dem Binnenmarkt eingeführt und möglicherweise von Millionen von Kindern und Jugendlichen genutzt wurden. Anbieter sozialer Medien und anderer digitaler Dienste sollten mehr Verantwortung dafür übernehmen, sicherzustellen und nachzuweisen, dass Merkmale in ihren Diensten nicht schädlich sind, bevor sie sie Minderjährigen zur Verfügung stellen.

Daher könnte es zur Regel werden, dass Anbieter sozialer Medien und anderer digitaler Dienste bei der Einführung, Betreibung oder Aktualisierung potenziell für Kinder und Jugendliche risikobehafteter Dienste vor der Markteinführung nachweisen müssen, dass diese Dienste oder neuen Funktionen für Minderjährige sicher sind. Der Schutz von Kindern und Jugendlichen sollte integraler Bestandteil der Architektur sozialer Medien+ und bereits am Beginn ihrer Entwicklung und Gestaltung ein wichtiger Standard sein.

„Kein Spielzeug, kein Arzneimittel und kein Fahrzeug erreicht Kinder, ohne dass vor der Markteinführung eine unabhängige Bewertung vorgenommen wird; digitale Produkte sind die auffällige Ausnahme. Sie werden erst geprüft, nachdem Schäden bereits sichtbar geworden sind.“

— ALEX COONEY,

GESCHÄFTSFÜHRERIN UND
MITBEGRÜNDERIN VON CYBERSAFEKIDS

Durchsetzung und Evaluierung stärken

Nicht zuletzt muss auch die Durchsetzung der bestehenden Rechtsvorschriften auf nationaler und EU-Ebene gestärkt werden. Die EU verfügt über eines der weltweit modernsten legislativen Instrumentarien, das sie nutzen kann, um sicherzustellen, dass Minderjährige sicher und vertrauensvoll in der Online-Welt navigieren können. Die Wirksamkeit dieser Vorschriften hängt jedoch von ihrer Durchsetzung ab. Lücken in den bestehenden Rechtsvorschriften müssen geschlossen und die Zusammenarbeit zwischen den Regulierungsbehörden auf nationaler und EU-Ebene muss verstärkt werden.

Möglicherweise sind zusätzliche Ressourcen erforderlich, um die Durchsetzungskapazitäten zu verbessern. Die Bewertung der bestehenden Instrumente ist von entscheidender Bedeutung, um sicherzustellen, dass die Rechtsvorschriften und ihre Durchsetzung Ergebnisse bringen. Die Zivilgesellschaft und Forschende können in dieser Hinsicht einen wichtigen Beitrag leisten. Ihre Rolle sollte gestärkt werden, um sicherzustellen, dass Rechtsvorschriften wirksam konzipiert und umgesetzt werden, um das Ziel zu erreichen, Kindern und Jugendlichen im Internet ein sicheres Heranwachsen zu ermöglichen.

Geltendes EU-Recht

Im folgenden Abschnitt werden die bestehenden EU-Rechtsvorschriften und -Instrumente untersucht, die der EU und den Mitgliedstaaten für den Schutz Minderjähriger im Internet^b zur Verfügung stehen. Schwerpunkt dieser Analyse sind die EU-Rechtsvorschriften, die nach Ansicht der Ko-Vorsitzenden des Sonderausschusses weiter gestärkt oder verstärkt durchgesetzt werden müssen. Natürlich gibt es viele wichtige Instrumente, die in diesem Kapitel nicht im Einzelnen untersucht werden, aber ein wesentlicher Bestandteil der bestehenden EU-Politik sind.

Dazu gehören insbesondere der Rahmenbeschluss zur Bekämpfung von Rassismus und Fremdenfeindlichkeit aus dem Jahr 2008, die Richtlinie zur Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt, die Richtlinie über Verfahrensgarantien in Strafverfahren für Kinder, die Verdächtige oder beschuldigte Personen in Strafverfahren sind, die Opferschutzrichtlinie und die Empfehlung der Kommission zu integrierten Kinderschutzsystemen.

Präventive Maßnahmen wie digitale Bildung und Kompetenzen (einschließlich KI-Kompetenzen), Bildung zu Aspekten des persönlichen Wohlergehens sowie die Unterstützung von Minderjährigen, Betreuungspersonen und Pädagogen werden in Kapitel 4 untersucht, dessen Schwerpunkt die Stärkung der Rolle von Kindern und Jugendlichen im Internet ist.

GESETZ ÜBER DIGITALE DIENSTE („DIGITAL SERVICES ACT“) UND LEITLINIEN ZUM SCHUTZ MINDERJÄHRIGER

Das Gesetz über digitale Dienste enthält vollständig harmonisierte Vorschriften für die Erbringung von Vermittlungsdiensten, um ein sicheres, berechenbares und vertrauenswürdiges Online-Umfeld zu schaffen, in dem die Rechte der Nutzerinnen und Nutzer, insbesondere von Minderjährigen, geachtet werden. Das Gesetz über digitale Dienste wurde 2022 angenommen und gilt seit dem 25. August 2023

b. Anmerkung: In den folgenden Abschnitten dieses Kapitels werden die Begriffe „Kinder“ und „Minderjährige“ so verwendet, wie sie in bestimmten Rechtsinstrumenten verwendet werden.

uneingeschränkt für sehr große Online-Plattformen und sehr große Online-Suchmaschinen^c. Das Gesetz über digitale Dienste gilt seit dem 17. Februar 2024 für alle anderen in seinen Anwendungsbereich fallenden Dienste.

Angesichts der Zunahme digitaler Dienste, die im digitalen Zeitalter zu einem wichtigen Bestandteil unseres täglichen Lebens geworden sind, werden mit dem Gesetz über digitale Dienste die seit 2000 in der Richtlinie über den elektronischen Geschäftsverkehr verankerten Grundprinzipien weiterentwickelt, um neuen Online-Risiken und -Herausforderungen für Minderjährige zu begegnen und ein verantwortungsvolles Verhalten der Anbieter digitaler Dienste zu fördern.

Letztlich soll mit dem Gesetz über digitale Dienste ein Online-Umfeld geschaffen werden, in dem alle ihre Grundrechte wahrnehmen können. Dazu gehört auch, dass Online-Plattformen verpflichtet werden, für ein hohes Maß an Privatsphäre, Sicherheit und Schutz von Minderjährigen online zu sorgen²³⁴.

Geltungsbereich

Im Gesetz über digitale Dienste werden insbesondere Anbieter von Vermittlungsdiensten reguliert. Dabei handelt es sich um digitale Dienste, die das Hosting von Inhalten und Interaktionen Dritter online erleichtern. Die Definition des Begriffs „Vermittlungsdienste“ umfasst Anbieter, die lediglich Informationen übermitteln (z. B. Internetdiensteanbieter), „Caching“-Dienste (Übermittlung von Informationen mit vorübergehender Speicherung), darunter auch Netzbetreiber, und das Hosting von Daten auf Anfrage von Nutzern (z. B. Cloud-Anbieter und Online-Plattformen).

Vermittlungsdienste umfassen beispielsweise alle Online-Plattformen wie Online-Marktplätze, soziale Medien, Online-Spiele oder Videospiele, auf denen Nutzer spielen und ihre eigenen Inhalte erstellen können (es sei denn, diese Funktionen sind nur geringfügige „Add-ons“ zu einem bestehenden Videospiel), App-Stores, Video-Sharing- und Streaming-Websites sowie Online-Plattformen, auf denen Nutzerinnen und Nutzer Inhalte einsehen, posten und teilen können.

Das Gesetz über digitale Dienste gilt nicht für private oder direkte (interpersonelle) Messaging-Dienste oder -funktionen und auch nicht für digitale Dienste ohne Vermittlungsfunktion^d. Um die Verhältnismäßigkeit zu gewährleisten, gelten einige der Verpflichtungen, die Online-Plattformen durch das Gesetz über digitale Dienste auferlegt werden, nicht für Anbieter von Online-Plattformen, die aufgrund ihres Umsatzes und der Zahl ihrer Mitarbeiter Kleinst- oder Kleinunternehmen sind. Diese Ausnahme gilt nicht, wenn diese Dienste angesichts der Zahl ihrer Nutzer als sehr große Online-Plattformen ausgewiesen sind.

Durchsetzung

Mit dem Gesetz über digitale Dienste wird die Kommission ermächtigt, auf der Grundlage eines breiten Spektrums von Risiken für Minderjährige förmliche Prüfverfahren gegen die größten Plattformen einzuleiten und gleichzeitig flexibel auf neue Risiken und technologische Entwicklungen zu reagieren. Diese Prüfverfahren müssen jederzeit im Einklang mit dem ordnungsgemäßen Verfahrensablauf und allen anderen erforderlichen Rechtsgarantien für Unternehmen stehen.

- c.** Als „sehr große Online-Plattformen“ und „sehr große Online-Suchmaschinen“ sind im Rahmen des Gesetzes über digitale Dienste alle Dienste mit monatlich mehr als 45 Millionen aktiven Nutzerinnen und Nutzern in der EU definiert.
- d.** Der Begriff „Vermittlungsfunktion“ bezieht sich auf Dienste, die die Übertragung von Inhalten Dritter zwischen verschiedenen Nutzerinnen und Nutzern des betreffenden Dienstes erleichtern. Als Beispiele für nicht vermittelnde Dienste können Online-Einzelhändler, viele Videospiele ohne Interaktion mit Dritten oder Erstellung von Inhalten sowie einzelne Websites oder Apps genannt werden.

Angesichts der vollständig harmonisierten Vorschriften des Gesetzes über digitale Dienste, bei dem es sich um eine unmittelbar geltende Verordnung handelt, können die EU-Mitgliedstaaten keine nationalen Rechtsvorschriften erlassen oder beibehalten, die das Gesetz über digitale Dienste duplizieren oder den Anbietern von Vermittlungsdiensten Verpflichtungen auferlegen. Dazu gehört auch, Online-Plattformen Verpflichtungen zur Altersüberprüfung aufzuerlegen.

Dies würde die direkte und einheitliche Anwendung der Vorschriften im gesamten Binnenmarkt beeinträchtigen. Durch das nationale Recht kann jedoch im Einklang mit dem Unionsrecht ein Mindestalter für den Zugang zu bestimmten Produkten oder Dienstleistungen vorgeschrieben werden, wie auch in den Leitlinien der Kommission zum Schutz Minderjähriger dargelegt.

Die Durchsetzung des Gesetzes über digitale Dienste beruht auf einem System geteilter Aufsichts- und Durchsetzungsbefugnisse zwischen der nationalen und der EU-Ebene. Die ausschließliche Zuständigkeit für die Überwachung sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen (siehe unten) liegt bei der Kommission.

Sehr große Online-Plattformen und sehr große Online-Suchmaschinen

Im Rahmen des Gesetzes über digitale Dienste gelten für sehr große Online-Plattformen und sehr große Online-Suchmaschinen^e angesichts ihrer großen Reichweite und ihres großen Einflusses zusätzliche Verpflichtungen. Mit diesen Verpflichtungen werden Bedenken hinsichtlich der weitverbreiteten Risiken, die diese Dienste verursachen können, Rechnung getragen, denen höchste Standards der Sorgfaltspflicht gegenüberstehen.

Gemäß dem Gesetz über digitale Dienste²³⁵ müssen sehr große Online-Plattformen und sehr große Online-Suchmaschinen proaktiv tatsächliche und vorhersehbare systemische Risiken ermitteln, bewerten und mindern, die sich aus der Erbringung ihrer Dienste ergeben, darunter auch Risiken, die Minderjährige betreffen. Bei Plattformen mit weniger als 45 Millionen monatlichen Nutzern sind die nationalen Behörden des EU-Mitgliedstaats, in dem das Unternehmen seinen Sitz hat, für die Durchsetzung des Gesetzes über digitale Dienste zuständig.

Sehr große Online-Plattformen und sehr große Online-Suchmaschinen müssen angemessene, verhältnismäßige und wirksame Maßnahmen ergreifen, um die ermittelten Risiken zu mindern. Dies kann die Anpassung der Gestaltung, der Merkmale und der Funktionsweise ihrer Dienste sowie die Anpassung algorithmischer Systeme, die als Teil ihrer Dienste eingesetzt werden, umfassen. Sehr große Online-Plattformen und sehr große Online-Suchmaschinen müssen Nutzerinnen und Nutzern für jedes ihrer Empfehlungssysteme mindestens eine Option anbieten, die nicht auf Profiling beruht.

Da die Überprüfung durch unabhängige Sachverständige sichergestellt werden muss, unterliegen Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen hinsichtlich der Einhaltung ihrer Verpflichtungen aus dem Gesetz über digitale Dienste einer Rechenschaftspflicht, deren Umsetzung durch unabhängige Prüfungen sichergestellt wird.

e. Die vollständige Liste der benannten sehr großen Online-Plattformen und sehr großen Online-Suchmaschinen ist abrufbar unter Europäische Kommission (2026), [Supervision of the designated very large online platforms and search engines under DSA](#).

Im Gesetz über digitale Dienste verankerte Leitlinien zum Schutz Minderjähriger

In den im Gesetz über digitale Dienste verankerten Leitlinien zum Schutz Minderjähriger ist der Maßstab für die Durchsetzung festgelegt, um sicherzustellen, dass alle Online-Plattformen, die Minderjährigen zugänglich sind, ein hohes Maß an Privatsphäre, Sicherheit und Schutz für Minderjährige aufweisen, die ihre Dienste nutzen.

Zu den wichtigsten in den Leitlinien empfohlenen Maßnahmen gehören:

- // Die Konten von Minderjährigen werden durch Voreinstellung auf das höchste Maß an Datenschutz, Sicherheit und Schutz gebracht, beispielsweise in Bezug auf Geolokalisierung und Empfehlungen anderer Konten.
- // Wenn bestimmte Produkte oder Dienstleistungen ein hohes Risiko für Minderjährige bergen (beispielsweise durch den Zugang zu pornografischen Inhalten) und wenn diese Risiken nicht durch weniger restriktive Maßnahmen gemindert werden können, wird eine Altersüberprüfung eingerichtet. Es wird klar festgelegt, was die Plattform als Inhalte und Verhaltensweisen ansieht, die für Minderjährige schädlich sind. Dies schließt alle Inhalte und Verhaltensweisen ein, die nach dem Recht der Union oder der Mitgliedstaaten rechtswidrig sind. Es werden Informationen über diese Standards und Erwartungen übermittelt. Es werden Moderationsstrategien und -verfahren festgelegt, in denen definiert ist, wie Inhalte und Verhaltensweisen erkannt und moderiert werden, um die Exposition Minderjähriger gegenüber diesen Inhalten zu begrenzen.
- // Es wird verhindert, dass über unbekannte Konten Kontakt mit Minderjährigen aufgenommen wird; die personenbezogenen Informationen, Daten und Inhalte in sozialen Medien bleiben gegenüber Konten, mit denen sie nicht in Verbindung stehen, verborgen. So haben beispielsweise zwei benannte sehr große Online-Plattformen die Profile von Nutzerinnen und Nutzern unter 16 Jahren automatisch auf „privat“ gesetzt. Dies bedeutet, dass die von ihnen hochgeladenen Videos nur von den von ihnen genehmigten Personen eingesehen werden können.

„Die Leitlinien von Artikel 28 des Gesetzes über digitale Dienste sollten als für digitale Anbieter verbindlich erklärt werden. Dies wäre wirksam und legitim, stünde im Einklang mit den geltenden Rechts- und Regulierungsvorschriften und wäre vor allem ein entscheidendes Mittel zur Wahrung der Rechte von Kindern im digitalen Umfeld.“

— SONIA LIVINGSTONE,

PROFESSORIN AN DER LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE UND MITGLIED DES EU KIDS ONLINE-NETZWERKS

- // Um sexuelle Erpressung zu verhindern, wird verboten, dass Screenshots von Inhalten heruntergeladen oder erstellt werden, die von Minderjährigen veröffentlicht wurden.
- // Empfehlungssysteme werden verändert, um das Risiko zu verringern, dass Minderjährige auf schädliche Inhalte stoßen oder durch sogenannte Rabbit-Hole-Effekte gebunden werden, bei denen Minderjährige längeren Inhaltsketten im Zusammenhang mit Essstörungen, Selbstverletzung oder Selbstmord ausgesetzt sind.
- // Es werden Schutzvorkehrungen für KI-Chatbots eingeführt, die in Online-Plattformen integriert sind. Minderjährige werden gewarnt, dass sich Interaktionen mit einer KI-Funktion von menschlichen Interaktionen unterscheiden und dass die durch solche Funktionen bereitgestellten Informationen sachlich falsch oder irreführend sein können.
- // Es werden Maßnahmen zur Verbesserung der Moderationsinstrumente eingeführt. Es wird sichergestellt, dass die Melde-, Feedback- und Beschwerdemechanismen für die Nutzerinnen und Nutzer wirksam, sichtbar, kinderfreundlich und leicht zugänglich sind. Es wird sichergestellt, dass solche Mechanismen eine Berichterstattung und Rückmeldung über alle relevanten Elemente der Erfahrungen Minderjähriger auf der Plattform ermöglichen.
- // Es werden Mindestanforderungen an Instrumente zur elterlichen Kontrolle festgelegt. Diese Instrumente sollten altersgerecht, benutzerfreundlich, und leicht zugänglich und aktivierbar sein. Sie sollten auch interoperabel und wirksam sein und das Recht Minderjähriger auf Privatsphäre oder auf Zugang zu Diensten nicht unverhältnismäßig einschränken.
- // Es werden Tools zur Nutzerunterstützung eingeführt. Dazu gehören direkt sichtbare Warnmeldungen, und Links zu einschlägigen Hilfsangeboten oder anderen Quellen, wenn Minderjährige potenziell illegale Inhalte suchen, hochladen, generieren, teilen und empfangen. Es könnten auch Optionen zur Gewährleistung der Kontrolle über die Erfahrungen Minderjähriger in Form der Einschränkung von Interaktionen und Kontakten eingesetzt werden.
- // Der Schutz Minderjähriger vor wirtschaftlich ausbeuterischen Praktiken wird gewährleistet. Minderjährige dürfen nicht Praktiken und Techniken ausgesetzt werden, die übermäßige oder unerwünschte Ausgaben oder Suchtverhalten verursachen können (z. B. bezahlte Lootboxen).
- // Es werden Governance-Praktiken festgelegt, einschließlich interner Strategien, Verfahren, Rollen und Zuständigkeiten, um eine Sicherheitskultur für Minderjährige im eigenen Dienst zu fördern.
- // Es wird sichergestellt, dass alle Informationen, Warnhinweise und sonstigen Mitteilungen kinderfreundlich, altersgerecht, leicht verständlich und für alle Minderjährigen zugänglich sowie an der jeweiligen Nutzungsstelle klar dargestellt sind. Allgemein werden im Rahmen des Gesetzes über digitale Dienste alle Nutzerinnen und Nutzer, darunter auch Minderjährige, durch Mindestanforderungen geschützt (beispielsweise müssen Online-Plattformen ihre allgemeinen Geschäftsbedingungen in der Sprache des jeweiligen EU-Mitgliedstaats verständlich machen, damit die Nutzerinnen und Nutzer, darunter auch Minderjährige, die von ihnen akzeptierten allgemeinen Geschäftsbedingungen kennen).

Ein risikobasierter Ansatz

In den Leitlinien des Gesetzes über digitale Dienste wird ein risikobasierter Ansatz verfolgt, da sich Art und Grad des für Minderjährige bestehenden Risikos zwischen den verschiedenen Online-Plattformen unterscheiden können. In den Leitlinien wird anerkannt, dass diese Risiken je nach Größe, Reichweite und Art der Plattform, ihrer Art, ihrer beabsichtigten oder gegenwärtigen Nutzung, ihrer Merkmale und ihrer Nutzerbasis sowie ihrer Auswirkungen auf die Rechte von Kindern und weitere Rechte und Freiheiten variieren können. Die Plattformen sollten diese Faktoren bei der Anwendung der Leitlinien berücksichtigen.

Im Einklang mit diesem risikobasierten Ansatz wird in den Leitlinien dargelegt, wie Anbieter ihren Verpflichtungen zur Gewährleistung eines hohen Maßes an Privatsphäre, Sicherheit und Schutz von Minderjährigen in verhältnismäßiger und angemessener Weise nachkommen sollten. Die Anbieter sollten die Auswirkungen der von ihnen ergriffenen Schutzmaßnahmen auf die Rechte von Kindern und auf andere Rechte und Freiheiten berücksichtigen und sich dabei auf die höchsten verfügbaren Standards, die Perspektive und die Rechte von Kindern stützen. Wenn es Hinweise darauf gibt, dass eine Praxis, ein Merkmal oder eine Gestaltungsoption Risiken für Kinder birgt, sollte das Vorsorgeprinzip angewandt und eingehalten werden, bis Nachweise dafür vorliegen, dass die betreffenden Aspekte nicht schädlich sind.

Spezifische Verbote im Rahmen des Gesetzes über digitale Dienste

In Bezug auf Werbung ist es Anbietern von Online-Plattformen nach dem Gesetz über digitale Dienste verboten, Werbung auf der Grundlage von Profiling unter Verwendung der personenbezogenen Daten Minderjähriger anzuzeigen, wenn sie mit hinreichender Sicherheit wissen, dass der Nutzer des Dienstes minderjährig ist.

Auch „Dark Patterns“ sind durch das Gesetz über digitale Dienste verboten. Dies bezieht sich auf eine Art und Weise der Gestaltung von Online-Schnittstellen, durch die Nutzerinnen und Nutzer dazu bewegt oder dahin gehend manipuliert werden sollen, bestimmte Entscheidungen zu treffen, die ihren Interessen zuwiderlaufen. Das Verbot von Dark Patterns gilt in Situationen, die nicht bereits unter das Verbraucherrecht (Richtlinie über unlautere Geschäftspraktiken, UGP-Richtlinie) und die Datenschutzvorschriften (Datenschutz-Grundverordnung (DSGVO)) fallen.

Vertrauenswürdige Hinweisgeber

Das Gesetz über digitale Dienste erleichtert auch die Meldung illegaler Inhalte (wie rechtswidrige Hassrede und Darstellungen sexuellen Missbrauchs von Kindern) und Waren durch Nutzerinnen und Nutzer, indem benutzerfreundliche Kennzeichnungssysteme, darunter auch für Minderjährige, vorgeschrieben werden. Organisationen der Zivilgesellschaft, die Expertinnen und Experte für die Erkennung bestimmter Arten illegaler Online-Inhalte sind, kann der Status eines „vertrauenswürdigen Hinweisgebers“ zuerkannt werden.

Wenn vertrauenswürdige Hinweisgeber Plattformen auf illegale Inhalte hinweisen, werden diese Hinweise vorrangig behandelt. Derzeit haben die Koordinatoren für digitale Dienste mehr als 70 Organisationen als vertrauenswürdige Hinweisgeber benannt, die Kompetenzbereiche wie den Schutz von Minderjährigen im Internet, Betrug bis hin zum Kampf gegen Produktfälschungen vertreten.

DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO)

In der Datenschutz-Grundverordnung (DSGVO) wird bei der Verarbeitung personenbezogener Daten ein risikobasierter Ansatz verfolgt. Je größer das Risiko ist, das die Verarbeitung personenbezogener Daten für die Rechte und Freiheiten natürlicher Personen darstellt, desto stringenter sind die den für die Verarbeitung Verantwortlichen auferlegten Verpflichtungen und desto strenger sind die zu treffenden Sicherheitsvorkehrungen.

In der DSGVO ist ausdrücklich vorgesehen, dass Kinder besonderen Schutz verdienen. Wenn Kinder auf einen Online-Dienst zugreifen, muss sichergestellt sein, dass durch konkrete Datenschutzmaßnahmen ein angemessenes Niveau des Schutzes gegenüber den Risiken, die sich aus der Nutzung des Dienstes durch Kinder ergeben, gewährleistet ist. In der Verordnung wird anerkannt, dass Kinder die Risiken und Folgen der Verwendung ihrer personenbezogenen Daten möglicherweise nicht in vollem Umfang absehen können.

Einschlägige Datenschutzgrundsätze

Organisationen, die Daten verarbeiten, müssen die Datenschutzgrundsätze einhalten, die für den Schutz von Kindern im Internet von großer Bedeutung sind. So sind Organisationen nach dem Grundsatz der Datenminimierung verpflichtet, die Menge der von Kindern erhobenen Daten und deren anschließende Nutzung so gering wie möglich zu halten.

Nach dem Grundsatz der Zweckbindung dürfen Daten von Kindern, die für einen bestimmten Zweck erhoben werden, von der Organisation nicht für andere Zwecke verwendet werden. Nach dem Grundsatz der Integrität und Vertraulichkeit muss die Organisation geeignete Sicherheitsmaßnahmen ergreifen, um die Daten des Kindes vor unrechtmäßiger oder unbefugter Verwendung zu schützen.

Eine weitere wichtige Maßnahme ist die Verpflichtung für Organisationen, die personenbezogene Daten erheben und verwenden, die Datenschutzbestimmungen durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen ²³⁶ einzuhalten. Dies setzt voraus, dass Datenschutzmaßnahmen technisch in den Dienst integriert sind und dass standardmäßig die strengsten Datenschutzstandards zur Anwendung kommen.

Durch diese Anforderungen wird auch verlangt, dass die Organisation geeignete technische und organisatorische Maßnahmen zum Schutz Minderjähriger ergreift. Die Einhaltung dieses Grundsatzes kann je nach angebotenen Dienst und Risiko für die betroffene Person unterschiedliche Maßnahmen erfordern. Beispiele für solche Maßnahmen:

- // Sicherstellen, dass personenbezogene Daten von Kindern nicht systematisch an Dritte weitergegeben werden,
- // sicherstellen, dass die Identität oder Kontaktinformationen von Kindern Dritten nicht ohne Einwilligung der Eltern zur Verfügung gestellt werden,
- // standardmäßiges Abschalten der Geolokalisierung,
- // Vermeidung von Techniken des „Nudging“, die Kinder dazu ermutigen oder anregen, unnötige Informationen bereitzustellen.

In der DSGVO sind auch spezifische Transparenzanforderungen für Kinder festgelegt. Wenn Kinder ein Produkt oder einen Dienst nutzen, das bzw. der ihre personenbezogenen Daten verarbeitet (beispielsweise, wenn sie ein Konto bei einem bestimmten Dienst haben), müssen in klarer und einfacher Sprache leicht zugängliche Erläuterungen über die Art und Weise der Verwendung der personenbezogenen Daten des Kindes bereitgestellt werden.

Dies ist besonders wichtig, da einige Kinder nicht wissen, was mit dem Begriff „personenbezogene Daten“ gemeint ist (z. B. Fotos und Videos), und ihnen auch nicht bewusst ist, dass ihre Daten für Zwecke wie die Anpassung gezielter Werbung und In-App-Erfahrungen verwendet werden können.

Rechtsgrundlage

Ein zentrales Sicherheitsmerkmal der DSGVO besteht darin, dass die Organisation, die personenbezogene Daten verarbeitet (der Verantwortliche), über eine entsprechende Rechtsgrundlage verfügen muss. Sie muss sich auf eine der sechs Rechtsgrundlagen stützen, die mit der DSGVO geschaffen wurden ²³⁷. Bezüglich dieser sechs Rechtsgrundlagen gibt es keine Hierarchie. Die für die Verarbeitung Verantwortlichen sollten unter Berücksichtigung der Anforderungen der einzelnen Rechtsgrundlagen die am besten geeignete wählen.

Eine dieser Rechtsgrundlagen ist die Einwilligung. Die Einwilligung muss freiwillig für den bestimmten Fall, in informierter Weise und durch eine eindeutige, bestätigende Handlung abgegeben werden, und die betroffene Person muss diese Einwilligung so einfach widerrufen können, wie sie sie abgab ²³⁸. Die Einwilligung kann nicht freiwillig erteilt werden, wenn Kinder keine echte Wahl haben oder sich zur Einwilligung gezwungen fühlen. Damit die Einwilligung in informierter Weise erteilt wird, muss der Verantwortliche in klarer, einfacher, kindgerechter Sprache erläutern, wie er die von ihm erhobenen Daten zu verarbeiten beabsichtigt ²³⁹.

Wenn sich ein „Dienst der Informationsgesellschaft“^f (wie Plattformen sozialer Medien und Videospiele) auf die Einwilligung als Rechtsgrundlage stützt, können Kinder ihre Einwilligung zur Verarbeitung ihrer personenbezogenen Daten ab einem Alter von 16 Jahren erteilen.

Die DSGVO bietet den Mitgliedstaaten die Möglichkeit, dieses Alter auf ein Alter zwischen 13 und 16 Jahren zu senken. Ist das Kind jünger als 16 Jahre, ist die Verarbeitung rechtmäßig, wenn der Träger der elterlichen Verantwortung seine Einwilligung erteilt oder die erteilte Einwilligung gebilligt hat.

Die Mitgliedstaaten haben unterschiedliche Altersbereiche festgelegt, innerhalb derer sich die Dienste der Informationsgesellschaft auf die Einwilligung stützen können. Nach den Ende 2025 verfügbaren Zahlen haben sieben Mitgliedstaaten 13 Jahre als Mindestalter für die Einwilligung festgelegt, sechs Mitgliedstaaten 14 Jahre, fünf Mitgliedstaaten 15 Jahre und neun Mitgliedstaaten 16 Jahre.

Gemäß dem Grundsatz der Rechenschaftspflicht muss ein Verantwortlicher nachweisen können, dass er die DSGVO eingehalten hat. Dazu gehört auch, dass er sicherzustellen hat, dass die von ihm eingeholte Zustimmung gültig ist. In der Praxis kann es für einen Verantwortlichen jedoch schwierig sein, sicherzustellen, dass die gegebenenfalls vom Träger der elterlichen Verantwortung eingeholte Einwilligung

^f Die meisten Online-Dienste gelten als Dienste der Informationsgesellschaft. Dazu gehören Apps, Suchmaschinen, Plattformen der sozialen Medien, Online-Nachrichtendienste oder internetgestützte Sprachtelefoniedienste, Online-Marktplätze, Dienste für das Streaming von Inhalten (z. B. Video-, Musik- oder Glücksspieldienste), Nachrichten- oder Bildungswebsites sowie Websites, die Nutzerinnen und Nutzern über das Internet andere Waren oder Dienstleistungen anbieten. Siehe Artikel 4 Absatz 25 der DSGVO.

gültig ist. Es kann schwierig sein, zu bestätigen, dass die Person, die die Einwilligung für das Kind erteilt, rechtlich dazu befugt ist.

Darüber hinaus sollte ein Verantwortlicher im Einklang mit dem Grundsatz der Datenminimierung nur die zu diesem Zweck erforderlichen Daten verarbeiten und die Verarbeitung sensibler personenbezogener Daten (z. B. Dokumente, die auf sensible Betreuungsvereinbarungen hinweisen) vermeiden, um eine gültige Einwilligung angemessen nachzuweisen.

Das Erfordernis, die Zustimmung des Trägers der elterlichen Verantwortung einzuholen, gilt jedoch nicht, wenn Daten auf einer anderen Rechtsgrundlage, z. B. aufgrund eines Vertrags oder eines berechtigten Interesses, verarbeitet werden (siehe unten). Dies bedeutet, dass die zusätzlichen Garantien, die mit der Verarbeitung von Daten von Kindern auf der Grundlage einer Einwilligung einhergehen, nicht gelten, wenn sich ein Social-Media-Unternehmen auf einen dieser Gründe stützt, um die Daten von Kindern zu verarbeiten (z. B. um ein Konto eines Kindes für den Zugang zu dem Dienst und seine Interaktionen mit dem Dienst einzurichten).

Wenn eine Organisation personenbezogene Daten auf der Grundlage eines Vertrags verarbeitet, ist es Sache jedes Mitgliedstaats, das Alter festzulegen, in dem ein Kind einen Vertrag schließen kann.

Ein weiterer Grund, auf den sich Online-Dienste stützen, ist das berechtigte Interesse. Dieser Begriff bezieht sich auf die Verarbeitung personenbezogener Daten eines Kindes zur Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen oder eines Dritten, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten des Einzelnen überwiegen. Ein berechtigtes Interesse ist keine standardmäßige Rechtsgrundlage für die Verarbeitung.

Wenn Verantwortliche ein berechtigtes Interesse an der Verarbeitung personenbezogener Daten von Kindern gemäß der DSGVO geltend machen, müssen sie im Einklang mit dem Grundsatz der Rechenschaftspflicht sicherstellen, dass sie alle Anforderungen des Artikels 6 Absatz 1 Buchstabe f der DSGVO erfüllen, bevor sie die Verarbeitung durchführen^g. Eine dieser Anforderungen besteht darin, dass die Interessen oder Grundrechte und Grundfreiheiten des Kindes gegenüber dem berechtigten Interesse des Verantwortlichen oder eines Dritten nicht überwiegen dürfen²⁴⁰.

Der EuGH hat festgestellt, dass bei der Durchführung einer solchen Beurteilung durch einen Verantwortlichen der Situation, in der es sich bei der betroffenen Person um ein Kind handelt, besondere Aufmerksamkeit gewidmet werden muss. Nach Erwägungsgrund 38 der DSGVO verdienen Kinder besonderen Schutz. Darüber hinaus hat der EuGH festgestellt, dass ein solcher besonderer Schutz gelten sollte, wenn personenbezogene Daten von Kindern für Werbezwecke, zur Erstellung von Persönlichkeits- oder Nutzerprofilen oder zum Zweck des Anbietens von Diensten, die sich unmittelbar an Kinder richten, verarbeitet werden²⁴¹.

Die Verantwortlichen sollten auch das Ausmaß und die Intensität eines Eingriffs in die Rechte und Freiheiten des Kindes berücksichtigen. Sie sollten nachweisen können, dass das Wohl des Kindes als vorrangige Erwägung berücksichtigt wurde und dass geeignete Schutzmechanismen umgesetzt wurden²⁴². Bei der Abwägung widerstreitender Interessen sollte das Wohl des Kindes eine vorrangige Erwägung sein.

g. Wie der EuGH bestätigt hat, sieht Artikel 6 Absatz 1 Buchstabe f DSGVO drei kumulative Voraussetzungen für die Rechtmäßigkeit der Verarbeitung vor: „Erstens muss von dem für die Verarbeitung Verantwortlichen oder von einem Dritten ein berechtigtes Interesse wahrgenommen werden, zweitens muss die Verarbeitung der personenbezogenen Daten zur Verwirklichung des berechtigten Interesses erforderlich sein und drittens dürfen die Interessen oder Grundrechte und Grundfreiheiten [der betroffenen Person] ... nicht überwiegen“. Siehe die Rechtssache C-252/21, Meta/Bundeskartellamt (ECLI:EU:C:2023:537), Rn. 106.

Die für die Verarbeitung Verantwortlichen sollten auch die berechtigten Erwartungen eines Kindes hinsichtlich der Verwendung seiner personenbezogenen Daten berücksichtigen. Die Erwartungen des Kindes können auch je nach Alter des Kindes variieren ²⁴³. Je nach Komplexität der Verarbeitung erhöht die begrenzte Fähigkeit eines Kindes, Datenverarbeitung zu verstehen, das Risiko unerwarteter oder unverhältnismäßiger Folgen der Verarbeitung.

Es wird darauf hingewiesen, dass der Europäische Datenschutzausschuss (EDSA) der Auffassung ist, dass bestimmte Arten von Datenverarbeitungsvorgängen, z. B. umfangreiche Profilerstellung und gezielte Werbung ²⁴⁴ vorbehaltlich bestimmter begrenzter Ausnahmen im Allgemeinen nicht mit der Verpflichtung im Einklang stehen, den besonderen Schutz von Kindern zu gewährleisten ²⁴⁵.

Kollidieren die berechtigten Interessen eines Verantwortlichen mit den Interessen oder Grundrechten und Grundfreiheiten eines Kindes, so sollten im Allgemeinen die Interessen und Rechte des Kindes Vorrang haben. Ist dies nicht möglich, sollte sich ein Verantwortlicher bezüglich der Verarbeitung der Daten auf eine andere Rechtsgrundlage stützen oder diese einstellen.

Weitere einschlägige Bestimmungen

In der DSGVO ist ferner ein strengerer Schutz von Kindern im Hinblick auf das Recht auf Löschung vorgesehen, weil auch zu berücksichtigen ist, dass sich das Kind möglicherweise nicht vollständig über die mit der Verarbeitung verbundenen Risiken im Klaren war und diese Daten später löschen möchte ²⁴⁶. Sie sieht ferner vor, dass Kinder nicht Gegenstand von Profiling oder automatisierter Entscheidungsfindung ²⁴⁷ sein dürfen, und sie bietet Kindern besonderen Schutz, wenn diese das Ziel von Marketingaktivitäten sind ²⁴⁸.

Der Europäische Datenschutzausschuss (EDSA) hat festgestellt, dass „Unternehmen generell davon Abstand nehmen [sollten], bei Kindern zu Werbezwecken Profiling anzuwenden [...] und dass ein solches Profiling unter sehr begrenzten Umständen zulässig sein sollte, z.B. wenn dies zum Schutz des Wohlbefindens/Wohls des Kindes erforderlich ist ²⁴⁹.

In der DSGVO werden auch die Umstände festgelegt, unter denen eine Datenschutz-Folgenabschätzung (DSFA) erforderlich ist. In Rahmen einer DSFA müssen Organisationen die Risiken bewerten, die mit der vorgeschlagenen Verarbeitung personenbezogener Daten der Nutzer verbunden sind, und erforderlichenfalls das Risiko für Nutzer, einschließlich Kindern, verringern. Bei den Risikobewertungen müssen die unterschiedlichen Altersstufen und entwicklungsbedingten Bedürfnisse minderjähriger Nutzer berücksichtigt werden.

Bei Risikobewertungen für Kinder müssen auch die Risiken für deren allgemeines Wohlbefinden, die sich aus der Verarbeitung personenbezogener Daten von Kindern ergeben, berücksichtigt werden. Dies schließt jeden körperlichen, geistigen oder finanziellen Schaden ein, dem sie infolge der Verarbeitung ausgesetzt sein können. Bei der Durchführung einer Datenschutz-Folgenabschätzung in Bezug auf die Verarbeitung personenbezogener Daten von Kindern muss der Grundsatz des Kindeswohls eines der wichtigsten Instrumente zur Risikobewertung sein.

Ist das Risiko nach der Einführung der vorgeschlagenen Maßnahmen immer noch hoch, muss die Organisation ihre Datenschutzbehörde konsultieren. Die Datenschutzbehörde ist verpflichtet, schriftliche Empfehlungen abzugeben; ferner kann sie von ihren Befugnissen, einschließlich des Verbots der Verarbeitung, Gebrauch machen, wenn die Risiken zu hoch sind und nicht angemessen gemindert werden können ²⁵⁰.

EU-VERORDNUNG ÜBER KÜNSTLICHE INTELLIGENZ

(KI-VERORDNUNG)

Zusätzlich zum Gesetz über digitale Dienste wird mit der Verordnung über künstliche Intelligenz (KI-Verordnung) ein umfassender Rechtsrahmen für die Regulierung von KI in der EU geschaffen. Bei der Stärkung des Schutzes der Rechte des Kindes spielt die KI-Verordnung eine wichtige Rolle, indem darin die Entwicklung und der Einsatz von KI Maßnahmen zum Schutz der Gesundheit, der Sicherheit und der Grundrechte vorgeschrieben ist. Mit der KI-Verordnung wird ein risikobasierter Ansatz verfolgt und für KI-Systeme werden Vorschriften eingeführt, die auf dem möglichen Risikoniveau, das von ihnen ausgehen kann, beruhen.

Mehrere KI-Anwendungsfälle mit erheblichen Auswirkungen auf die Rechte des Kindes werden im Rahmen der KI-Verordnung als hochriskant eingestuft, z. B. Fälle, in denen KI im Bereich der allgemeinen und beruflichen Bildung eingesetzt wird. Um sicherzustellen, dass sie sicher und vertrauenswürdig sind, müssen Hochrisiko-KI-Systeme bestimmte Anforderungen wie Risikomanagement, Transparenz und menschliche Aufsicht erfüllen. Insbesondere muss das Risikomanagementsystem eines Hochrisiko-KI-Systems berücksichtigen, ob mit nachteiligen Auswirkungen auf Personen unter 18 Jahren zu rechnen ist.

Bei der Bewertung der Auswirkungen der spezifischen Verwendung eines Hochrisiko-KI-Systems auf die Grundrechte müssen^h bestimmte Betreiber solcher Systeme die Kategorien von Personen und Gruppen, zu denen auch Kinder gehören können, berücksichtigen, die wahrscheinlich von der Nutzung des Systems betroffen sind. Die Europäische Kommission hat einen Entwurf von Leitlinien für die Einstufung von Hochrisiko-KI-Systemen zur öffentlichen Konsultation veröffentlicht; diese enthalten die Beispiele für Praktiken, die in den Anwendungsbereich der KI-Verordnung²⁵¹ fallen bzw. nicht in den Anwendungsbereich fallen.

Aufgrund der Weiterentwicklung von KI-Systemen haben sich darüber hinaus die gesetzgebenden Organe zur weiteren Stärkung der Vorschriften, die auch zu einem besseren Schutz von Minderjährigen beitragen, rasch auf den Digitalen Omnibus zu KI geeinigt. Insbesondere sind KI-Systeme, die nicht einvernehmliche, eindeutig sexuelle und intime Inhalte oder Darstellungen sexuellen Kindesmissbrauchs erzeugen, wie KI-„Auszieh-Apps“, verboten. Die in der Omnibus-Verordnung zur KI vereinbarten Verpflichtungen für Hochrisiko-KI-Systeme gelten ab Dezember 2027 (für eigenständige KI-Systeme wie bestimmte KI-Systeme in der Bildung) und August 2028 (für KI-Systeme, die in regulierte Produkte wie Spielzeug eingebettet sind).

Verbotene Praktiken

In der KI-Verordnung sind KI-Praktiken verboten, die Kinder manipulieren, täuschen oder ihre Schutzbedürftigkeit ausnutzen. Mit diesen Verboten soll verhindert werden, dass KI-Systeme Minderjährige manipulieren oder kognitive und andere Einschränkungen ausnutzen, die bei Kindern bestehen können, wenn sie Entscheidungen treffen, die sie andernfalls nicht getroffen hätten; zudem sollen sie vor schädlicher unzulässiger Beeinflussung, Manipulation und Ausbeutung geschützt werden.

h. Die in der Omnibus-Verordnung zur KI vereinbarten Verpflichtungen für Hochrisiko-KI-Systeme gelten ab Dezember 2027 (für eigenständige KI-Systeme wie bestimmte KI-Systeme in der Bildung) und August 2028 (für KI-Systeme, die in regulierte Produkte eingebettet sind, beispielsweise Spielzeug).

Diese Verbote traten am 2. Februar 2025 in Kraft. Die Kommission hat Leitlinien zu verbotenen KI-Praktiken veröffentlicht, die Beispiele für Praktiken enthalten, die in den Anwendungsbereich der KI-Verordnung²⁵² fallen bzw. nicht in deren Anwendungsbereich fallen.

Ein Beispiel für eine verbotene KI-Praxis ist eine KI-gestützte Anwendung, die Minderjährige dazu ermutigt, im Gegenzug für digitale Belohnungen und virtuelles Lob immer riskantere Herausforderungen wie das Erklettern von Möbeln, die Erkundung hoher Regale oder die Handhabung scharfer Gegenstände zu bewältigen. Solche Systeme nutzen die Schutzbedürftigkeit von Kindern aus, indem sie ihre natürliche Neugier und ihren Wunsch nach Belohnung missbrauchen, und laufen Gefahr, ihnen erheblichen Schaden zuzufügen.

Ein weiteres Beispiel für eine verbotene KI-Praxis sind Spiele, die so konzipiert sind, dass sie hochgradig suchterzeugend sind, indem sie die Schutzbedürftigkeit von Kindern und Jugendlichen ausnutzen (einschließlich fehlender Selbstkontrolle). Bei solchen Spielen wird KI zur Analyse des individuellen Verhaltens und der individuellen Vorlieben von Kindern eingesetzt, auf deren Grundlage sie dann durch Pläne für suchterzeugende Verstärkung und Dopamin-Loops personalisierte, nicht vorhersagbare Belohnungen erzeugt. Dies fördert übermäßiges Spielen und zwanghaftes Nutzen.

Diese Spiele sind so konzipiert, dass sie hochgradig suchterzeugend sind (oder eine entsprechende Wirkung haben), wobei die Schutzbedürftigkeit von Kindern ausgenutzt wird. Hierzu zählen ihre begrenzte Fähigkeit zum Erkennen langfristiger Folgen, ihre Empfindlichkeit gegenüber Druck, ihr Mangel an Selbstkontrolle und ihre Neigung zu sofortiger Belohnung.

KI-Modelle mit allgemeinem Verwendungszweck

Für die leistungsfähigsten KI-Modelle mit allgemeinem Verwendungszweck (general-purpose AI, GPAI) mit systemischem Risiko sind in der KI-Verordnung spezifische Risikobewertungs- und Risikominderungspflichten vorgeschrieben. Die meisten führenden Anbieter von GPAI-Modellen unterzeichneten den GPAI-Verhaltenskodex²⁵³, um diese Vorschriften einhalten zu können.

GPAI-Anbieter müssen konkrete Risikoszenarien bewerten und abmildern. Dies kann die Verbreitung rechtswidriger, falscher oder diskriminierender Inhalte, die mit rechtswidrigen, gewalttätigen, hasserfüllten, radikalisierten oder falschen Inhalten verbunden sind, umfassen, wobei die Ergebnisse dieses Risikomanagementprozesses vor der Markteinführung solcher Modelle der Europäischen Kommission zu melden sind.

Zu den Risikominderungsmaßnahmen, die Anbieter von GPAI-Modellen treffen müssen, gehören die Überwachung und Filterung des Inputs und/oder der Outputs des Modells. Dies schließt auch ein, dass die Erzeugung schädlicher Inhalte verhindert wird. Die Verpflichtungen in Bezug auf KI-Modelle mit allgemeinem Verwendungszweck traten am 2. August 2025 in Kraft.

Transparenzpflichten

In der KI-Verordnung sind für Anbieter und Betreiber bestimmter KI-Systeme²⁵⁴ Transparenzpflichten vorgeschrieben, um Betrug, Identitätsbetrug und Täuschung zu verhindern. Nach der KI-Verordnung müssen Anbieter sicherstellen, dass KI-Systeme, die für die direkte Interaktion mit Menschen vorgesehen sind (z. B. Chatbots), so konzipiert und entwickelt werden, dass die betroffenen Menschen darüber informiert werden, dass sie mit einem KI-System interagieren, sofern dies nicht offensichtlich ist. Diese Verpflichtung gilt in jedem Fall für Chatbots, die mit Kindern interagieren.

Die Offenlegung trägt den Risiken emotionaler Abhängigkeit nicht in vollem Umfang Rechnung. Aufgrund des interaktiven und häufig ansprechenden Charakters dieser Systeme ist es jedoch von entscheidender Bedeutung, dass die Nutzer ausdrücklich darauf hingewiesen werden, dass sie mit einem KI-System zu tun haben, das so programmiert ist, dass es ihre Interaktion mit dem System verstärkt, und nicht mit einer Person.

Generative KI-Systeme

Anbieter und Betreiber generativer KI-Systeme sind verpflichtet, Inhalte wie Bilder, Audio- oder Videoinhalte zu kennzeichnen und erkennbar zu machen, wenn sie künstlich erzeugt oder manipuliert wurden; außerdem sind Deepfakes und bestimmte KI-generierte Veröffentlichungen zu öffentlichen Angelegenheiten zu kennzeichnen.

Betreiber eines Emotionserkennungssystems oder eines Systems zur biometrischen Kategorisierung müssen Personen, die dem Betrieb des Systems ausgesetzt sind, davon in Kenntnis setzen. Die Europäische Kommission erleichtert die Einhaltung dieser Verpflichtungen unter anderem durch die Veröffentlichung eines Praxisleitfadens für die Markierung und Kennzeichnung von KI-generierten Inhalten²⁵⁵ sowie durch Leitlinien, die nach ihrer Veröffentlichung zur öffentlichen Konsultation aktuell ausgearbeitet werden²⁵⁶. Die Verpflichtungen in Bezug auf die Transparenzanforderungen gelten seit dem 2. August 2026.

KI-Begleiter

KI-Begleiter gewinnen bei Kindern zunehmend an Beliebtheit, und im Zusammenhang mit ihrer Nutzung sind bestimmte Risiken festgestellt worden. Nach der Verordnung hängt die Einstufung von KI-Begleitern und ähnlichen Chatbots in erster Linie von ihrem vorgesehenen Zweck, ihrer Funktionalität und dem Kontext ihrer Verwendung ab.

Je nachdem, welche dieser Faktoren zutreffen, kann ein KI-Begleiter eine verbotene Praxis darstellen (z. B. in Fällen, in denen die Schutzbedürftigkeit von Kindern auf in erheblichem Maße schädliche Weise ausgenutzt wird). Sie können auch als Hochrisiko-KI-System gelten (z. B. wenn sie Emotionserkennungsfunktionen enthalten oder wenn auf sie bestimmte Anwendungsfälle in Bildungskontexten zutreffen). Schließlich können sie Transparenzpflichten unterliegen, wonach die Nutzer darüber informiert werden müssen, dass sie nicht mit einer Person interagieren.

VERBRAUCHERSCHUTZINSTRUMENTE

Bei der Auseinandersetzung mit den Schäden, denen Kinder im digitalen Umfeld ausgesetzt sind, ist es wichtig, die Ansätze der strafrechtlichen sowie der zivilrechtlichen Haftung und der Produkthaftung zu beachten.

Die strafrechtliche Haftung könnte sich auf das Verbot und die Bestrafung bestimmter schädlicher Verhaltensweisen wie die Verbreitung von Material über sexuellen Kindesmissbrauch oder Online-Grooming beziehen und stützt sich auf die staatliche Strafverfolgung und strafrechtliche Sanktionen. Die Verfolgung von Straftaten ist zwar für die schwersten Straftaten unerlässlich, erfolgt aber in erster Linie reaktiv. Dies geschieht in der Regel erst, nachdem bereits Schaden entstanden ist, und zielt auf einzelne Täter ab, anstatt die systemischen Rahmenbedingungen anzugehen, die diesen Schaden erst ermöglichen. Die Kriminalisierung bestimmter Verhaltensweisen beinhaltet jedoch auch wichtige präventive und antizipatorische Elemente.

Ein zivil- und produkthaftungsrechtlicher Ansatz könnte hingegen Präventiv- und Ausgleichsmaßnahmen zwischen verschiedenen privaten Parteien vorsehen. Dieser Ansatz befasst sich mit der Aufteilung der Rechte, Pflichten und Verantwortlichkeiten zwischen privaten Parteien, einschließlich der Unternehmen, die soziale Medien und andere digitale Dienste konzipieren und betreiben; im Rahmen dieses Ansatzes werden auch Rechtsbehelfe bei Verstößen gegen diese Pflichten bereitgestellt.

Das Verbraucherschutzrecht spielt in Zivil- und Produkthaftungsfällen eine entscheidende Rolle. Ein wichtiger Gesichtspunkt ist dabei, dass diese Perspektive sowohl Regulierungsbehörden als auch privaten Prozessparteien ermöglicht, die Gestaltungsentscheidungen von Online-Diensteanbietern anzufechten. Diese Produkthaftungsperspektive bildete den Hauptantriebsfaktor bei den folgenreichsten rechtlichen Entwicklungen der jüngsten Zeit in den Vereinigten Staaten.

„Plattformen sollten mit dem Kind wachsen. ... Jedes Empfehlungssystem, das einem Minderjährigen dient, muss im Interesse des Wohlbefindens des Kindes und nicht im Interesse des Engagements optimiert werden.“

— GABRIELE BATTIMELLI,
BIK+-BOTSCHAFTERIN AUS ITALIEN

In den Vereinigten Staaten beruht einer der jüngsten Fälle zu suchterzeugenden Gestaltungsmerkmalen auf Plattformen auf dem Verbraucherrecht. Eine Geschworenen-Jury in New Mexico entschied im März 2026, dass Meta als Betreiber seiner Online-Plattformen vorsätzlich gegen Verbraucherschutzgesetze verstoßen hat, und forderte das Unternehmen zur Zahlung von 375 Mio. USD auf.

Das Verfahren wurde vom Generalstaatsanwalt auf der Grundlage von Rechtsvorschriften über unlautere Praktiken angestrengt, die sich gegen die Gestaltung von Plattformen und Sicherheitspraktiken richten und die auch Empfehlungssysteme einschließen, bei denen Minderjährige Sexualstraftätern ausgesetzt waren. Die Jury stellte fest, dass das Unternehmen die Verbraucher hinsichtlich der Sicherheit seiner Dienstleistungen irreführt hatte, während interne Dokumente zeigten, dass sich das Unternehmen des Schadens bewusst war.

Parallel dazu führte das erste Vorreiter-Verfahren zur „Sucht in den sozialen Medien“ in Los Angeles, in dem es unter anderem um Klagen in Bezug auf

fahrlässige Gestaltung und fehlende Warnungen ging, zu einem Urteil der Jury gegen Meta und YouTube. Die Rechtssache stützt sich auf das private Deliktsrecht. Das Gericht stellte ausdrücklich fest, dass Merkmale wie endloses Scrollen, algorithmische Feeds, Mechanismen zur automatischen Wiedergabe und Interaktionsmaximierung zu dem Schaden beitrugen, den ein Minderjähriger erlitt. In dem Urteil wird anerkannt, dass suchterzeugende Gestaltungsmerkmale anfechtbare Produktmängel darstellen können, insbesondere wenn sich die Unternehmen der Risiken bewusst sind und diese nicht mindern.

In der EU gilt das EU-Verbraucherschutzrecht für Kinder als Gruppe von schutzbedürftigen Verbrauchern durch verschiedene Rechtsinstrumente. Diese Vorschriften fungieren als horizontales „Sicherheitsnetz“, das für alle Händler, Waren oder Dienstleistungen gilt, die sich u. a. im digitalen Umfeld an Verbraucher richten, unabhängig vom Geschäftsmodell oder der verwendeten Technologie.

In den bestehenden EU-Verbraucherschutzvorschriften, insbesondere in der Richtlinie über unlautere Geschäftspraktiken (UGP-Richtlinie), werden Kinder als schutzbedürftige Verbraucher anerkannt, die einen verstärkten Schutz benötigen. Nach der UGP-Richtlinie sind irreführende und aggressive Geschäftspraktiken, die die Leichtgläubigkeit oder mangelnde Erfahrung von Kindern ausnutzen, verboten.

Ferner ist auch verboten, Minderjährige zum Kauf beworbener Produkte zu ermuntern oder Eltern dazu zu drängen, diese Produkte für sie zu kaufen. Wie in den Leitlinien der UGP-Richtlinie²⁵⁷ erläutert, können Dark Patterns, Ausgaben- oder Aufmerksamkeitsmaximierungsmerkmale (z. B. unklare In-App-Währungen) oder unlauteres Influencer-Marketing ebenfalls unlautere Geschäftspraktiken darstellen. Dennoch ergab die Eignungsprüfung zur digitalen Fairness²⁵⁸, dass Verbraucher im Allgemeinen und Kinder und Jugendliche im Besonderen im Internet besser geschützt werden müssen.

In der Richtlinie über die Rechte der Verbraucher sind vorvertragliche Verpflichtungen, beispielsweise Transparenz in Bezug auf die Preisgestaltung, die Identität des Unternehmers oder das Widerrufsrecht, vorgeschrieben. Sie richtet sich zwar nicht speziell an Kinder, sondern gilt für alle digitalen Transaktionen (z. B. den Kauf virtueller Währungen direkt innerhalb eines Spiels), einschließlich solcher, an denen Minderjährige beteiligt sind.

Darüber hinaus werden vertragliche Klauseln, die nicht individuell ausgehandelt wurden, nach der Richtlinie über missbräuchliche Vertragsklauseln als missbräuchlich eingestuft und werden unverbindlich, wenn durch sie ein erhebliches Missverhältnis zum Nachteil des Verbrauchers entsteht. Dies gilt auch, wenn der Verbraucher minderjährig ist.

Schließlich ist in der Verordnung über die allgemeine Produktsicherheit vorgeschrieben, dass alle in ihren Anwendungsbereich fallenden Verbraucherprodukte, einschließlich vernetzter Produkte, sicher sein müssen. Der Anwendungsbereich dieser Verordnung ist weit gefasst, sodass sie als Sicherheitsnetz für alle in der EU in Verkehr gebrachten oder auf dem EU-Markt bereitgestellten Produkte dienen kann.

Bei der Bewertung der Sicherheit von Produkten müssen die Hersteller die Kategorien von Verbrauchern berücksichtigen, die das Produkt verwenden; zu diesem Zweck müssen sie das Risiko für schutzbedürftige Verbraucher wie Kinder prüfen. Außerdem müssen sie entsprechende Maßnahmen zur Risikominderung treffen. Der Schwerpunkt der Verordnung liegt auf dem Schutz sowohl der körperlichen als auch der geistigen Gesundheit der Verbraucher, was beispielsweise für Apps oder Chatbots relevant sein kann, die bei Minderjährigen beliebt sind.

PRODUKTHAFTUNGSRICHTLINIE

Die Produkthaftungsrichtlinie ist ein harmonisierter Rahmen für die zivilrechtliche Haftung, mit dem sichergestellt wird, dass Opfer fehlerhafter Produkte im Schadensfall Schadensersatz vom Hersteller verlangen können. Die neue Produkthaftungsrichtlinie trat am 8. Dezember 2024 in Kraft und muss bis zum 9. Dezember 2026 von den Mitgliedstaaten umgesetzt werden.

Die überarbeitete Produkthaftungsrichtlinie lässt die wesentlichen Elemente der ursprünglichen Produkthaftungsrichtlinie unberührt. Die Erbringung des Nachweises, dass ein Produkt fehlerhaft ist und dass ein ursächlicher Zusammenhang zwischen der Fehlerhaftigkeit und dem konkret erlittenen Schaden besteht, obliegt dem Opfer. In der überarbeiteten Produkthaftungsrichtlinie wird der Anwendungsbereich in der Weise präzisiert, dass auch Software einschließlich Anwendungen, Betriebssystemen und KI-Systemen abgedeckt wird; ferner werden Haftungsregeln für den Fall festgelegt, dass Produkte wesentlich verändert werden und dadurch ein „zweites Leben“ erhalten.

Ferner wird klargestellt, dass entschädigungsfähige Schäden im Rahmen der Produkthaftungsrichtlinie auch medizinisch anerkannte psychische Schäden umfassen können. Mit der Produkthaftungsrichtlinie werden außerdem die Haftungsvorschriften an zunehmend komplexe globale Wertschöpfungsketten angepasst, indem sichergestellt wird, dass mindestens ein in der EU niedergelassener haftbarer Wirtschaftsakteur (möglicherweise einschließlich Plattformen) ermittelt werden kann.

Die neue Produkthaftungsrichtlinie bietet in Fällen, in denen fehlerhafte digitale Produkte Kindern Schaden zufügen, einen Weg zur Entschädigung. So kann beispielsweise ein Kind, das aufgrund der suchterzeugenden Gestaltung einer Anwendung Depressionen entwickelt oder sich nach gefährlichen Reaktionen eines Chatbots selbst verletzt, nun Anspruch auf Entschädigung im Rahmen der Produkthaftungsrichtlinie haben.

RICHTLINIE ÜBER AUDIOVISUELLE MEDIENDIENSTE

(AVMD-RICHTLINIE)

Die AVMD-Richtlinie ist das Kernstück des EU-Medienrechts zur Regulierung audiovisueller Inhalte. Sie enthält sektorspezifische Verpflichtungen für audiovisuelle Mediendienste und Video-Sharing-Plattformen zum Schutz Minderjähriger vor schädlichen audiovisuellen Inhalten.

Gemäß der AVMD-Richtlinie müssen Video-Sharing-Plattformen unabhängig von ihrer Größe die EU-Standards für Medieninhalte in ihre allgemeinen Geschäftsbedingungen aufnehmen. Hierzu zählen auch Standards, die Minderjährige vor Inhalten schützen sollen, die ihre körperliche, geistige oder sittliche Entwicklung beeinträchtigen können. Video-Sharing-Plattformen sind ferner verpflichtet, geeignete Maßnahmen zu ergreifen (z. B. Mechanismen zur Meldung oder Kennzeichnung schädlicher Inhalte, Altersüberprüfung, elterliche Kontrolle und Systeme zur Bewertung von Inhalten), um zu verhindern, dass Minderjährige schädliche audiovisuelle Inhalte sehen. Die schädlichsten Arten von Inhalten, wie Pornografie oder grundlose Gewalt, müssen den strengsten Maßnahmen, mit denen verhindert wird, dass Minderjährige schädliche Inhalte sehen, unterliegen.

Bei der laufenden Bewertung und der bevorstehenden, für das dritte Quartal 2026 geplanten Überprüfung der AVMD-Richtlinie wird ein wichtiger Schwerpunkt auf dem Schutz von Minderjährigen als schutzbedürftige Zuschauer online liegen. Die Überprüfung wird der Bewertung der Relevanz der geltenden Vorschriften und der Ermittlung möglicher Mängel in den bestehenden Rechtsvorschriften gelten. Dies schließt auch die Bewertung ein, ob mehr für die Sicherstellung dessen getan werden sollte, dass Zuschauer, insbesondere Minderjährige, angemessen geschützt werden, wenn sie audiovisuelle Inhalte online anschauen. Hierzu zählen auch Inhalte, die von Influencern zur Verfügung gestellt werden, wobei Marktentwicklungen und regulatorische Entwicklungen zu berücksichtigen sind. Diese Entwicklungen und die sich verändernden Zuschauergewohnheiten bringen Herausforderungen mit sich, die die Zuschauer, insbesondere Minderjährige, gefährden können.

Im Online-Umfeld sind neue Bedrohungen und Risiken entstanden, die dazu geführt haben, dass Minderjährige zunehmend schädlichen audiovisuellen Inhalten wie Cybermobbing, Essstörungen und der Ermutigung zu Selbstmord oder Selbstverletzung ausgesetzt sind. Eine Fragestellung im Rahmen der Überprüfung wird sein, ob eine weitere Spezifizierung des Begriffs „schädliche audiovisuelle Inhalte“ erforderlich ist und welche Maßnahmen benötigt werden, damit sichergestellt werden kann, dass Minderjährige solche Inhalte nicht ansehen.

VERORDNUNG ÜBER POLITISCHE WERBUNG

In der Verordnung über politische Werbung sind Transparenz- und Sorgfaltspflichten für die Erbringung politischer Werbedienstleistungen festgelegt. Mit der Verordnung werden spezifische Anforderungen für den Einsatz von auf der Verarbeitung personenbezogener Daten beruhenden Targeting- und Anzeigenschaltungsverfahren in politischer Online-Werbung eingeführt. Die Verordnung fördert den Schutz Minderjähriger und ermöglicht gleichzeitig gleiche Bedingungen für Erstwähler.

Einerseits ist nach der Verordnung über politische Werbung die Verwendung von Profiling, bei dem personenbezogene Daten Minderjähriger verarbeitet werden, von denen bekannt ist, dass sie mindestens ein Jahr jünger als das nationale Wahlalter sind, verboten. Andererseits ermöglicht die Verordnung transparente politische Werbung, um Erstwähler zu erreichen, sodass sie ihre demokratischen Entscheidungen in voller Kenntnis der Sachlage treffen können.

SCHUTZ VOR SEXUELLEM MISSBRAUCH UND

SEXUELLER AUSBEUTUNG VON KINDERN IM INTERNET

Sexueller Missbrauch und sexuelle Ausbeutung von Kindern im Internet gehören zu den gefährlichsten Risiken, denen Kinder und Jugendliche in der digitalen Welt ausgesetzt sein können. Täter sind Erwachsene, aber auch andere Minderjährige. Kinder und Jugendliche müssen über Risiken, einschließlich Sexting und Sextortion, und über mögliche rechtliche Folgen für die Täter informiert werden.

Für Opfer, die von Angehörigen und Betreuungspersonen ausgebeutet werden, sind häufig Maßnahmen zum Schutz von Kindern auf der Grundlage des Zivilrechts in Verbindung mit sozialer Betreuung und sicherer Unterbringung erforderlich. Viele Opfer benötigen möglicherweise eine Psychotherapie.

Maßnahmen zum Schutz von Kindern vor sexuellem Missbrauch und sexueller Ausbeutung im Internet sind Teil der strafrechtlichen Dimension des Kinderschutzes, die an der Schnittstelle zwischen den Zuständigkeiten der EU und der Mitgliedstaaten liegt.

Durch die Festlegung bestimmter Inhalte, die entweder für sich genommen eine rechtswidrige Tätigkeit sind oder im Zusammenhang damit stehen, führen diese Instrumente auch zu den einschlägigen Bestimmungen über die Sorgfaltspflicht im Rahmen des Gesetzes über digitale Dienste. Sie befassen sich mit der Frage, wie gegen rechtswidrige Inhalte vorgegangen werden kann, und bieten einen wirksamen Rahmen zur Bekämpfung der Verbreitung solcher Inhalte.

Die Europäische Kommission hat Maßnahmen getroffen, um sexuellen Missbrauch von Kindern im Internet zu verhindern und zu bekämpfen. Im Jahr 2022 legte sie einen Vorschlag für einen dauerhaften, umfassenden EU-Rechtsrahmen zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern vor. Für Anbieter von Online-Diensten umfasst dies Verpflichtungen, die Verbreitung von Material über sexuellen Kindesmissbrauch und das Grooming von Kindern über ihre Dienste zu verhindern. Nur wenn die Präventionsmaßnahmen nicht ausreichen, könnten Online-Diesteanbieter verpflichtet werden, sexuellen Kindesmissbrauch im Internet aufzudecken, zu melden, zu entfernen oder zu sperren.

Nach dem Vorschlag wären die zuständigen nationalen Behörden befugt, den Erlass von Anordnungen zur Aufdeckung, Entfernung oder Sperrung durch Justiz- oder unabhängige Verwaltungsbehörden zu beantragen. Die Anordnungen würden erst nach einer gründlichen Prüfung ihrer Erforderlichkeit und Verhältnismäßigkeit erlassen.

In dem Vorschlag ist auch die Einrichtung eines neuen EU-Zentrums zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern vorgesehen, das Anbieter digitaler Dienste und Behörden bei der Erfüllung ihrer Verpflichtungen aus der Verordnung unterstützen soll. Die Verhandlungen über die Verordnung sind noch nicht abgeschlossen. Die Europäische Kommission unterstützt das Europäische Parlament und den Rat bei der Erzielung einer Einigung, die den wirksamen Schutz von Kindern unter uneingeschränkter Achtung aller betroffenen Grundrechte sowie die Kohärenz mit den bestehenden Rechtsvorschriften, insbesondere dem Gesetz über digitale Dienste, gewährleistet.

Parallel dazu hat die jüngste Einigung der beiden gesetzgebenden Organe über die Neufassung der Richtlinie zur Bekämpfung des sexuellen Missbrauchs von Kindern den EU-Rahmen gegen sexuellen Missbrauch und sexuelle Ausbeutung von Kindern, sowohl online als auch offline, weiter gestärkt. Mit den überarbeiteten Vorschriften wird der bestehende Rahmen aktualisiert, um sicherzustellen, dass neue Bedrohungen wie KI-generiertes Material über sexuellen Kindesmissbrauch, Grooming und Sextortion sowie Live-Streaming von sexuellem Kindesmissbrauch unter Strafe gestellt und wirksam strafrechtlich verfolgt werden.

Mit den überarbeiteten Vorschriften wird auch der Rechtsrahmen zur Prävention des sexuellen Missbrauchs von Kindern und zur Unterstützung der Opfer gestärkt. Dies wird erreicht, indem für Personen, die in engem und unmittelbarem Kontakt mit Kindern arbeiten, Zuverlässigkeitsüberprüfungen vorgeschrieben werden oder indem sichergestellt wird, dass Opfer über einen ausreichenden Zeitraum nach der Begehung der Straftat Strafverfolgungsmaßnahmen erwirken können.

Neben Gesetzgebungsinitiativen trifft die EU auch nichtlegislative Maßnahmen wie die Finanzierung und die Förderung von Koordination und Zusammenarbeit. So kommen beispielsweise im Netz zur Prävention des sexuellen Missbrauchs von Kindern fünfzig Expertinnen und Experten zusammen, um bewährte Verfahren auszutauschen, Informationen für die Forschung bereitzustellen und die Entwicklung und Umsetzung gründlich überprüfter Maßnahmen zur Prävention sexuellen Missbrauchs von Kindern, auch online, zu unterstützen.

Das Strafrecht ist notwendig, um den sexuellen Missbrauch von Kindern zu bekämpfen, kann jedoch nicht das einzige Instrument zur wirksamen Bekämpfung dieses schrecklichen Verbrechens sein. Der Schutz von Kindern vor sexuellem Missbrauch und sexueller Ausbeutung erfordert einen gesamtgesellschaftlichen Ansatz. Er sollte Behörden, Strafverfolgungsbehörden, Justizbehörden, Bildungseinrichtungen, Organisationen der Zivilgesellschaft, Familien, Gemeinschaften, soziale Medien und andere Anbieter digitaler Dienste einbeziehen. Eine wirksame Prävention und Reaktion auf diese Straftaten hängt nicht allein von soliden gesetzgeberischen Maßnahmen ab, sondern auch von koordinierten Anstrengungen und sektorübergreifenden, vielschichtigen Maßnahmen.

PRÄVENTION VON RADIKALISIERUNG

Die EU-Verordnung zur Bekämpfung der Verbreitung terroristischer Online-Inhalte schützt gefährdete Bevölkerungsgruppen, einschließlich Kindern, vor radikalisiertem Online-Material. Nach der Verordnung sind Hostingdiensteanbieter verpflichtet, terroristische Inhalte innerhalb einer Stunde nach Eingang einer Entfernungsanordnung einer zuständigen nationalen Behörde zu entfernen.

Ergänzt wird dies durch mehrere nichtlegislative Initiativen. Das EU-Internetforum ist eine solche Maßnahme. Das Forum ist eine öffentlich-private Plattform, auf der sich die EU-Mitgliedstaaten, die Strafverfolgungsbehörden, die Industrie und die Zivilgesellschaft zur Koordinierung von Maßnahmen gegen Missbrauch zusammenfinden. Solcher Missbrauch beinhaltet auch die Ausbeutung von Online-Plattformen durch Terroristen, gewaltbereite Extremisten und andere böswillige Akteure wie Akteure, die zum Zweck

des sexuellen Missbrauchs, des Drogenhandels, der organisierten Kriminalität, des Menschenhandels oder der Schleusung von Migranten Kontakt zu Kindern aufnehmen (Grooming).

Für Kinder in der gesamten EU besteht – sowohl online als auch offline – die Gefahr, Opfer von Kriminalität zu werden oder für Straftaten angeworben zu werden. Die Europäische Kommission arbeitet derzeit an einem Aktionsplan zum Schutz von Kindern vor Kriminalität. Durch die Ermittlung verbleibender Lücken soll der Aktionsplan die bestehenden Instrumente ergänzen und einen kohärenteren, besser koordinierten Ansatz bieten, damit der Schutz von Kindern vor Kriminalität – sowohl als Opfer als auch als Täter und sowohl online als auch offline – verbessert werden kann.

AKTIONSPLAN GEGEN CYBERMOBBING

Cybermobbing ist für Kinder und Jugendliche im Internet ein wachsendes Problem, das erhebliche Auswirkungen auf die psychische Gesundheit und das Wohlbefinden, die Teilhabe und die Entwicklung von Kindern hat.

Um der besorgniserregenden Verbreitung von Cybermobbing entgegenzuwirken, erließ die Europäische Kommission im März 2026 den Aktionsplan gegen Cybermobbing²⁵⁹. Der Aktionsplan zielt darauf ab, Cybermobbing zu verhindern, seine Meldung zu erleichtern und eine wirksame Unterstützung der Opfer zu gewährleisten. Im Rahmen des Aktionsplans werden die EU-Mitgliedstaaten aufgefordert, auf nationaler Ebene ergänzende Maßnahmen zu ergreifen.

Empfohlen werden beispielsweise die Entwicklung nationaler Strategien gegen Mobbing sowie die Stärkung von Prävention und Früherkennung in Schulen und anderen Einrichtungen, in denen Kinder Zeit verbringen. Weitere wichtige Bereiche, in denen im Rahmen des Aktionsplans Maßnahmen getroffen werden können, sind die Verbesserung der Angebote zur Unterstützung von Opfern und die Sicherstellung, dass die Meldesysteme mit einer angemessenen rechtlichen, sozialen, psychologischen und pädagogischen Unterstützung in Verbindung stehen.

Parallel dazu werden die EU-Mitgliedstaaten in der Empfehlung der Kommission zur Entwicklung und Stärkung integrierter Kinderschutzsysteme im Interesse des Kindeswohls²⁶⁰ aufgefordert, alle geeigneten gesetzgeberischen, administrativen, sozialen und pädagogischen Maßnahmen zu ergreifen, um Mobbing, auch online, zu verhindern und Kinder davor zu schützen. Dies schließt auch die Entwicklung umfassender Pläne gegen Mobbing ein.

EU-LÖSUNG FÜR DIE ALTERSVERIFIKATION

Neben den bestehenden Rechtsvorschriften hat die Europäische Kommission ein operatives Instrumentarium für die Altersverifikation entwickelt und erweitert, um Kinder und Jugendliche im Internet zu schützen und ihre Konfrontation mit schädlichen Online-Inhalten zu begrenzen. Dieses Instrumentarium bietet Netze, Plattformen, technische Lösungen und Kanäle, mit denen Minderjährige online geschützt und gestärkt werden.

Die Kommission hat eine EU-Lösung für die Altersverifikation entwickelt, die robust und benutzerfreundlich ist und die Privatsphäre wahrt. Zu diesem Zweck wurde den Mitgliedstaaten ein Konzept für die individuelle Anpassung und Umsetzung zur Verfügung gestellt. Bei einer individuellen Anpassung können unterschiedliche Altersgruppen berücksichtigt werden. Die Mitgliedstaaten können die Lösung als eigenständige App veröffentlichen und/oder als Altersverifikationsfunktion in ihre europäische Brieftasche für die Digitale Identität integrieren. Die Lösung ist quelloffen, sodass auch Drittländer oder Marktteilnehmer die Lösung übernehmen und weiterentwickeln können.

Die EU-Lösung für die Altersverifikation könnte ein geeignetes Instrument für die Anwendung von Altersbeschränkungen in der Praxis sein, wenn sie mit geeigneten Optionen für Minderjährige für den Nachweis ihres Alters einhergeht. Die EU-Mitgliedstaaten verfolgen unterschiedliche Ansätze bei der Verwendung und Ausgabe von Ausweisdokumenten oder eID und nicht jeder Minderjährige hat vielleicht einen eigenen Reisepass. Daher ist für das effektive Funktionieren der Altersverifikation in der EU die Ernennung vertrauenswürdiger Anbieter von Altersnachweisen, die einen solchen Nachweis für das erforderliche Alter ausstellen können, von entscheidender Bedeutung.

Zur Beschleunigung dieses Prozesses gab die Europäische Kommission eine Empfehlung zur Schaffung eines gemeinsamen Rahmens für EU-weite Altersverifikationstechnik heraus. Im Rahmen der Empfehlung arbeitet die Kommission gemeinsam mit den EU-Mitgliedstaaten an der Ausarbeitung eines EU-Systems zur Altersverifikation. Im Rahmen des Systems werden die Anforderungen an das Vertrauensmodell, die Governance und die von den Anbietern der Altersnachweisbescheinigungen und Altersverifikationslösungen zu erfüllenden Anforderungen im Einzelnen festgelegt.

In der Empfehlung werden die EU-Mitgliedstaaten aufgefordert, das EU-Konzept zur Altersverifikation zu nutzen, es an ihre nationalen Gegebenheiten anzupassen und bis zum 31. Dezember 2026 Lösungen für die Altersüberprüfung auf der Grundlage des Konzepts zur Verfügung zu stellen.

Die Mitgliedstaaten wurden ferner aufgefordert, der Kommission bis zum 30. Juni 2026 einen Umsetzungsplan vorzulegen, in dem sie darlegen, wie sie beabsichtigen, eine EU-Lösung für die Altersverifikation zur Verfügung zu stellen. Die Mitgliedstaaten werden aufgefordert, bei der Einführung ihrer nationalen Lösungen zusammenzuarbeiten und mit der Europäischen Kommission, Forschenden und der Zivilgesellschaft in Kontakt zu treten. Die Herausforderungen für die Altersüberprüfung, zu denen auch mögliche Risiken einer regulatorischen Fragmentierung in der EU zählen, werden später in diesem Kapitel im Abschnitt „Unerledigte Angelegenheiten“ geprüft.

Ergebnisse der bestehenden Durchsetzungsmaßnahmen

Die bestehenden EU-Rechtsvorschriften sind nur so wirksam wie ihre Durchsetzung. Mit dem Gesetz über digitale Dienste wurde eine grundlegend neue Durchsetzungsstruktur eingeführt, die in Bezug auf die größten Plattformen bei der Kommission zentralisiert ist und mittels Koordinatoren für digitale Dienste mit der nationalen Durchsetzungsarchitektur kombiniert wird. Diese Struktur führt nun zu Entscheidungen, Verfahren und sichtbaren Änderungen bei der Einhaltung der Vorschriften und es zeichnet sich bereits eine Erfolgsbilanz ab.

In der KI-Verordnung wird eine ähnlich angepasste Durchsetzungsstruktur gewählt, bei der für KI-Modelle mit allgemeinem Verwendungszweck und die meisten auf KI-Modellen mit allgemeinem Verwendungszweck basierenden KI-Systemen die Durchsetzung bei der Kommission zentralisiert ist, wenn der Anbieter des KI-Systems mit dem des Modells identisch ist (oder innerhalb desselben Unternehmens angesiedelt ist). Mit der Omnibus-Verordnung über künstliche Intelligenz wird eine weitere Innovation eingeführt, wobei die Durchsetzung im Zusammenhang mit KI-Systemen, die im Rahmen des Gesetzes über digitale Dienste als sehr große Online-Plattformen oder sehr große Online-Suchmaschinen benannt oder in diese integriert wurden, ebenfalls bei der Kommission zentral zusammenläuft.

Die DSGVO wird von unabhängigen nationalen Datenschutzbehörden durchgesetzt. Sie erlassen weiterhin Entscheidungen und verhängen erhebliche Geldbußen und andere Abhilfemaßnahmen, wenn die Datenschutzbehörden feststellen, dass die Verantwortlichen gegen Datenschutzvorschriften verstoßen haben.

Die Durchsetzung der AVMD-Richtlinie wird von den nationalen Regulierungsbehörden und -stellen sichergestellt. Mit der AVMD-Richtlinie wurden Anforderungen zur Gewährleistung der institutionellen und funktionellen Unabhängigkeit der nationalen Regulierungsbehörden und -stellen eingeführt, die durch das Europäische Medienfreiheitsgesetz gestärkt wurden.

Die Durchsetzung der Verbraucherschutzgesetze, einschließlich der Vorschriften, die sich aus Richtlinien und Verordnungen der EU ergeben, fällt in erster Linie in die Zuständigkeit der Behörden und Gerichte der Mitgliedstaaten. Die Kommission verfügt derzeit zwar nicht über direkte Durchsetzungsbefugnisse im Bereich des Verbraucherrechts, koordiniert und unterstützt jedoch die Durchsetzungsmaßnahmen der Mitgliedstaaten im Rahmen der Verordnung über die Zusammenarbeit im Verbraucherschutz. Damit wird ein Rahmen für die grenzüberschreitende Zusammenarbeit bei der Durchsetzung geschaffen, der es den für die Zusammenarbeit beim Verbraucherschutz zuständigen Behörden der Mitgliedstaaten ermöglicht, grenzüberschreitende und EU-weite Verstöße gegen das Verbraucherrecht gemeinsam zu bekämpfen.

DURCHSETZUNGSSTRUKTUR DES GESETZES ÜBER DIGITALE DIENSTE

Die Durchsetzungsstruktur des Gesetzes über digitale Dienste umfasst die direkte, zentralisierte Zuständigkeit der Kommission für sehr große Online-Plattformen und sehr große Online-Suchmaschinen sowie die Koordinierung und Zusammenarbeit mit mehreren nationalen Behörden, insbesondere im Rahmen des Europäischen Gremiums für digitale Dienste, das sich auch auf eine spezielle Arbeitsgruppe zum Schutz Minderjähriger stützt.

Es handelt sich hierbei um einen neuen Durchsetzungsrahmen, der sich durch den Vorteil auszeichnet, dass die Durchsetzung für die größten Plattformen, die nahtlos über Grenzen hinweg tätig sind, zentral auf Kommissionsebene zusammenläuft. Einige dieser Plattformen gehören zu den größten und am besten mit Ressourcen ausgestatteten Unternehmen der Welt, deren Erträge häufig das BIP von EU-Mitgliedstaaten übersteigen. Dieser Rahmen fördert darüber hinaus die kohärente Anwendung der Vorschriften in der gesamten EU und bis hinunter zur nationalen Ebene (z. B. durch die Leitlinien zum Schutz Minderjähriger und die Rechtsprechung).

Die Abschreckungswirkung ist erheblich, wobei Befugnisse zur Verhängung von Geldstrafen, die zu den größten der Welt zählen, und einstweilige Maßnahmen zu einer raschen Änderung der Praktiken von Plattformen führen können, wie die Verpflichtungszusagen von TikTok und die Einstellung von TikTok Lite in der EU²⁶¹ zeigen. Im Kontext von Ermittlungen verfügt die Europäische Kommission über solide Durchsetzungsinstrumente und Ermittlungsbefugnisse. Hierzu zählt insbesondere die Möglichkeit, granulare, sensible Daten und Informationen anzufordern und in den Räumlichkeiten von Anbietern Kontrollen durchzuführen. Dies erlaubt einen Zugang zu den Systemen, der Gestaltung und den Entscheidungen der Anbieter, den es bisher nicht gab.

In Extremfällen, in denen die Zuwiderhandlung anhält und dadurch einen ernsthaften, akuten Schaden verursacht, kann die Kommission den Koordinator für digitale Dienste (Digital Services Coordinator, DSC) des Mitgliedstaats, in dem der Anbieter ansässig ist, ersuchen, die zuständige Justizbehörde aufzufordern, die vorübergehende Beschränkung des Zugangs zu dem Dienst anzuordnen²⁶².

Die Durchsetzungsmaßnahmen der Europäischen Kommission erforderten einen erheblichen Kapazitätsaufbau und beschleunigen sich nun zunehmend. Wie die vorläufigen Ergebnisse zu TikTok hinsichtlich einer potenziell suchterzeugenden Gestaltung und zu Meta in Bezug auf die Altersfeststellung zeigen, nimmt die zeitliche Effektivität dieser Maßnahmen schrittweise zu. Dazu trugen auch die in den Leitlinien zum Schutz Minderjähriger festgelegten Benchmarks für die Einhaltung der Vorschriften bei.

Die anfängliche Übersicht über die Erwartungen der Kommission in Bezug auf zentrale Fragen bei Durchsetzungsmaßnahmen, einschließlich vorläufiger Feststellungen und Verpflichtungen, sollte auch den Anbietern zugehen und sich in der laufenden Praxis der Risikobewertungs- und Risikominderungszyklen widerspiegeln. Dies dürfte bereits zu Änderungen bei den Plattformdiensten führen, bevor die Einleitung förmlicher Durchsetzungsmaßnahmen erforderlich wird.

Angesichts der Ressourcen, die für die Einleitung rechtlicher Schritte gegen Unternehmen, die Durchsetzungsmaßnahmen der Kommission unterliegen, erforderlich sind, sollte mit jedem Durchsetzungsrahmen sichergestellt werden, dass auch Zeit für die Gewährleistung der Verfahrensanforderungen investiert wird und alle denkbaren Vorsichtsmaßnahmen getroffen werden, damit Rechtssachen nach allen Graden des Ermessens vor Gericht Bestand haben.

Der risikobasierte, technologieneutrale Ansatz des Gesetzes über digitale Dienste bildet die Grundlage für zukunftssichere Durchsetzungsmaßnahmen. Dieser entwickelt sich Dank der Risikobewertungs- und Auditzyklen der Plattformen, der damit verbundenen Verpflichtungszusagen oder anderer Reaktionen auf Durchsetzungsmaßnahmen sowie der Benennung neuer Dienste fortwährend weiter. Die kürzlich eingeleitete Untersuchung gegen X im Zusammenhang mit seinem KI-System Grok und der nicht einvernehmlichen Weitergabe intimer Bilder (einschließlich durch KI erzeugter Bilder) zeigt, wie die Durchsetzung im Rahmen des Gesetzes über digitale Dienste rasch neue problematische Praktiken oder Funktionen abdecken kann, die in Online-Plattformen enthalten sind.

Ebenso zeigt die kürzlich erfolgte Benennung von WhatsApp als sehr große Online-Plattform, wie Dienste in den Anwendungsbereich des Gesetzes über digitale Dienste fallen können, wenn sie die Merkmale und Eigenschaften von Online-Plattformen annehmen.

BESCHLÜSSE UND VERFAHREN IM ZUSAMMENHANG

MIT DEM GESETZ ÜBER DIGITALE DIENSTE

Die Europäische Kommission und die nationalen Behörden haben seit dem Inkrafttreten des Gesetzes über digitale Dienste eine Reihe von Durchsetzungsmaßnahmen zum Schutz Minderjähriger eingeleitet oder abgeschlossen. Die unten aufgeführten Entscheidungen und Verfahren haben den Maßstab gesetzt, an dem die Einhaltung der Vorschriften durch die Plattformen nun beurteilt wird. Mit dem Vorschreiten der Durchsetzungsmaßnahmen wird sich dies weiterentwickeln und beispielsweise andere Dienstleistungen und Fragestellungen abdecken, wobei eine kontinuierliche Risikobewertung und Risikominderung sowie Auditzyklen als Informationsgrundlage dienen werden.

Im Februar 2026 nahm die Europäische Kommission vorläufige Feststellungen an, wonach die potenziell suchterzeugende Gestaltung von TikTok nicht den Schutzstandards des Gesetzes über digitale Dienste entspricht. In diesen Ergebnissen wird die Auffassung vertreten, dass TikTok die grundlegende Gestaltung seines Dienstes ändern muss, z. B. durch die Deaktivierung wichtiger suchterzeugender Funktionen wie „unendliches Scrollen“, die Einführung wirksamer „Bildschirmzeitpausen“ (auch während der Nacht) und die Anpassung seines Empfehlungssystems²⁶³.

Im März 2026 nahm die Kommission vorläufige Feststellungen in Bezug auf vier sehr große pornografische Plattformen (Pornhub, XNXX, Stripchat und XVideos) an, da sie keine ordnungsgemäße Altersüberprüfung eingeführt hatten²⁶⁴. Ergänzt wurde dies durch eine koordinierte Maßnahme des Europäischen Gremiums für digitale Dienste gegen kleinere Plattformen mit pornografischen Inhalten²⁶⁵.

Im April 2026 veröffentlichte die Europäische Kommission ferner einen vorläufigen Bericht, in dem sie feststellte, dass Meta gegen das Gesetz verstoßen hat, da es Minderjährige unter 13 Jahren nicht an der Nutzung von Instagram und Facebook hinderte²⁶⁶.

Außerdem laufen Durchsetzungsmaßnahmen gegen Snapchat, die der Untersuchung mutmaßlich unzureichender Altersfeststellungs- und Standardeinstellungen, eines unzureichenden Schutzes Minderjähriger vor Grooming oder der Anwerbung für kriminelle Aktivitäten und unwirksamer Instrumente zur Moderation von Inhalten dienen, mit denen die Verbreitung von Informationen, die die Nutzer zum Verkauf rechtswidriger Produkte, einschließlich Drogen, und altersbeschränkter Waren führen, verhindert wird²⁶⁷.

Im Rahmen akzeptierter Verpflichtungszusagen stimmte AliExpress einem Standardsystem zu, das die Sichtbarkeit von für Erwachsene vorgesehenen Produkten einschränkt, einschließlich der automatischen Verwischung von Bildern von Produkten für Erwachsene durch KI-gestütztes Echtzeit-Scannen²⁶⁸.

Auf nationaler Ebene untersucht die niederländische Regulierungsbehörde für Verbraucher und Märkte (ACM) die Videospielplattform Roblox im Zusammenhang mit möglichen Risiken, denen Minderjährige auf der Plattform²⁶⁹ ausgesetzt sind.

Weitere Verfahren in Bezug auf suchterzeugende Gestaltung, Empfehlungssysteme, die Verbreitung rechtswidriger Inhalte (einschließlich Darstellungen sexuellen Kindesmissbrauchs) und Schutzmaßnahmen für Marktplätze laufen gegen Facebook, Instagram, X betreffend Grok²⁷⁰, Shein²⁷¹ und Temu²⁷². Eine frühere Untersuchung von TikTok Lite führte zum Verpflichtungsbeschluss der Kommission und zur endgültigen Einstellung dieser Funktion auf dem EU-Markt.

Die Auswirkungen der bevorstehenden Durchsetzungsmaßnahmen in Bezug auf die oben genannten Dienstleistungen und Themen verdeutlichen die konkreten Erwartungen der Kommission und setzen hohe Maßstäbe für die Einhaltung der Vorschriften. Dies wird in Änderungen der Dienstleistungserbringung nicht nur für einzelne Online-Plattformen, die Gegenstand der Untersuchung sind, sondern auch für alle anderen Anbieter, die in den Anwendungsbereich des Gesetzes über digitale Dienste fallen, einfließen.

Um das Potenzial des Gesetzes über digitale Dienste voll auszuschöpfen, muss es nun, da diese Durchsetzungsstruktur einsatzbereit ist, möglicherweise weiter gestärkt werden, um sicherzustellen, dass Durchsetzungsfälle mit der erforderlichen Schnelligkeit und Dringlichkeit durchgeführt werden können und die volle Wirkung des Gesetzes über digitale Dienste erzielt wird. Zu diesem Zweck sollten sämtliche Behörden, die auf nationaler und EU-Ebene an der Durchsetzung beteiligt sind, beständig über angemessene Ressourcen für die Erfüllung ihres Auftrags verfügen.

DURCHSETZUNGSSTRUKTUR DER KI-VERORDNUNG

Die Durchsetzungsstruktur der KI-Verordnung umfasst die unmittelbare, zentralisierte Zuständigkeit der Kommission für die Durchsetzung in Bezug auf KI-Modelle mit allgemeinem Verwendungszweck (einschließlich KI-Modellen mit allgemeinem Verwendungszweck mit systemischem Risiko) und KI-Systeme auf der Grundlage von KI-Modellen mit allgemeinem Verwendungszweck, bei denen das Modell und das System von demselben Anbieter oder von Anbietern entwickelt werden, die Teil desselben Unternehmens sind.

Mit der Omnibus-Verordnung über künstliche Intelligenz wird eine weitere Innovation eingeführt, wobei die Durchsetzung im Zusammenhang mit KI-Systemen, die im Rahmen des Gesetzes über digitale Dienste als sehr große Online-Plattformen oder sehr große Online-Suchmaschinen benannt oder in diese

integriert wurden, ebenfalls bei der Europäischen Kommission zentral zusammenläuft. Die Durchsetzung in Bezug auf andere KI-Systeme, die in den Anwendungsbereich der KI-Verordnung fallen, unterliegt der Zuständigkeit der nationalen Marktüberwachungsbehörden.

Die Durchsetzungsbefugnisse des Europäischen Büros für künstliche Intelligenz und der nationalen Marktüberwachungsbehörden gelten ab dem 2. August 2026. Ab diesem Datum wird das Büro für künstliche Intelligenz die Vorschriften für KI-Modelle mit allgemeinem Verwendungszweck²⁷³, KI-Systeme mit allgemeinem Verwendungszweck mit systemischem Risiko²⁷⁴ und KI-Systeme auf der Grundlage von KI-Modellen mit allgemeinem Verwendungszweck, bei denen das Modell und das System von demselben Anbieter oder einem Anbieter, der Teil desselben Unternehmens ist, entwickelt werden, sowie für KI-Systeme, die in sehr große Online-Plattformen und sehr große Online-Suchmaschinen integriert sind, durchsetzen. Die in der Omnibus-Verordnung zur KI vereinbarten Verpflichtungen für Hochrisiko-KI-Systeme gelten ab Dezember 2027 (für eigenständige KI-Systeme wie bestimmte KI-Systeme in der Bildung) und August 2028 (für KI-Systeme, die in regulierte Produkte wie Spielzeug eingebettet sind).

DURCHSETZUNGSSTRUKTUR DER DSGVO

Die DSGVO wird von den Datenschutzbehörden in den einzelnen EU-Mitgliedstaaten durchgesetzt, die befugt sind, Beschwerden zu untersuchen, Kontrollen durchzuführen, Abhilfemaßnahmen anzuordnen und Geldbußen für Verstöße gegen das Datenschutzrecht zu verhängen.

Verarbeitet ein Unternehmen (Verantwortlicher) in mehr als einem Mitgliedstaat personenbezogene Daten, ist die federführende Datenschutzbehörde, d. h. die Datenschutzbehörde am Ort der Hauptniederlassung des Unternehmens, für die Aufsicht über dieses Unternehmen zuständig.

Die federführende Aufsichtsbehörde arbeitet mit den Datenschutzaufsichtsbehörden der anderen EU-Mitgliedstaaten, in denen die Datenverarbeitung Auswirkungen hat, zusammen und koordiniert ihre Maßnahmen mit ihnen. Dies wird als Mechanismus der einzigen Anlaufstelle bezeichnet.

Die Datenschutzbehörden können auf der Grundlage von Einzelbeschwerden, obligatorischen Meldungen von Verstößen, Medienberichten oder eigenen Untersuchungen Ermittlungen einleiten. Organisationen, bei denen ein Verstoß gegen Datenschutzvorschriften festgestellt wurde, können mit Verarbeitungsverböten, Befolgungsanordnungen oder Geldbußen bis zu 20 Mio. EUR oder 4 % des weltweiten Jahresumsatzes belegt werden, je nachdem, welcher Betrag höher ist.

Wie in der Charta der Grundrechte der Europäischen Union festgelegt und in der DSGVO bekräftigt, müssen sämtliche Datenschutzbehörden unabhängig sein. Alle Mitgliedstaaten müssen sicherstellen, dass die Datenschutzbehörden mit den personellen, technischen und finanziellen Ressourcen zur wirksamen Wahrnehmung ihrer Aufgaben und Befugnisse ausgestattet werden.

Im Europäischen Datenschutzausschuss (EDSA) kommen alle Aufsichtsbehörden zusammen, damit die einheitliche Anwendung der DSGVO sichergestellt wird. Er bringt Leitlinien für die Anwendung der DSGVO heraus. Der EDSA arbeitet derzeit an Leitlinien für die Verarbeitung von Daten von Kindern. Der EDSA fördert auch die Zusammenarbeit zwischen Datenschutzbehörden.

Die DSGVO ist technologieneutral und verfolgt einen risikobasierten Ansatz. Dies bedeutet, dass Organisationen die einschlägigen technischen und organisatorischen Maßnahmen ergreifen müssen, die in einem angemessenen Verhältnis zu dem Risiko stehen, das von ihren Datenverarbeitungstätigkeiten ausgeht.

Ende letzten Jahres wurde die DSGVO-Verfahrensverordnung verabschiedet. Mit ihr wurden neue Vorschriften eingeführt, um bei der Durchsetzung der DSGVO die Zusammenarbeit zwischen den nationalen Datenschutzbehörden zu verbessern und so die Bearbeitung grenzüberschreitender Datenschutzbeschwerden zu beschleunigen. Im Mai 2025 veröffentlichten die Datenschutzbehörden die Helsinki-Erklärung zu mehr Klarheit, Unterstützung und Engagement. In dieser Erklärung kamen sie überein, die einheitliche Anwendung und Durchsetzung der DSGVO zu verbessern.

AUSGEWÄHLTE MASSNAHMEN UND VERFAHREN

ZUR DURCHSETZUNG DER DSGVO

Die DSGVO ist seit 2018 in Kraft. In dieser Zeit wurden wegen Verstößen gegen die Datenschutzvorschriften Geldbußen in Höhe von mehr als 7 Mrd. EUR gegen Organisationen verhängt²⁷⁵. Die Datenschutzbehörden können von ihren Befugnissen Gebrauch machen, um Unternehmen dazu zu verpflichten, ihre Verarbeitungstätigkeiten mit den Vorschriften in Einklang zu bringen. Dies ermöglicht den Datenschutzbehörden, vor der Einleitung einer Untersuchung mit den Verantwortlichen Kontakt aufzunehmen, wodurch Zeit und Ressourcen eingespart werden.

So arbeitete beispielsweise die irische Datenschutzkommission im Februar 2023 mit Meta im Zusammenhang mit Markierungen auf Instagram zusammen. Wenn ein Kind ein öffentliches Konto markieren wollte, bei dem es kein Follower war, erhielt es die Meldung „Konto konnte nicht markiert werden. Stelle Dein Konto auf öffentlich um, damit du andere, die keine Follower von dir sind, markieren kannst“²⁷⁶.

Diese Meldung enthielt auch die Schaltfläche „Weiter zu den Einstellungen“, die den Nutzer zu einem Menü führte, in dem er sein Konto von privat auf öffentlich umstellen konnte. In dieser Konfiguration wurden Kinder weder vor den möglichen Folgen dieser Änderung gewarnt, noch wurden sie zur Seite mit häufig gestellten Fragen (FAQ) oder Artikeln im Hilfezentrum weitergeleitet.

Nach Gesprächen mit dem Datenschutzverantwortlichen wurden Änderungen an den Nutzerbenachrichtigungen vorgenommen. Die Meldung wurde aktualisiert und lautet nun „Konto konnte nicht markiert werden. Dein Konto ist privat, sodass du nur deine eigenen Follower markieren kannst. Du kannst deine Privatsphäre in den Einstellungen verwalten“.

„Weiter zu den Einstellungen“ wurde durch die Schaltfläche „Mehr erfahren“ ersetzt, die die Nutzer zu einem Artikel im Hilfezentrum führt, in dem sie herausfinden können, wie sie ihr Nutzerkonto jederzeit privat gestalten können, welche Unterschiede zwischen privaten und öffentlichen Konten bestehen, wie die Nutzer die Privatsphäre auf Instagram verwalten können und welche Informationen Eltern darüber erhalten, „Wer die Posts meines Kindes auf Instagram sehen kann“.

Die Datenschutzbehörden trafen mehrfach Entscheidungen in Bezug auf Verstöße gegen die DSGVO im Zusammenhang mit den Daten von Kindern. Sie erließen zudem Verarbeitungsverbote, nach denen einem Verantwortlichen vorgeschrieben wurde, personenbezogene Daten betroffener Personen, einschließlich Daten von Kindern, erst dann zu verarbeiten, wenn ihre Verarbeitung im Einklang mit den Anforderungen der DSGVO steht. Eine Auswahl solcher Maßnahmen wird nachstehend aufgeführt.

Mehrere Datenschutzbehörden leiteten Untersuchungen gegen Verantwortliche ein, die gegen den Grundsatz des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen verstießen. Beispielsweise verhängte die irische Datenschutzkommission gegen TikTok eine Geldbuße in Höhe von 345 Mio. EUR, da festgestellt worden war, dass das Unternehmen gegen mehrere Bestimmungen der DSGVO verstieß.

Hierzu zählten der Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen sowie der Grundsatz der Datenminimierung. Die Datenschutzkommission stellte fest, dass TikTok gegen diese Bestimmungen verstieß, da es die Konten von Kindern standardmäßig inner- oder außerhalb von TikTok für alle als öffentlich einstellte.

Die irische Datenschutzkommission stellte ferner fest, dass TikTok Dark Patterns verwendete, um Kinder dazu zu bewegen, sich standardmäßig für öffentliche Konten zu entscheiden. Dies bedeutete, dass jeder den Inhalt dieser Konten einsehen konnte, was einen Verstoß gegen den Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen sowie gegen den Grundsatz der Verarbeitung nach Treu und Glauben darstellte. Sie stellte ferner fest, dass TikTok versäumte, sicherzustellen, dass erwachsene Nutzer, die das Konto eines Kindes durch den Begleiter-Modus „Family Pairing“ beaufsichtigen, als Elternteil oder Vormund des Kindes verifiziert wurden ²⁷⁷.

Darüber hinaus verhängte die irische Datenschutzkommission gegen Instagram eine Geldbuße in Höhe von 450 Mio. EUR, da sie festgestellt hatte, dass Instagram gegen den Grundsatz des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen verstieß. Instagram hatte Kindern ermöglicht, Geschäftskonten einzurichten, bei denen im Profil öffentlich zugängliche Kontaktdaten angegeben werden mussten. Die Datenschutzkommission stellte fest, dass Instagram gegen diesen Grundsatz verstieß, da alle Nutzerkonten standardmäßig als öffentlich zugänglich eingestellt wurden. Dies bedeutete, dass jeder den Inhalt des Kindes einsehen konnte, sofern dieses die Einstellung nicht änderte ²⁷⁸.

Die italienische Datenschutzbehörde verhängte aufgrund von Bedenken hinsichtlich der Sicherheit von Kindern, insbesondere angesichts des Todes eines zehnjährigen italienischen Mädchens, ein vorübergehendes Verbot der Verarbeitungstätigkeiten von TikTok. Mit dem Verbot wurde die Verarbeitungstätigkeit von TikTok für Nutzer, deren Alter nicht mit Sicherheit festgestellt werden konnte, mit sofortiger Wirkung beschränkt. Dies führte dazu, dass die Plattform das Alter ihrer italienischen Nutzer erneut überprüfte und mehr als eine halbe Million Konten schloss, bei denen der Verdacht bestand, dass sie Minderjährigen unter 13 Jahren gehörten; dies ist das Alter, ab dem TikTok Kindern die Nutzung seines Dienstes erlaubt ²⁷⁹.

Anfang dieses Jahres leitete die irische Datenschutzkommission gegen X eine Untersuchung im Zusammenhang mit der Erstellung nicht einvernehmlicher sexualisierter Bilder, u. a. auch von Kindern, die das KI-Tool Grok verwendeten, ein. Die Datenschutzkommission wird prüfen, ob X die Artikel über Datenminimierung und Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen einhält ²⁸⁰.

DURCHSETZUNG DER AVMD-RICHTLINIE UND

ONLINE-SCHUTZ MINDERJÄHRIGER

Der Schutz von Minderjährigen ist ein Schwerpunktbereich bei der Durchsetzung durch die Medienregulierungsbehörden. Im Jahr 2024 bewertete die Gruppe europäischer Regulierungsstellen für audiovisuelle Mediendienste (ERGA) die von den Medienregulierungsbehörden angenommenen Maßnahmen zum Schutz Minderjähriger. Sie gelangte zu dem Schluss, dass Kriterien für die Einstufung schädlicher Inhalte für Minderjährige festgelegt und präzisiert werden müssen.

Ein Beispiel für die im Hinblick auf den Schutz Minderjähriger erfolgte Umsetzung der AVMD-Richtlinie in Bezug auf Video-Sharing-Plattformen findet sich in Italien. AGCOM, die italienische Regulierungsbehörde für das Kommunikationswesen, stellte fest, dass auf TikTok Videos über „französische Narben“ zu

finden sind. AGCOM leitete auf der Grundlage der Verordnung über Video-Sharing-Plattformen (VSP) ein Interventionsverfahren ein, das TikTok, eine Video-Sharing-Plattform mit Sitz in Irland, dazu veranlasste, die Videos zu entfernen.

Die deutsche Regulierungsbehörde DLM erließ Maßnahmen gegen Porno-Plattformen in Zypern und Tschechien. Das grenzüberschreitende Verfahren stützte sich, wie in der AVMD-Richtlinie vorgesehen, auf die Richtlinie über den elektronischen Geschäftsverkehr. Rechtsgrundlage war der Jugendmedienschutz-Staatsvertrag (JMStV), mit dem die AVMD-Richtlinie umgesetzt wird; einschlägige Bestimmungen waren das Verbot der Verbreitung von Pornografie an Minderjährige und Vorschriften zur Altersüberprüfung.

Das Europäische Medienfreiheitsgesetz (European Media Freedom Act, EMFA)²⁸¹, mit dem ein grenzüberschreitendes Verfahren zur Durchsetzung von Verpflichtungen für in einem anderen Mitgliedstaat niedergelassene Video-Sharing-Plattformen eingeführt wird, wurde auch in Bezug auf mehrere in Zypern niedergelassene Porno-Plattformen in Kraft gesetzt. Dies veranlasste die betreffenden Plattformen dazu, die Verpflichtungen der AVMD-Richtlinie zum Schutz Minderjähriger, einschließlich der Altersüberprüfung, einzuhalten. Die zyprische Regulierungsbehörde prüft derzeit die Antworten der einschlägigen Anbieter (Stripchat) zu der Frage, wie sie die Altersüberprüfung in mehreren Ländern, z. B. in Deutschland, eingesetzt haben.

NETZ FÜR DIE ZUSAMMENARBEIT IM RAHMEN DER VERORDNUNG

ÜBER DIE ZUSAMMENARBEIT IM VERBRAUCHERSCHUTZ

(CONSUMER PROTECTION COOPERATION NETWORK, CPC-NETZ)

Wie in der Verbraucheragenda 2030 dargelegt, wird die Europäische Kommission zur weiteren Stärkung des Verbraucherrechts eine Überarbeitung der Verordnung über die Zusammenarbeit im Verbraucherschutz vorschlagen. Dies könnte möglicherweise dazu beitragen, in bestimmten Fällen die direkten Durchsetzungsbefugnisse auf EU-Ebene zu zentralisieren.

Dies würde sowohl zur Beschleunigung als auch zu einer stärkeren Abschreckungswirkung von Durchsetzungsmaßnahmen im Rahmen der CPC-Verordnung führen. Außerdem würde ein Beitrag zum besseren Schutz Minderjähriger geleistet, die aufgrund ihrer erhöhten Schutzbedürftigkeit und ihrer mangelnden Erfahrung einem hohen Risiko einer Gefährdung durch unlautere Online-Geschäftspraktiken ausgesetzt sind.

AUSGEWÄHLTE DURCHSETZUNGSMASSNAHMEN DES CPC-NETZES

Für den digitalen Sektor veröffentlichte die Europäische Kommission im März 2025 den gemeinsamen Standpunkt des CPC-Netzes zu Star Stable Online²⁸². Das Netzwerk stellte Verstöße gegen die UGP-Richtlinie und die Richtlinie über die Rechte der Verbraucher fest, beispielsweise, dass Kinder dazu gedrängt werden, virtuelle Währungen oder Gegenstände direkt im Spiel (In-Game) zu kaufen oder Erwachsene dazu zu bewegen, dies für sie zu tun, Dark Patterns (Behauptungen über die Knappheit virtueller In-Game-Währung oder In-Game-Inhalte), das Fehlen klarer, transparenter, an Kinder angepasster Informationen über den Kauf und die Verwendung virtueller In-Game-Währungen und mangelnde Offenlegung kommerzieller Inhalte durch Influencer. Die Kommission fördert derzeit den Dialog zwischen dem CPC-Netz und dem Unternehmen, um diesen Verstößen gegen das EU-Verbraucherrecht ein Ende zu setzen.

Im März 2025 veröffentlichte die Kommission die wichtigsten Grundsätze des CPC-Netzes zu virtuellen In-Game-Währungen, die die gemeinsame Auslegung der bestehenden EU-Verbraucherschutzvorschriften (insbesondere der Richtlinie über unlautere Geschäftspraktiken und der Richtlinie über die Rechte der Verbraucher) durch die CPC-Behörden widerspiegeln. Diese zentralen Grundsätze zielen darauf ab, Transparenz und Fairness bei der Verwendung käuflich erwerbbarer virtueller Währungen in der Videospielbranche zu fördern und sicherzustellen, dass die Schutzbedürftigkeit der Verbraucher, insbesondere von Kindern, geachtet wird²⁸³.

Das Thema Influencer-Marketing ist für das CPC-Netz von großem Interesse, unter anderem auch, wenn diese Praktiken Kinder betreffen. Im Jahr 2023 führten die nationalen CPC-Behörden aus 22 Mitgliedsstaaten eine umfassende Überprüfung der Beiträge von 576 Influencern durch, um zu überprüfen, ob diese ihre Werbetätigkeiten offenlegen, wie im EU-Verbraucherrecht vorgeschrieben ist. Ein Ergebnis der Überprüfung war, dass 62 % der überprüften Influencer für weitere Ermittlungen vorgemerkt wurden²⁸⁴. Darüber hinaus startete die Europäische Kommission die Rechtsplattform für Influencer, auf der Influencer praktische Informationen über die Einhaltung des EU-Rechts finden können²⁸⁵.

Im Februar 2022 wurde eine koordinierte Maßnahme des CPC-Netzes gegen TikTok eingeleitet. Dabei ging es um Bedenken der CPC-Behörden im Zusammenhang mit verstecktem Marketing, aggressiven Werbetechniken, die sich an Kinder richten, und bestimmten Vertragsklauseln in den Richtlinien von TikTok, die als irreführend und verwirrend für die Verbraucher angesehen werden könnten.

Im Juni 2022 verpflichtete sich TikTok, seine Praktiken an die EU-Vorschriften über Werbung und Verbraucherschutz anzugleichen²⁸⁶. Die CPC-Behörden überwachen die Einhaltung der Vorschriften durch TikTok, insbesondere, ob deren Geschäftspraktiken (z. B. Werbung) hinreichend transparent sind, damit Kinder ihre Beschaffenheit verstehen können.

VERBRAUCHERBILDUNG UND RECHTSBEHELFE

Durch die kürzlich erfolgte Annahme der Richtlinie (EU) 2025/2647 zur Überarbeitung der Richtlinie über alternative Streitbeilegung können Verbraucher auf die außergerichtliche Streitbeilegung zurückgreifen, um Streitigkeiten im Zusammenhang mit digitalen Diensten und Inhalten sowie Streitigkeiten im Zusammenhang mit vorvertraglichen Informationen beizulegen, wenn ein Vertrag abgeschlossen worden ist.

Durch die Ausweitung des Anwendungsbereichs der Richtlinie wurde die außergerichtliche Streitbeilegung durch die Möglichkeit, mehr verbraucherrechtliche Streitigkeiten auf diese Weise beizulegen, an das digitale Zeitalter angepasst. Beispiele hierfür sind Streitigkeiten im Zusammenhang mit einem Videospielabonnement oder mit der Beschreibung eines Produkts, das sich an Minderjährige richtet. Die Richtlinie über Verbandsklagen ermöglicht benannten qualifizierten Einrichtungen wie Verbraucherorganisationen und öffentlichen Stellen, Klagen zum Schutz der Kollektivinteressen der Verbraucher anzustrengen. Dies gilt auch für Minderjährige, die von rechtswidrigen Praktiken von Unternehmen betroffen sind.

Klagen können auf die Einstellung rechtswidriger Praktiken und kollektive Rechtsbehelfe für Verbraucher abzielen. Erhoben werden können Klagen zur Durchsetzung von Verbraucherrechten, die unter mehr als 70 in Anhang I der Richtlinie aufgeführte EU-Rechtsakte fallen; hierzu zählen die Richtlinie über unlautere Geschäftspraktiken, die DSGVO, das Gesetz über digitale Märkte, das Gesetz über digitale Dienste oder die KI-Verordnung. Wenn ein neuer EU-Rechtsakt, der für den Schutz der Kollektivinteressen der Verbraucher relevant ist, von den EU-Gesetzgebern geprüft wird, kann er in den Anhang aufgenommen werden, wodurch seine Durchsetzung über das EU-Modell des kollektiven Rechtsschutzes für Verbraucher ermöglicht wird.

Unerledigte Angelegenheiten

SCHÄDLICHE GESTALTUNG WIRD NICHT AUSREICHEND ANGEANGEN

Die Durchsetzung der bestehenden Rechtsvorschriften befindet sich zwar in vielen Fällen noch in der Anfangsphase, aber sofern genügend Zeit und Ressourcen zur Verfügung stehen, ist davon auszugehen, dass sie Änderungen am Geschäftsmodell der sozialen Medien und anderer Anbieter digitaler Dienste mit sich bringt, indem festgelegt wird, welche Elemente dieses Modells letztlich mit den Grundrechten in der EU, einschließlich der Rechte des Kindes, vereinbar sind.

Ein klares Beispiel hierfür ist das Verbot von Werbung auf der Grundlage von Profiling für Minderjährige. Ähnlich wie das Verbot von Werbung auf der Grundlage von Profiling unter Verwendung besonderer Kategorien sensibler Daten wird mit diesem Verbot die Akzeptanz einer Praxis, die den Kern des Geschäftsmodells mehrerer Plattformen bildet, unmittelbar abgelehnt.

Ein weiteres Beispiel sind die Risikobewertungs- und Risikominderungspflichten, die Anbietern sozialer Medien und anderen Anbietern digitaler Dienste auferlegt werden. Diese Verpflichtungen zwingen die Anbieter, sich verstärkt darum zu bemühen, die Risiken zu erfassen, die ihre Dienste für die Grundrechte – einschließlich der Rechte des Kindes – mit sich bringen, und diese Risiken zu verhindern und zu mindern.

Dennoch besteht nach wie vor eine Reihe von Mängeln. Erstens beruhen die bestehenden EU-Rechtsvorschriften häufig auf einzeln aufgeführten Praktiken (z. B. spezifischen suchterzeugenden Merkmalen). Dies führt zu einer strukturellen Verzögerung. Ein funktionsbezogener Ansatz kann zu Regelungslücken führen, da sich digitale Dienste im Laufe der Zeit über die in den Rechtsvorschriften ausdrücklich aufgezählten und behandelten Merkmale hinaus weiterentwickeln. Diese Entwicklung kann absichtlich erfolgen, um eine Durchsetzung durch die Regulierungsbehörden zu vermeiden.

Darüber hinaus sind Risiken häufig bereichsübergreifend und ergeben sich nicht aus einem einzelnen Merkmal oder einer einzelnen Funktion, sondern aus der Interaktion mehrerer Merkmale oder der Gestaltung einer Dienstleistung im weiteren Sinne. Neue Formen audiovisueller Inhalte sind zu prüfen.

Immersive Umgebungen, die auf Technologien der erweiterten Realität und Kurzformat-Autoplay-Videos beruhen, brachten beispielsweise Risiken für Kinder mit sich, die bei der Einführung der einschlägigen gesetzgeberischen Instrumente nicht vorhergesehen wurden.

Rechtsvorschriften können im Verlauf ihrer Umsetzung angepasst werden, wie die Ermittlungen gegen X/Grok nach dem Gesetz über digitale Dienste und die Benennung von WhatsApp als sehr große Online-Plattform zeigen. Diese Anpassung erfolgt jedoch für jedes Merkmal einzeln, nachdem der Schaden in dem für förmliche Durchsetzungsverfahren üblichen Tempo festgestellt wurde.

Darüber hinaus wird in den bestehenden EU-Rechtsvorschriften das Kerngeschäft von Plattformen indirekt geregelt, indem ein auf den Grundrechten basierender Rahmen geschaffen wurde, innerhalb dessen jedes Geschäftsmodell betrieben werden sollte. So müssen beispielsweise Anbieter sehr großer Online-Plattformen und -Suchmaschinen spezifische Transparenz- und Gestaltungsanforderungen in Bezug auf Empfehlungssysteme einhalten²⁸⁷, und Anbieter sehr großer Online-Plattformen müssen für jedes ihrer Empfehlungssysteme mindestens eine Option anbieten, die nicht auf Profiling²⁸⁸ beruht; aber wie sie ihre Empfehlungssysteme konkret gestalten sollten oder nicht gestalten dürfen, kann im Rahmen von Durchsetungsmaßnahmen bestimmt werden.

Derzeit befinden sich Regulierungsbehörden häufig im Hintertreffen, wenn sie versuchen, in der sich rasch wandelnden Welt sozialer Medien+, in der explizite Merkmale und Funktionen festgelegt werden können, die sich auch nach der Markteinführung digitaler Dienste weiterentwickeln, die Rechtsvorschriften durchzusetzen. Dadurch sind möglicherweise Millionen von Nutzerinnen und Nutzern, darunter auch Kinder und Jugendliche, Gefahren ausgesetzt. In einigen Fällen können Risiken erst dann eintreten oder deutlich werden, wenn die Dienste bereits auf den Markt gebracht wurden, beispielsweise aufgrund der Art und Weise, wie diese Merkmale oder Funktionen in der Praxis genutzt werden, oder in Abhängigkeit vom jeweiligen Kontext. Was die Durchsetzung betrifft, so liegt die Beweislast, wenn Anbieter bestreiten, dass sie ihren Sorgfaltspflichten nicht nachgekommen sind, – heute – häufig bei den Durchsetzungsbehörden der EU und der Mitgliedstaaten, die im Wege langwieriger und kostspieliger Gerichtsverfahren gegen sehr gut aufgestellte große Unternehmen nachweisen müssen, dass soziale Medien und andere digitale Dienste schädlich sind.

„Unser Ziel ist nicht, Kinder auszuschließen, sondern dafür zu sorgen, dass die digitale Welt ihnen entsprechend ihrer Entwicklung gerecht wird. Wenn Technologieanbieter Zugang zu unseren Kindern haben wollen, müssen sie nachweisen, dass sie die Anforderungen erfüllen.“

– LEANDA BARRINGTON-LEACH,
EXEKUTIVDIREKTORIN DER
5RIGHTS FOUNDATION

Daher könnte es zur Regel werden, dass Anbieter sozialer Medien und anderer digitaler Dienste, die für Kinder und Jugendliche potenziell risikobehaftete Dienste einführen, betreiben oder aktualisieren, vor der Markteinführung nachweisen müssen, dass diese Dienste oder neuen Funktionen für Minderjährige sicher sind.

UNTERSCHIEDLICHE NATIONALE ANSÄTZE IN BEZUG AUF

ALTERSBESCHRÄNKUNGEN UND DIE EINWILLIGUNG VON KINDERN

Die Altersfrage ist die sichtbarste politische Lücke in den bestehenden Rechtsvorschriften. Zwei Aktionsbereiche sollten hier geprüft werden. Erstens wird in der DSGVO generell festgelegt, dass Kinder 16 Jahre alt sein müssen, um einem „Dienst der Informationsgesellschaft“ ihre Einwilligung zur Verarbeitung ihrer personenbezogenen Daten zu erteilen. Die DSGVO bietet den Mitgliedstaaten die Möglichkeit, dieses Alter auf ein Alter zwischen 13 und 16 Jahren zu senken. Ist das Kind jünger als 16 Jahre (oder ein anderes von einem Mitgliedstaat vorgeschriebenes Alter), ist die Verarbeitung nur rechtmäßig, wenn der Träger der elterlichen Verantwortung seine Einwilligung dazu erteilt oder diese mit dessen Zustimmung erteilt wird.

Zweitens erlassen mehrere EU-Mitgliedstaaten derzeit Rechtsvorschriften über Altersbeschränkungen für Minderjährige beim Zugang zu sozialen Medien und anderen digitalen Diensten oder erwägen dies, wobei einige in Bezug auf die Schwellenwerte der EU und der Mitgliedstaaten für die Einwilligung sogar unterschiedliche Ansätze verfolgen. Die Ansätze der Mitgliedstaaten in Bezug auf das Mindestalter unterscheiden sich hinsichtlich des Anwendungsbereichs, der Altersgrenze, der erfassten Dienste und der Frage, ob die Einwilligung der Eltern den Schwellenwert außer Kraft setzen kann.

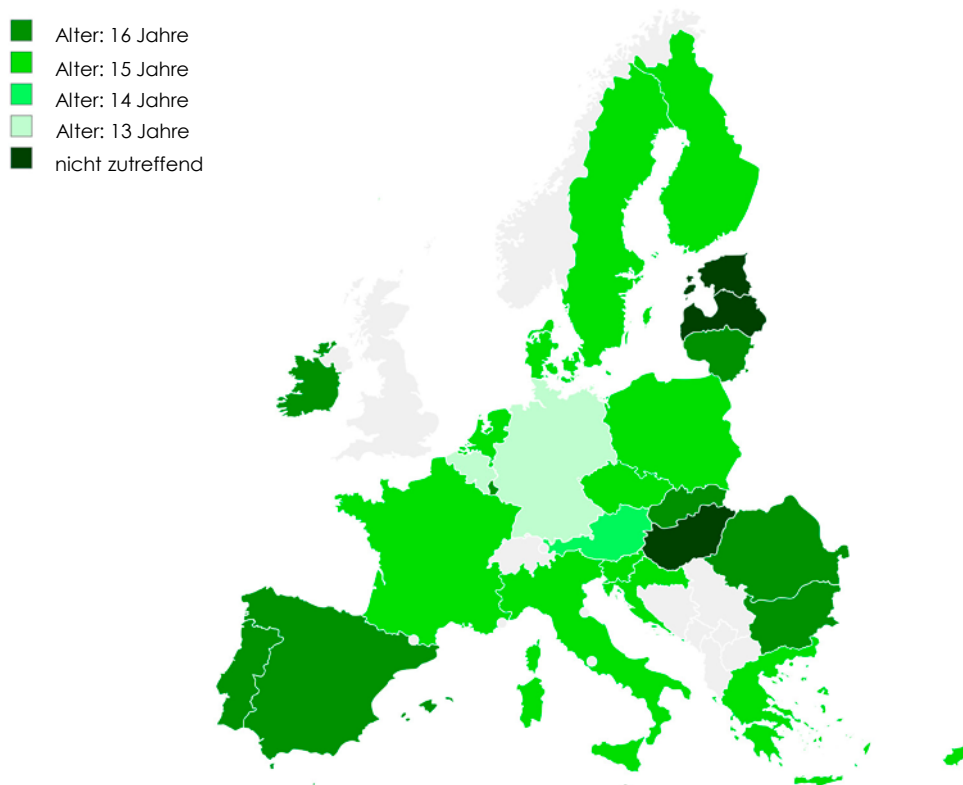
Die starke Zunahme nationaler Initiativen zur Festlegung von Altersbeschränkungen für den Zugang zu sozialen Medien und anderen digitalen Diensten birgt die Gefahr einer Fragmentierung des Binnenmarkts und eines ungleichen Schutzniveaus für Minderjährige in der EU. Mehrere Mitgliedstaaten, darunter Österreich, Zypern, Dänemark, Frankreich, Luxemburg, Griechenland, Spanien und Slowenien, fordern einen EU-weiten Ansatz für Altersbeschränkungen beim Zugang zu sozialen Medien+.

In der Erklärung von Jütland, die im Oktober 2025 auf Initiative des dänischen Ratsvorsitzes von 25 Mitgliedstaaten unterzeichnet wurde, wurde ein sichereres digitales Umfeld für Minderjährige gefordert, unter anderem durch Altersüberprüfungen und Bewertungen bezüglich des Alters, in dem Minderjährigen Zugang zu sozialen Medien und anderen digitalen Diensten gewährt werden sollte. In den Schlussfolgerungen des Europäischen Rates vom 23. Oktober 2025 und vom 19. März 2026 wird hervorgehoben, wie wichtig der Online-Schutz Minderjähriger ist.

In sämtlichen Mitgliedstaaten laufen derzeit entweder in den nationalen Parlamenten, Regierungen oder in der Zivilgesellschaft Debatten, in deren Mittelpunkt die Einführung von Altersbeschränkungen auf verschiedenen Ebenen steht. Die vorgeschlagenen Beschränkungen reichen von 13 bis 16 Jahren, wobei mitunter unterschiedliche Altersstufen mit oder ohne Einwilligung der Eltern in Betracht gezogen werden. Italien, Frankreich und Griechenland haben die Kommission über das Informationssystem für technische Vorschriften (Technical Regulations Information System, TRIS) förmlich von Gesetzesentwürfen in Kenntnis gesetzt.

Frankreich, Italien und Dänemark erwägen Beschränkungen für unter 15-Jährige. Zypern und Rumänien schlagen eine Grenze bei 16 Jahren und Deutschland schlägt eine Grenze von 13 Jahren vor. Griechenland und Dänemark schlagen zwei Stufen mit eingeschränktem Zugang unter 15 Jahren und Zugang nur mit Zustimmung der Eltern für 12- bis 15-Jährige (13 bis 15 Jahre im Falle Dänemarks) vor.

Abbildung 1: EU-Mitgliedstaaten, die Altersbeschränkungen für soziale Medien und andere digitale Dienste vorschlagen oder erwägen



Da viele Mitgliedstaaten die Einführung eines Mindestalters für soziale Medien+ mit unterschiedlichen Anwendungsbereichen und begleitende Verpflichtungen in Erwägung ziehen, wäre ein harmonisierter Ansatz auf EU-Ebene wichtig, um sicherzustellen, dass Minderjährigen in der gesamten EU online das gleiche Schutzniveau geboten wird. Um ein gleiches Schutzniveau zu gewährleisten, ist es ferner von entscheidender Bedeutung, zu prüfen, wie mögliche Altersbeschränkungen mit Sicherheitsmaßnahmen zusammenhängen, insbesondere denen, die durch EU-Rechtsvorschriften, einschließlich des Gesetzes über digitale Dienste, vorgeschrieben werden.

Von den Mitgliedstaaten vorgeschlagene Altersbeschränkungen können sich auf spezifische, von einzelnen Arten sozialer Medien und anderer digitaler Dienste ausgehende Risiken beziehen oder darauf abzielen, diesen zu begegnen. Um ein gleiches Schutzniveau für Minderjährige zu gewährleisten, muss ein harmonisierter Ansatz für die Altersüberprüfung mit Sicherheitsmaßnahmen einhergehen, die von den Regulierungsbehörden wirksam durchgesetzt werden, sowie mit Sicherheitsmerkmalen, die von sozialen Medien und anderen Anbietern digitaler Dienste eingeführt werden (entweder durch einen Ansatz der Sicherheit durch Technikgestaltung oder durch datenschutzfreundliche Voreinstellungen).

„Ein klares EU-weites Mindestalter würde Eltern in unmittelbarer Zukunft unterstützen, den Gruppen- und Sozialdruck auf Kinder verringern, und einen starken Anreiz für Plattformen schaffen, ihre Dienste im Einklang mit der Sicherheit und dem Wohlbefinden von Kindern umzugestalten.“

– LIES CRAEYNST,
GRÜNDERIN VON KIDSUNPLUGGED

ANSÄTZE IN BEZUG AUF ALTERSBESCHRÄNKUNGEN UND EINWILLIGUNG

Mitglied-staat	Diskussionsstand und angedachte Maßnahmen zu Altersbeschränkungen für digitale Dienste	Vorgeschlagenes oder in Betracht gezogenes Mindestalter	Mindestalter für eine Einwilligung in die Online-Datenverarbeitung
Belgien	Im April 2026 billigte die flämische Regierung einen Vorentwurf eines Dekrets zur Einführung eines gesetzlichen Mindestalters von 13 Jahren für bestimmte Online-Plattformen, die für Minderjährige schädlich sein können.	13	13
Bulgarien	Im Mai 2026 schlug eine Oppositionspartei Änderungen des Kinderschutzgesetzes vor, um den Zugang von Kindern unter 16 Jahren zu sozialen Medien zu beschränken. Der Zugang könnte ab dem Alter von 13 Jahren mit Zustimmung der Eltern gestattet werden.	16	14
Tschechien	Noch kein Vorschlag. Die Regierungspartei ANO (PfE) plant, in diesem Jahr Rechtsvorschriften zum Verbot für Kinder unter 15 Jahren vorzuschlagen.	15	15
Dänemark	Gesetzgebungsvorschlag wird derzeit ausgearbeitet. Im November 2025 verkündete die Regierung eine politische Einigung, Kindern unter 15 Jahren den Zugang zu sozialen Medien zu untersagen, ihn aber möglicherweise ab dem Alter von 13 Jahren zu gestatten, wenn die Eltern zustimmen.	15	15
Estland	Allgemeine Ablehnung der Idee, für den Zugang zu sozialen Medien Altersbeschränkungen aufzuerlegen.	nicht zutreffend	13
Deutschland	Bisher kein Gesetzgebungsvorschlag. Im November 2025 erklärte die Regierung ihre grundsätzliche Unterstützung für eine mögliche Regulierung und setzte einen Sachverständigenausschuss ein, der am 24. Juni seinen Bericht veröffentlichte. Dort werden ein Mindestalter von 13 Jahren und Beschränkungen des Marktzugangs zu nicht sicheren Diensten vorgeschlagen und ein Vorgehen auf EU-Ebene gefordert. Politische Parteien und NRO haben verschiedene Vorschläge unterbreitet.	13	16
Irland	Noch keine Gesetzgebungsinitiative. Der Tánaiste (Stellvertretender Ministerpräsident) spricht sich für eine Beschränkung des Zugangs zu sozialen Medien für Kinder unter 16 Jahren aus. Der Gemischte Ausschuss für Kunst, Medien, Kommunikation, Kultur und Sport sprach sich im Mai 2026 gegen ein solches Verbot aus.	16	16
Griechenland	Über ein Gesetz wird voraussichtlich im Sommer 2026 abgestimmt und es soll ab Januar 2027 in Kraft treten.	15	15
Spanien	Im April 2025 legte die spanische Regierung einen Gesetzesvorschlag zur Anhebung des Mindestalters für eine Zustimmung zur Verarbeitung personenbezogener Daten vor. Im Februar 2026 kündigte der Ministerpräsident an, dass Spanien den Zugang zu digitalen Plattformen für Kinder unter 16 Jahren verbieten werde.	16	14

Mitglied- staat	Diskussionsstand und angedachte Maßnahmen zu Altersbeschränkungen für digitale Dienste	Vorgeschlagenes oder in Betracht gezogenes Mindestalter	Mindestalter für eine Einwilligung in die Online- Datenverarbeitung
Frankreich	2025 wurde ein Gesetz vorgeschlagen (beide Parlamentskammern haben ihre Standpunkte angenommen, müssen sich jedoch noch auf den Kompromisstext verständigen). Das Gesetz soll im September 2026 in Kraft treten. Frankreich schlägt eine differenzierte Regelung vor: der Zugang von unter 15-Jährigen zu als schädlich eingestuften sozialen Medien soll komplett verboten und der zu den übrigen sozialen Medien an die Einwilligung der Eltern geknüpft werden.	15	15
Kroatien	Ein Gesetzgebungsvorschlag aus dem Jahr 2025 wurde im März 2026 abgelehnt.	15	16
Italien	Die Regierung plant eine Gesetzesinitiative, um den Zugang von Kindern unter 15 Jahren zu sozialen Medien zu verbieten. Parallel dazu wurden 2024 und 2026 zwei getrennte parlamentarische Initiativen eingereicht, die jedoch derzeit nicht vorankommen, da die Ministerpräsidentin erklärt hat, nicht unbedingt ein Verbot anzustreben.	15	14
Zypern	Die Regierung hat im Jahr 2026 eine Gesetzgebungsinitiative angekündigt.	15	14
Lettland	Noch kein Gesetzgebungsvorschlag. Im März 2026 einigte sich die Regierungskoalition darauf, eine Verordnung auszuarbeiten, um den Zugang zu sozialen Medien unter einem bestimmten Alter zu beschränken.	nicht zutreffend	13
Litauen	2026 wurde ein Gesetzgebungsvorschlag unterbreitet.	16	14
Luxemburg	In einer Entschließung des Parlaments (Januar 2026) wird die Schaffung eines EU-Rahmens oder die Koordinierung von Maßnahmen mit BE, DE und FR gefordert.	16	16
Ungarn	Noch kein Vorschlag.	nicht zutreffend	16
Malta	Im Februar 2026 fand eine öffentliche Konsultation zur Reform der sozialen Medien statt. Derzeit laufen die Anschlussarbeiten.	nicht zutreffend	13
Niederlande	In den Koalitionsplänen (Januar 2026) wird gefordert, auf EU-Ebene ein Mindestalter für den Zugang zu sozialen Medien festzulegen.	15	16
Österreich	Die Bundesregierung hat angekündigt, im Sommer 2026 einen Gesetzgebungsvorschlag vorzulegen.	14	14
Polen	Einige Mitglieder der unteren Kammer des Parlaments (Sejm) und das Ministerium für digitale Angelegenheiten haben Maßnahmen angekündigt.	15	16
Portugal	Eine parlamentarische Gesetzgebungsinitiative aus dem Jahr 2026 befindet sich in der Anhörungsphase.	16	13

Mitglied- staat	Diskussionsstand und angedachte Maßnahmen zu Altersbeschränkungen für digitale Dienste	Vorgeschlagenes oder in Betracht gezogenes Mindestalter	Mindestalter für eine Einwilligung in die Online- Datenverarbeitung
Rumänien	Ein Gesetzgebungsvorschlag zur Bestimmung des Alters der „digitalen Volljährigkeit“ wurde 2025 veröffentlicht. Andere werden ebenfalls in verschiedenen Verfahrensstadien erörtert.	15-16	16
Slowenien	Im Februar 2026 kündigte die Regierung Vorbereitungen zur Regulierung der Nutzung sozialer Medien für Kinder bis zum Alter von 15 Jahren an.	15	15
Slowakei	Ein Legislativvorschlag wurde 2026 vom Ministerium für Investitionen, regionale Entwicklung und Informatik angekündigt.	16	16
Finnland	Der Ministerpräsident und seine Partei veröffentlichten im November 2025 ein Positionspapier, in dem ein Verbot des Zugangs zu sozialen Medien für Kinder unter 15 Jahren befürwortet wird. In den nationalen Empfehlungen wird angeraten, soziale Medien unter 13 Jahren nicht zu nutzen.	15	13
Schweden	Die Regierung setzte einen Ausschuss ein, um zu prüfen, ob Kindern unter einem bestimmten Alter der Zugang zu sozialen Medien möglicherweise untersagt werden könnte; der Ausschuss hat eine Altersgrenze von 15 Jahren vorgeschlagen.	15	13

NUTZUNG DER EU-LÖSUNG FÜR DIE ALTERSVERIFIKATION

DURCH DIE MITGLIEDSTAATEN

Die EU-Lösung für die Altersverifikation ist technisch auf dem neuesten Stand und ihr Konzept kann von den Mitgliedstaaten und Marktteilnehmern angepasst werden. Die Wirksamkeit dieser Instrumente hinsichtlich der Stärkung des Online-Schutzes von Kindern wird jedoch letztlich davon abhängen, ob sie von den Mitgliedstaaten, Marktteilnehmern, sozialen Medien und anderen Anbietern digitaler Dienste tatsächlich genutzt werden.

Die Benennung vertrauenswürdiger Anbieter von Altersnachweisen ist auch für das reibungslose Funktionieren der EU-Lösung für die Altersverifikation von entscheidender Bedeutung. Trotz wiederholter Aufforderungen der Europäischen Kommission müssen viele Mitgliedstaaten hinsichtlich der Benennung vertrauenswürdiger Anbieter von Altersnachweisen noch tätig werden.

Eine harmonisierte EU-weite Altersbeschränkung für den Zugang zu sozialen Medien und anderen digitalen Diensten kann ohne ein Ökosystem zur Altersverifikation, das zum Nachweis des Alters Minderjähriger genutzt werden kann, nicht durchgesetzt werden. Die derzeitige EU-Lösung für die Altersverifikation kann im Einklang mit den nationalen Rechtsvorschriften technisch von 18 Jahren und älter auf andere Altersgruppen, z. B. Jugendliche, ausgeweitet werden.

Ohne vertrauenswürdige Anbieter von Altersnachweisen, die Altersnachweise für Minderjährige ausstellen können, laufen Anbieter sozialer Medien und anderer digitaler Dienste jedoch Gefahr, dass auf andere weniger robuste (z. B. Eigenerklärung) und/oder weniger datenschutzfreundliche Methoden zurückgegriffen wird, und die Mitgliedstaaten könnten Schwierigkeiten haben, eine wirksame Altersverifikation sicherzustellen.

DURCHSETZUNGSBEDARF: KAPAZITÄT, GESCHWINDIGKEIT

UND KOORDINIERUNG ZWISCHEN REGULIERUNGSBEHÖRDEN

Die bisherige Durchsetzung zeigt, dass die bestehenden gesetzgeberischen Instrumente zu Entscheidungen und sichtbaren Änderungen bei der Einhaltung der Rechtsvorschriften führen können. Zudem werden dadurch mehrere Herausforderungen deutlich.

Eine wirksame Durchsetzung ist von entscheidender Bedeutung für die Gewährleistung der Sicherheit von Kindern im Internet. Dafür sind ausreichende Befugnisse und gut aufgestellte Behörden erforderlich. In der Praxis können widersprüchliche Durchsetzungsstrukturen zu einer Reihe von Problemen führen. Dazu zählen die weitere Belastung begrenzter Ressourcen, der Zeitaufwand für die Einrichtung, eine erhöhte Komplexität sowie möglicherweise konkurrierende oder sich überschneidende Zuständigkeiten. Diese Probleme können für soziale Medien und andere Anbieter digitaler Dienste einen Negativanreiz für rechtskonformes Verhalten bieten oder sie sogar dazu veranlassen, die Einhaltung der Vorschriften zu vermeiden oder zu verzögern.

Eine große Herausforderung für die Regulierungsbehörden ist die Aufrechterhaltung eines angemessenen Personalbestandes mit dem erforderlichen Fachwissen. Da die Tätigkeiten der Anbieter immer komplexer werden, müssen die Regulierungsbehörden sicherstellen, dass sie über genügend angemessen qualifiziertes Personal verfügen, um wirksam bewerten zu können, ob bei sozialen Medien und anderen digitalen Diensten die Rechtsvorschriften eingehalten werden. Dies gilt sowohl auf EU-Ebene als auch auf nationaler Ebene.

Generell stellt die Verfügbarkeit und Koordinierung personeller und finanzieller Ressourcen für Kinderschutzsysteme (auch zur Unterstützung der behördlichen Durchsetzung) eine weitere Herausforderung²⁸⁹ dar. Eine Umkehr der Beweislast für die Durchsetzung, wie sie vorstehend erörtert wurde, kann dazu beitragen, die Durchsetzungskapazitäten zu verbessern und bessere Ergebnisse zu erzielen, ohne die begrenzten Ressourcen der Regulierungsbehörden sowohl auf EU-Ebene als auch auf nationaler Ebene zusätzlich zu belasten.

LÜCKE IN DER SICHERHEIT VON KINDERN: SEXUELLER MISSBRAUCH

UND SEXUELLE AUSBEUTUNG ONLINE

Die von 2021 bis zum 3. April 2026 geltende Übergangsverordnung enthielt befristete Vorschriften, die von bestimmten Verpflichtungen der Datenschutzrichtlinie für elektronische Kommunikation abweichen. Dadurch konnten Anbieter bestimmter interpersoneller Kommunikationsdienste Technologien für die Verarbeitung personenbezogener und anderer Daten einsetzen, um Material über sexuellen Kindesmissbrauch und Grooming aufzudecken und zu melden und Material aus ihren Diensten zu entfernen.

Im Dezember 2025 schlug die Europäische Kommission eine Verlängerung der Übergangsverordnung bis 2028 als vorübergehende Lösung bis zur Annahme der langfristigen Verordnung zur Prävention und

Bekämpfung des sexuellen Missbrauchs von Kindern vor. Das Europäische Parlament und der Rat konnten jedoch über diesen Vorschlag keine Einigung erzielen. Infolgedessen trat die Übergangsverordnung am 3. April 2026 außer Kraft, was zu Rechtsunsicherheit auf EU-Ebene führte.

In der langfristigen Verordnung über die Aufdeckung des sexuellen Missbrauchs von Kindern in der privaten Kommunikation, in der die meisten dieser Straftaten begangen werden, muss so bald wie möglich eine Lösung gefunden werden. Die proaktive Aufdeckung durch Anbieter dieser Dienste ist seit mehr als 15 Jahren die Hauptquelle für Ermittlungen im Zusammenhang mit sexuellem Kindesmissbrauch.

Die Aufdeckung sollte sich nicht nur auf bekanntes Material über sexuellen Kindesmissbrauch erstrecken, um eine Reviktimisierung zu verhindern, sondern auch auf neues Material über sexuellen Kindesmissbrauch, das häufig auf anhaltenden Missbrauch hindeutet und das auch KI-generiertes Material über sexuellen Kindesmissbrauch umfasst. Letzteres hat in den letzten Jahren exponentiell zugenommen (von 5 000 Meldungen im Jahr 2023 auf 1,3 Mio. Meldungen im Jahr 2025). Außerdem sollte auch die Aufdeckung von Grooming mit einbezogen werden, um drohenden Missbrauch zu verhindern und bereits stattfindenden Missbrauch zu unterbinden, der ebenfalls exponentiell zugenommen hat (um das Zwölfache in den letzten drei Jahren).

Weitere Lücken in den geltenden Rechtsvorschriften betreffen neu auftretende Formen des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern im Zusammenhang mit technologischen Entwicklungen wie KI-generiertes Material über sexuellen Kindesmissbrauchⁱ, Online-Grooming, Live-Streaming von Missbrauch, die Verbreitung von Anweisungen zur Begehung von Straftaten und der Betrieb eines Online-Dienstes zum Zweck des sexuellen Kindesmissbrauchs. Diese Fragen werden im Rahmen der vorgeschlagenen Überarbeitung des strafrechtlichen Rahmens (Richtlinie 2011/93/EU) behandelt.

Empfehlungen

EMPFEHLUNG 1

Eine harmonisierte EU-weite Zugangsbeschränkung für soziale Medien und andere digitale Dienste für Kinder unter 13 Jahren vorschlagen

Eine harmonisierte EU-weite Zugangsbeschränkung für soziale Medien und andere digitale Dienste, einschließlich KI-Begleitern, für Kinder unter 13 Jahren ist notwendig. Eine solche harmonisierte Zugangsbeschränkung würde einerseits die Umsetzung einer verhältnismäßigen, rechtskonformen Altersfeststellung erleichtern und andererseits die Festlegung von Anforderungen an die Anbieter sozialer Medien und anderer digitaler Dienste im Hinblick auf die Sicherheit durch Technikgestaltung begünstigen. Kinder unter 13 Jahren sollten nur mit Zustimmung und unter Aufsicht der Eltern oder im Bildungskontext zeitlich begrenzten Zugang zu altersgerechten sozialen Medien⁺ haben. Ab dem Alter von 13 Jahren sollten Jugendliche die Vorteile einer zunehmend eigenständigen Nutzung altersgerechter und sicherer sozialer Medien und anderer digitaler Dienste genießen können.

Harmonisierte Vorschriften über ein EU-weites Mindestalter von 13 Jahren würden zum reibungslosen Funktionieren des Binnenmarkts beitragen, indem ein einheitlicher Rahmen geschaffen würde, an den

ⁱ Um einen besseren Schutz der Rechte des Kindes zu gewährleisten, haben das Europäische Parlament und der Rat im Zusammenhang mit der Omnibus-Verordnung für künstliche Intelligenz vereinbart, ein Verbot von KI-Systemen aufzunehmen, die nicht einvernehmliche intime Inhalte und Darstellungen sexuellen Kindesmissbrauchs erzeugen. Dieses Verbot gilt mit Wirkung vom 2. Dezember 2026.

sich die Anbieter halten müssten. Durchsetzung und Aufsicht würden den Regulierungsbehörden sowohl auf nationaler Ebene als auch auf EU-Ebene durch harmonisierte Vorschriften erleichtert. Außerdem würde so dafür gesorgt, dass alle Minderjährigen in der EU dasselbe Maß an Schutz genießen, unabhängig von sozioökonomischen, kulturellen und einzelstaatlichen Faktoren.

EMPFEHLUNG 2

Funktionierende Systeme zur Altersfeststellung einführen, damit auf safety by design beruhende und altersgerechte Systeme zum Schutz und zur Stärkung Minderjähriger online ihre Wirkung entfalten können

Methoden der Altersverifikation – Altersüberprüfung und Altersschätzung – müssen verhältnismäßig sein und Mindestanforderungen unterliegen, insbesondere in Bezug auf die Grundrechte der Nutzerinnen und Nutzer, wozu auch Kinderrechte und die damit verbundenen Schutzvorkehrungen zählen. Alle zur Altersverifikation genutzten Methoden sollten höchsten Anforderungen in Bezug auf den Schutz der Privatsphäre und den Datenschutz genügen und auf die Verarbeitung von Ausweisdokumenten oder biometrischen Daten zum Zwecke der Altersschätzung verzichten. Es sollten technische Normen wie der „Null-Wissen-Beweis“ angewandt werden, um sicherzustellen, dass sowohl die zur Altersfeststellung verpflichtete Plattform als auch der Anbieter, der die Altersüberprüfung durchführt, keine Informationen erhalten, die das Tracking oder die Identifizierung der Nutzerinnen und Nutzer erlauben.

Die Methoden zur Altersverifikation sollten das Alter oder Altersgruppen entsprechend den Anforderungen präzise bestimmen können, und für eine einfache und zuverlässige Praxisanwendung unter realen Bedingungen geeignet sein. Die Methoden sollten robust sein, um einer Umgehung sowie Sicherheitsbedrohungen entgegenzuwirken, sie sollten inklusiv (und diskriminierungsfrei) sein und allen, die sie benötigen, gleichermaßen zur Verfügung stehen. Anbieter sozialer Medien und anderer digitaler Dienste müssen ihrer Verpflichtung nachkommen, zu verhindern, dass Minderjährige Dienste mit hohem Risikopotenzial nutzen oder mit Personen in Kontakt kommen, die sich als Kinder oder Jugendliche ausgeben.

Um eine EU-weit harmonisierte Altersbeschränkung in der Praxis durchzusetzen, müssen sich die Anbieter bei der Umsetzung von Altersbeschränkungen auf klare Leitlinien und Kriterien für den Einsatz von Technologien zur Altersverifikation stützen können. Darüber hinaus müssen Nutzer und Anbieter Zugang zu wirksamen, datenschutzfreundlichen, sicheren, inklusiven und nutzerfreundlichen Technologien zur Altersüberprüfung haben, damit sie diese in der Praxis durchsetzen können. In diesem Zusammenhang könnten EU-Lösungen für die Altersüberprüfung, die auf dem EU-Konzept für die Altersüberprüfung aufbauen, ein harmonisiertes, datenschutzfreundliches, dem neuesten Stand der Technik entsprechendes und interoperables Instrument für die Durchsetzung solcher Verpflichtungen auf EU-Ebene bieten.

Zur weiteren Stärkung dieses Rahmens müssen sowohl die Mitgliedstaaten als auch die Marktteilnehmer funktionsfähige Instrumente zur Altersverifikation bereitstellen, die an das EU-Konzept für die Altersüberprüfung angeglichen sind oder darauf aufbauen und der Empfehlung der Kommission zur Schaffung eines gemeinsamen Rahmens für EU-weite Technologien zur Altersüberprüfung folgen. In der Empfehlung der Kommission wird ein System festgelegt, in dem die Anforderungen an das Vertrauensmodell, die Governance und die Verpflichtungen der Anbieter von Lösungen zur Altersverifikation und von Altersnachweisen festgelegt werden.

Die Mitgliedstaaten sollten rasch vertrauenswürdige Anbieter von Altersnachweisen benennen. Für eine wirksame Altersverifikation von Minderjährigen müssen sie auch sicherstellen, dass Nachweise für Min-

derjährige, die jünger als 18 Jahre sind, bereitgestellt und/oder anerkannt werden. Dies beinhaltet, dass alle Minderjährige auch ohne einen nationalen Ausweis Zugang zu Mitteln zum Nachweis ihres Alters haben.

Es ist wichtig, dass die EU eine klare Rechtsgrundlage für die Umsetzung von Lösungen zur Altersverifikation schafft, um sicherzustellen, dass Anbieter sozialer Medien und anderer digitaler Dienste vertrauenswürdige Anbieter von Altersnachweisen akzeptieren. Die Altersfeststellung ist von entscheidender Bedeutung für gut funktionierende Beschwerdesysteme, die Kinder und Jugendliche in die Lage versetzen, ihre Rechte wahrzunehmen und sich online sicher zu bewegen.

EMPFEHLUNG 3

Vorschriften für zentrale Sicherheitsfunktionen bei der Gestaltung sozialer Medien und anderer digitaler Dienste erweitern und harmonisieren

Eine klar definierte Sicherung für die Sicherheit durch Technikgestaltung sowie altersgerechte Schutzvorkehrungen (z. B. potenzielle Beschränkungen für endloses Scrollen, automatische Wiedergabe, Push-Benachrichtigungen und problematische Systeme für personalisierte Empfehlungen) sollten in soziale Medien und andere digitale Dienste integriert werden. Soziale Medien und andere digitale Dienste sollten durch entsprechende integrierte Standardeinstellungen Schutz vor suchterzeugenden Gestaltungsmerkmalen, Dark Patterns, unerwünschter Kontaktaufnahme und dem Rabbit-Hole-Effekt bieten. Eine Erweiterung und Harmonisierung der Vorschriften über zentrale Sicherheitsfunktionen würde für Gewissheit und Einheitlichkeit im Bereich der sozialen Medien+ sorgen. Aufgrund der raschen technologischen Entwicklung sollten die Vorschriften über zentrale Sicherheitsfunktionen anpassbar sein, damit kontinuierlich auf neue schädliche Gestaltungsmerkmale reagiert werden kann.

EMPFEHLUNG 4

Beweislast, dass Produkte und Dienste für Minderjährige sicher sind, auf Anbieter sozialer Medien und anderer digitaler Dienste verlagern

Spezifische Altersbeschränkungen sollten gelten, bis die Anbieter sozialer Medien und anderer digitaler Dienste zentrale Sicherheitsfunktionen zum Schutz von Kindern und Jugendlichen einführen. Nur wenn Anbieter nachweisen können, dass sie sichere und altersgerechte Funktionen eingeführt haben und somit den von der EU und den Mitgliedstaaten ergriffenen Maßnahmen entsprechen, sollten sie ihre Dienste Minderjährigen anbieten dürfen. Wenn eine safe-by-design-Version vorhanden ist, sollten nicht altersgerechte Funktionen (Funktionen für Erwachsene) nur nach einer erfolgreichen Altersverifikation aktiviert werden können.

EMPFEHLUNG 5

Durchsetzungs- und Evaluierungskapazitäten stärken

Angesichts der zahlreichen Vorschriften, die inzwischen in Bezug auf die Sicherheit von Kindern im Internet gelten (Gesetz über digitale Dienste, DSGVO, Verordnung über Künstliche Intelligenz usw.), sollten die Aufsichtsbehörden aus unterschiedlichen Rechtsfeldern intensiver zusammenarbeiten und Informationen austauschen. So können Unstimmigkeiten vermieden und kohärente, verlässliche und wirksame rechtliche Rahmenbedingungen gewährleistet werden, deren Fundament der Schutz der Grundrechte bildet.

Die Europäische Kommission sollte prüfen, durch welche Mechanismen eine nahtlose Zusammenarbeit zwischen den Aufsichtsbehörden ermöglicht werden kann, damit bestehende Strukturen für die Rechtsdurchsetzung genutzt werden können. Darüber hinaus muss beurteilt werden, ob die für die Durchsetzung und Evaluierung zuständigen Regulierungsbehörden zusätzliche Ressourcen oder Umstrukturierungen benötigen. Es sollten Maßnahmen in Betracht gezogen werden, durch die die Zivilgesellschaft eine wichtigere Rolle bei der Durchsetzung einnehmen und einen größeren Beitrag zur Erweiterung der Durchsetzungskapazitäten leisten kann, wobei dies auch innerhalb bestehender Strukturen erfolgen kann. Die Durchsetzungsmechanismen sollten ergänzend ineinandergreifen und Überschneidungen sollten vermieden werden.

EMPFEHLUNG 6

Rasch Maßnahmen ergreifen, um sicherzustellen, dass für Anbieter sozialer Medien und anderer digitaler Dienste klare Verpflichtungen gelten, sexuellen Missbrauch von Kindern im Internet, auch im Rahmen interpersoneller Kommunikation, zu verhindern, aufzudecken, zu melden und zu sperren

Die Lücke im Bereich der Sicherheit von Kindern, die sich infolge des Auslaufens der Übergangsverordnung zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern aufgetan hat, muss rasch geschlossen werden. Der EU-Gesetzgeber sollte die vorgeschlagene langfristige Verordnung für die Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern rasch beschließen. Mehr als 80 % der Ermittlungen im Zusammenhang mit sexuellem Missbrauch von Kindern gehen auf Meldungen von Anbietern sozialer Medien und anderer digitaler Dienste zurück. Kinder haben oft zu große Angst, um Missbrauch zu melden. Die Aufdeckung von Material über sexuellen Missbrauch von Kindern, einschließlich im Rahmen interpersoneller Kommunikation ausgetauschten Materials, ist häufig die einzige Möglichkeit, den Missbrauch zu stoppen.

Zusammen mit der Neufassung der Richtlinie zur Bekämpfung des sexuellen Missbrauchs von Kindern, auf die sich die beiden gesetzgebenden Organe kürzlich einigten, werden diese Instrumente den EU-Rahmen gegen sexuellen Missbrauch und sexuelle Ausbeutung von Kindern sowohl online als auch offline stärken. Sie werden die Prävention und Ermittlung sowie die Unterstützung der Opfer verbessern. Darüber hinaus sollten Online-Plattformen die brancheninterne Zusammenarbeit bei schweren Online-Straftaten, die Kinder betreffen, stärken, indem sie Signale über schädliche Inhalte und böswillige Akteure austauschen. Anbieter sozialer Medien und anderer digitaler Dienste sollten die Zusammenarbeit mit dem EU-Internetforum verstärken, um Informationen über neu auftretende Bedrohungen und Missbrauchsmuster auszutauschen. Dies wird die frühzeitige Aufdeckung und Meldung mutmaßlicher Straftaten unterstützen. Darüber hinaus ist eine verstärkte Durchsetzung von Rechtsrahmen zum Schutz von Kindern wie der Opferschutzrichtlinie oder der Richtlinie zur Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt erforderlich.

EMPFEHLUNG 7**Mitgliedstaaten können zusätzliche vorsorgliche Zugangsbeschränkungen für soziale Medien und andere digitale Dienste für Kinder ab 13 Jahren einführen**

Zusätzliche vorsorgliche Zugangsbeschränkungen sollten als Ergänzung zu der EU-weit gültigen Zugangsbeschränkung für soziale Medien und andere digitale Dienste für unter 13-Jährige dienen. Jugendliche dürfen nur Zugang zu sozialen Medien+ haben, die in Bezug auf Inhalte und Gestaltung sicher und altersgerecht sind und bei deren Gestaltung ihre Rechte und Bedürfnisse berücksichtigt wurden. Die Situation hat sich in den Mitgliedstaaten von Land zu Land unterschiedlich entwickelt, und manche Mitgliedstaaten ziehen vielleicht eine Altersgrenze von mehr als 13 Jahren in Betracht. Alle auf nationaler Ebene erlassenen zusätzlichen vorsorglichen Zugangsbeschränkungen sollten laufend evaluiert und gegebenenfalls neu bewertet werden, sobald soziale Medien und andere digitale Dienste für Kinder und Jugendliche durch Voreinstellungen sicher gemacht wurden.

EMPFEHLUNG 8**Verbraucherschutzpolitik zum Schutz Minderjähriger im Internet nachschärfen**

Das Verbraucherschutzrecht spielt eine wichtige Rolle als Instrument zum Schutz von Kindern, das alle Arten von Unternehmern – Online-Shops für den elektronischen Geschäftsverkehr, Streaming auf Abonnementbasis sowie digitale Inhalte und Dienste, Videospiele und Apps – abdeckt und sicherstellt, dass kein Unternehmer, der mit Kindern interagiert, aus dem Anwendungsbereich durchsetzbarer Verbraucherschutzverpflichtungen herausfällt. Der Schutz von Kindern vor irreführenden, aggressiven und schädlichen Online-Marketingpraktiken, auch durch Online-Influencer, sollte gestärkt werden.

Das Sicherheitsnetz und die Vorschriften für seine Durchsetzung sollten gestärkt werden, um sicherzustellen, dass jedes Kind, das mit einem kommerziellen digitalen Dienst in der Europäischen Union interagiert, unabhängig von der Art des Dienstes, der Art des Unternehmers oder dem Mitgliedstaat, in dem der Unternehmer niedergelassen ist, in den Genuss eines grundlegenden Verbraucherschutzniveaus kommt.

Das bevorstehende Gesetz über digitale Fairness und die Überarbeitung der Verordnung über die Zusammenarbeit im Verbraucherschutz (CPC-Verordnung) bieten eine wichtige Gelegenheit, den Schutz von Kindern und Jugendlichen zum Herzstück des EU-Verbraucherrechts zu machen.

EMPFEHLUNG 9**Auswirkungen der umgesetzten Maßnahmen laufend beobachten und bewerten**

Alle neuen Instrumente, die im Anschluss an die Empfehlungen dieses Kapitels vorgeschlagen werden, sollten datengesteuerte Mechanismen und Ansätze zur kontinuierlichen Bewertung ihrer Auswirkungen und Wirksamkeit umfassen. Die Kommission sollte auch die Koordinierung der Durchsetzungsanstrengungen und die Straffung der Bewertungs- und Überwachungsverfahren, insbesondere in Bezug auf die Sicherheit von Kindern im Internet, verbessern.

Aufbauend auf dem Modell, das zur Verfolgung der Umsetzung des australischen Gesetzes über soziale Medien (einschließlich der kontinuierlichen Integration von Wissen und Erkenntnissen Sachverständiger) angewendet wird, sollte die Einführung einer EU-weiten Zugangsbeschränkung mit einer umfassenden Bewertung einhergehen. Der Schwerpunkt sollte dabei auf der Wirksamkeit, den Auswirkungen und den Anpassungen der Mindestaltersregelung liegen, wobei der Beteiligung von Kindern Vorrang eingeräumt werden sollte. Dies könnte durch die Nutzung bestehender Mechanismen wie der EU-Plattform für die Beteiligung von Kindern und des Programms „Better Internet for Kids“ (BIK+) sowie durch die Bündelung der Forschung zu diesem Thema in der gesamten EU und in verschiedenen Forschungsbereichen, auch in den Strukturforschungsprogrammen, erreicht werden.

Diese Bewertungen können sich auf laufende Arbeiten im Rahmen des Gesetzes über digitale Dienste und des Europäischen Zentrums für die Transparenz der Algorithmen (ECAT) stützen. Das Zentrum beobachtet kontinuierlich, wie sich die Lage im Bereich der Sicherheit von Kindern im Internet hinsichtlich neuer Trends, Möglichkeiten und des Einsatzes neuer und aufkommender Technologien entwickelt. Dies kann die Grundlage für die Einrichtung eines Systems zur strukturierten und regelmäßigen Datenerhebung aus repräsentativen Stichproben von Minderjährigen einschlägiger Altersgruppen in der gesamten EU bilden.

Der Schwerpunkt der Bewertung liegt auf dem Wohlergehen von Minderjährigen. Evaluierungsrahmen sollten Entwicklungsergebnisse, Indikatoren für psychische Gesundheit, Maßnahmen für das Wohlbefinden sowie Resilienzergebnisse umfassen, anstatt ausschließlich Parameter der Rechtskonformität, der Exposition oder der Nutzung in den Mittelpunkt zu stellen. Maßnahmen im Bereich der Sicherheit von Kindern sollten letztlich im Hinblick auf ihren Beitrag zu einer gesunden Entwicklung bewertet werden.

EMPFEHLUNG 10

Bei der Verarbeitung von Daten von Kindern im Rahmen der DSGVO durch Anbieter sozialer Medien und anderer digitaler Dienste sollte das Wohl der Kinder an erster Stelle stehen

Wenn soziale Medien und andere digitale Dienste als Verantwortliche oder Auftragsverarbeiter personenbezogene Daten von Kindern verarbeiten, sollten sie sicherstellen, dass sie sich auf die nach der DSGVO am besten geeignete Rechtsgrundlage stützen. Die Datenschutzbehörden prüfen, ob die für die Verarbeitung Verantwortlichen die Daten von Kindern im Rahmen einer geeigneten Rechtsgrundlage verarbeiten und ob die einschlägigen Bedingungen erfüllt sind.

Entscheidet sich ein Verantwortlicher dafür, die personenbezogenen Daten eines Kindes auf der Grundlage einer Einwilligung zu verarbeiten, so sollte er sicherstellen, dass er die gültige Einwilligung des Kindes und erforderlichenfalls die Zustimmung des Trägers der elterlichen Verantwortung eingeholt hat.

Wenn ein Verantwortlicher entscheidet, sich auf ein berechtigtes Interesse als Rechtsgrundlage für die Verarbeitung personenbezogener Daten von Kindern zu berufen, sollte er sicherstellen, dass alle Anforderungen des Artikels 6 Absatz 1 Buchstabe f erfüllt sind, bevor er die Verarbeitung durchführt. Eine dieser Anforderungen besteht darin, dass die berechtigten Interessen der für die Verarbeitung Verantwortlichen nicht durch die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person außer Kraft gesetzt werden. In diesem Zusammenhang ist besondere Sorgfalt erforderlich, wenn es sich bei der betroffenen Person um ein Kind handelt.

Wie in den Leitlinien des Europäischen Datenschutzausschusses (EDSA) zum berechtigten Interesse dargelegt wird, sollten die Verantwortlichen bei der Durchführung dieser Bewertung das Ausmaß und die Intensität eines Eingriffs in die Rechte und Freiheiten des Kindes berücksichtigen. Sie sollten auch die berechtigten Erwartungen eines Kindes hinsichtlich der Verwendung seiner personenbezogenen Daten berücksichtigen. Darüber hinaus sollten sie nachweisen, dass das Wohl des Kindes als vorrangige Erwägung berücksichtigt wurde und dass geeignete Schutzmechanismen bestehen. Bei der Abwägung der widerstreitenden Interessen sollte das Wohl des Kindes eine vorrangige Erwägung sein.

Kollidieren die berechtigten Interessen eines Verantwortlichen mit den Interessen oder Grundrechten und Grundfreiheiten eines Kindes, so sollten im Allgemeinen die Interessen und Rechte des Kindes Vorrang haben. Kann dies nicht sichergestellt werden, sollte der Verantwortliche entweder eine besser geeignete Rechtsgrundlage finden oder die personenbezogenen Daten des Kindes nicht verarbeiten.

EMPFEHLUNG 11

Die wirksame Umsetzung der Produkthaftungsrichtlinie sicherstellen

Die ursprünglich 1985 angenommene Richtlinie wurde während der letzten Amtszeit der Europäischen Kommission aktualisiert, um wichtigen Entwicklungen auf dem Gebiet der Technologie, der Wirtschaft und der Rechtsprechung Rechnung zu tragen. Dabei wurde das Ziel verfolgt, gleiche und faire Wettbewerbsbedingungen zu gewährleisten, Rechtssicherheit für Unternehmen zu schaffen und zugleich einen wirksamen Rechtsschutz für Opfer zu gewährleisten. Die Richtlinie trat am 8. Dezember 2024 in Kraft und muss von den Mitgliedstaaten bis zum 9. Dezember 2026 umgesetzt werden.

Angesichts der weltweit zunehmenden Produkthaftungsverfahren gegen digitale Dienstleister ist es von entscheidender Bedeutung, die wirksame und rechtzeitige Umsetzung und Durchführung der Produkthaftungsrichtlinie sicherzustellen. Darüber hinaus sollten die Regulierungsbehörden die Bürger wirksam über die Rechte informieren, die sich aus der Produkthaftungsrichtlinie ergeben (z. B. durch die Förderung aktualisierter Rechtsbehelfsmechanismen für natürliche Personen, die Klage wegen der Verwendung eines fehlerhaften Produkts, insbesondere Software, erheben wollen).

04

Minderjährige befähigen, sich sicher in der digitalen Welt zu bewegen

Im vorangegangenen Kapitel wurden die bestehenden Rechtsvorschriften und Instrumente beleuchtet, die der EU und den Mitgliedstaaten zum Online-Schutz von Kindern zur Verfügung stehen; außerdem wurden die Ergebnisse der laufenden Durchsetzung vorgestellt und Bereiche ermittelt, in denen die Rechtsvorschriften und Instrumente gestärkt und ergänzt werden müssen, um die Sicherheit von Kindern im Internet zu verbessern.

Die Welt der sozialen Medien+ lässt sich jedoch nicht allein auf Risiken reduzieren. Sie ist auch ein Raum der Chancen, der Kreativität und der Teilhabe. In diesem Kapitel werden die – wenn auch vergleichsweise begrenzten – Belege für die Möglichkeiten untersucht, die die Nutzung sozialer Medien und anderer digitaler Dienste durch Minderjährige bietet. Dabei werden Beiträge einer Jugendvertreterin, Marta Gonçalves, berücksichtigt, die an den Sitzungen des Sonderausschusses und an Diskussionen teilnahm, an deren Ende die Formulierung der Empfehlungen durch die Ko-Vorsitzenden stand.

In diesem Kapitel werden anschließend ausgewählte EU-Strategien und -Instrumente zur Förderung der Befähigung und Teilhabe von Minderjährigen im Internet thematisiert. Es schließt mit einer Reihe von Empfehlungen, wie Kinder und ihr unterstützendes Umfeld (Eltern und Betreuungspersonen, Lehrkräfte und andere pädagogische Fachkräfte) Hilfestellung bei der Nutzung der Chancen der Online-Welt leisten können.

Dieses Kapitel beruht auf den Säulen 5 und 6 der „Sechs Leitprinzipien“, die von den Ko-Vorsitzenden vorgelegt wurden, um die Bemühungen zur Stärkung der Sicherheit von Kindern im Internet zu steuern: Stärkung der Handlungskompetenz und Medienerziehung sowie Rechte und Teilhabe von Kindern. Ausgangspunkt dieser Analyse sind die jeweiligen Rahmen für die Rechte des Kindes auf internationaler und EU-weiter Ebene^a.

Um wirksam zu sein, müssen Maßnahmen zur Sicherheit von Kindern im Internet mit Maßnahmen zur Stärkung der Handlungskompetenz und Förderung der Teilhabe von Minderjährigen einhergehen. Die Maßnahmen müssen altersgerecht sein, den sich entwickelnden Fähigkeiten von Kindern und Jugendlichen Rechnung tragen und auf die sich verändernden Rollen von Betreuungspersonen und pädagogischen Fachkräften auf dem Weg Minderjähriger ins Erwachsenenalter zugeschnitten sein.

a. Insbesondere das Übereinkommen der Vereinten Nationen über die Rechte des Kindes und die Allgemeinen Bemerkungen des Ausschusses für die Rechte des Kindes, die Charta der Grundrechte der Europäischen Union und die EU-Kinderrechtsstrategie.

Von den Risiken abgesehen sollte anerkannt werden, dass die digitale Welt Kindern und Jugendlichen auch viele Chancen bietet. Wenn Minderjährige befähigt werden, sich sicher online zu bewegen, und mit soliden digitalen Kompetenzen ausgestattet sind, kann die Nutzung sozialer Medien und anderer digitaler Dienste dem Wohlbefinden und der sozialen Vernetzung zugutekommen, einen unterstützenden Kontakt zu Netzen Gleichaltriger ermöglichen und Chancen für Selbstentfaltung, gesellschaftliches Engagement und unabhängiges Lernen bieten.

Im nächsten Abschnitt werden die potenziellen Möglichkeiten im Zusammenhang mit der Nutzung sozialer Medien+ durch Kinder und Jugendliche untersucht. Zunächst aber kommt in diesem Kapitel eine Jugendvertreterin zu Wort.

Gestaltung einer besseren digitalen Welt

EIN AUFRUF ZUM HANDELN VON MARTA GONÇALVES,

PORTUGIESISCHE BOTSCHAFTERIN FÜR BETTER INTERNET FOR KIDS+

Ich bin in einer Welt aufgewachsen, in der das Internet fest zum Alltag gehörte. Für meine Generation ist das Onlinesein keine Aktivität, die man nur gelegentlich ausübt. Der digitale Raum ist der Ort, an dem wir lernen, gestalten, kommunizieren, Freundschaften aufbauen, Chancen entdecken und unsere Identität entwickeln. Deshalb geht es bei der Befähigung von Kindern und jungen Menschen zur sicheren Nutzung von sozialen Medien und anderen digitalen Technologien nicht nur darum, sie vor Schaden zu schützen. Es geht auch darum, sie in die Lage zu versetzen, uneingeschränkt an der Welt teilzuhaben, in der sie aufwachsen.

Allzu oft werden Diskussionen über das digitale Leben von Kindern ohne die Kinder selbst geführt. Regierungen, Unternehmen, pädagogische Fachkräfte und Erwachsene treffen Entscheidungen im Namen junger Menschen, fragen aber selten die am stärksten Betroffenen danach, was sie tatsächlich brauchen. Dies ist nicht nur unfair, das ist kontraproduktiv. Wir können kein besseres digitales Umfeld schaffen, indem wir Vermutungen über die Erfahrungen der Kinder anstellen.

Durch meine eigene Arbeit in den Bereichen Peer-Beratung und Jugendvertretung habe ich das unglaubliche Potenzial junger Menschen beobachtet, das sie entfalten, wenn man ihnen vertraut und Verantwortung überträgt. Kinder und Jugendliche können durch ihre Kreativität, Empathie, Entschlossenheit und Bereitschaft, einander zu helfen, bemerkenswerte Dinge erreichen. Wenn junge Menschen zusammenkommen, konsumieren sie nicht einfach nur Technologie. Sie nutzen sie, um zu lernen, Dinge zu gestalten, Probleme zu lösen und Gemeinschaften aufzubauen. Sie werden in einer Weise zu Vorbildern für ihre Altersgenossen, wie es Erwachsene nicht können.

Junge Menschen sind Expertinnen und Experten für ihre eigenen Lebensumstände. Sie kennen die Chancen, die sie schätzen, die Herausforderungen, mit denen sie konfrontiert sind, und die Lösungen, die wirklich etwas bewirken würden. Eine sinnvolle Teilhabe junger Menschen sollte nicht als symbolische Übung behandelt, sondern als wesentlicher Bestandteil der Gestaltung digitaler Strategien, Plattformen und Dienste, die wirklich funktionieren, anerkannt werden.

Das Verfahren des Sonderausschusses bot ein eindrucksvolles Beispiel dafür, wie eine sinnvolle Beteiligung junger Menschen aussehen kann. Während der drei Sitzungen wurden die Vertreterinnen und Vertreter von Kindern und jungen Menschen umfassend in die Diskussionen einbezogen, wobei sie sich zusammen mit anderen Sachverständigen beteiligten, ihre Sichtweisen einbrachten und die anderen an den Anliegen, die für sie am wichtigsten waren, teilhaben ließen.

Darüber hinaus hatte ich auch die Möglichkeit, an der Ausarbeitung des eigentlichen Berichts mitzuwirken, Abschnitte zu verfassen und während der gesamten Ausarbeitung der Empfehlungen Beiträge zu leisten. Wie in diesem Kapitel zum Ausdruck kommt (siehe beispielsweise den Abschnitt über Peer-Beratung), wurde ich nicht nur konsultiert, sondern sinnvoll in den Prozess integriert und ich leistete mit meinem Wissen und meiner Erfahrung einen Beitrag. Das Mitwirken an den Diskussionen, in denen Entscheidungen gestaltet und Argumente ausgetauscht wurden, unterschiedliche Standpunkte angehört und neue Erkenntnisse gewonnen wurden, hat deutlich gemacht, wie wichtig es ist, junge Menschen während des gesamten Prozesses einzubeziehen und ihre Lebenserfahrungen als Fachwissen anzuerkennen.

Obwohl das Hauptaugenmerk des Sonderausschusses auf der Entwicklung eines Konzepts für die Gewährleistung der Sicherheit von Kindern im Internet lag, war ich in gleichem Maße entschlossen, einen Beitrag dazu zu leisten, die Chancen, die von der digitalen Welt geboten werden, hervorzuheben.

Die Online-Welt hat Türen geöffnet, die sich frühere Generationen kaum vorstellen konnten. Sie ermöglicht Kindern, neue Sprachen zu erlernen, Musikinstrumente zu spielen, wissenschaftliche Themen zu entdecken, künstlerische Fähigkeiten zu entwickeln, neue Kulturen zu erkunden und unabhängig davon, wo auf der Welt sie leben, mit Menschen in Kontakt zu treten, die ihre Leidenschaften teilen. Für viele junge Menschen, insbesondere diejenigen, die sich in ihren Gemeinschaften vor Ort isoliert fühlen, werden digitale Räume zu Orten, an denen sie Zugehörigkeit, Inspiration und Vertrauen finden. Das Internet kann Chancen schaffen, die das Leben prägen, aber nur, wenn Kinder das Wissen und die Unterstützung erhalten, um sich darin sicher zurechtzufinden.

Die Erfahrung hat mich auch gelehrt, dass informierte Kinder selbstbestimmte Kinder sind. Wenn junge Menschen verstehen, wie digitale Plattformen funktionieren, wie sie ihre Privatsphäre schützen und wie sie Manipulation, Fehlinformationen oder schädliches Verhalten feststellen, werden sie selbstsicherer, wenn es darum geht, zu erkennen, wenn etwas nicht stimmt. Sie sind besser gerüstet, sich Hilfe zu suchen, Freundinnen und Freunde zu unterstützen und zu sichereren Online-Gemeinschaften beizutragen. Bei der digitalen Kompetenz geht es nicht darum, Kindern zu vermitteln, dass sie Technologien fürchten sollen. Es geht darum, ihnen das Vertrauen und das Wissen für ihre kritische, verantwortungsvolle und positive Nutzung zu vermitteln.

Wissen ist eines der wirkungsvollsten Instrumente, die wir einem Kind an die Hand geben können. Informationen ermöglichen fundierte Entscheidungen, stärken die Resilienz und schaffen Unabhängigkeit. Jedes Kind verdient Zugang zu klarer, altersgerechter Anleitung, die ihm hilft, sowohl die Chancen als auch die Risiken der digitalen Welt zu verstehen. Je mehr wir in Bildung, Teilhabe und digitale Kompetenz investieren, desto mehr befähigen wir junge Menschen, sich selbst und andere online zu schützen.

Die Zukunft der digitalen Welt wird von den Kindern von heute gestaltet. Sie sind nicht einfach nur künftige Bürgerinnen und Bürger, sondern bereits jetzt aktive Teilnehmerinnen und Teilnehmer, deren Stimmen, Ideen und Erfahrungen von Bedeutung sind. Wenn wir sie heute stärken, werden sie sich nicht nur in der digitalen Welt bewegen. Sie werden sie neu definieren, und zwar zum Besseren.



Marta Gonçalves

*Botschafterin für Better Internet
for Kids+, Portugal*

Marta Gonçalves

Chancen für Minderjährige in der digitalen Welt

VERBINDUNG UND SELBSTENTFALTUNG

In Kapitel 2 wurde bereits darauf hingewiesen, dass viele Kinder und Jugendliche soziale Medien+ nutzen, um online Kontakte zu knüpfen, miteinander zu interagieren und ihre Interessen mit anderen zu teilen, wobei Belege diese Erkenntnisse unterstreichen²⁹⁰.

Soziale Medien+ können Jugendliche ferner in die Lage versetzen, ihre Interessen online mit Gleichaltrigen zu teilen, offline gefundene Freundschaften zu pflegen und mit engen Freunden und Familienmitgliedern, die weit entfernt leben, in Kontakt zu bleiben²⁹¹.

Ganz allgemein kann die Nutzung sozialer Medien und anderer digitaler Dienste es Jugendlichen ermöglichen, Unterhaltungsangebote gemeinsam zu nutzen und über gemeinsame Online-Erfahrungen nachzudenken, wobei Forschungsarbeiten auf potenzielle Vorteile für die Stimmung und das Wohlbefinden von Jugendlichen hindeuten²⁹².

Soziale Medien+ können Jugendlichen auch Räume bieten, in denen sie sich äußern und ihre Identität erkunden können²⁹³. Untersuchungen deuten darauf hin, dass Online-Räume Umgebungen für die selektive Selbstoffenlegung bieten können, die als mit geringerem Einsatz (lower stakes) verbunden wahrgenommen werden²⁹⁴. Darüber hinaus nutzen einige Minderjährige private soziale Konten möglicherweise in ähnlicher Weise wie Offline-Tagebücher²⁹⁵.

Jugendliche nutzen soziale Medien+ zunehmend auch als kreatives Medium. Eine Umfrage aus dem Jahr 2022 unter 1 316 Jugendlichen in den USA ergab, dass 71 % die sozialen Medien als Raum betrachten, in dem sie ihre Kreativität zum Ausdruck bringen können²⁹⁶. Allerdings können solche Nutzungen Jugendliche Gefahren aussetzen.

Kurz gesagt: Die potenziellen Vorteile der Nutzung sozialer Medien und anderer digitaler Dienste durch Minderjährige zur Kontaktaufnahme und Selbstentfaltung müssen von den unterstützenden Bezugspersonen gegen die Risiken für die

„Es besteht dringender Bedarf an einem autonomen Ansatz für junge Menschen. Kinder werden von allen Seiten durch ängstliche Eltern eingeschränkt und die sozialen Medien bieten eine Möglichkeit, dem zu entfliehen. Junge Menschen müssen in Entscheidungen und Diskussionen über Online-Räume einbezogen werden, denn nur dann werden sie sich an die Vorschriften halten und durch Resilienz gestärkt werden, sodass sie wichtige Fähigkeiten zur kritischen Auseinandersetzung und zur Selbstorganisation für die unvorhersehbare digitale Zukunft entwickeln.“

— ZUZANNA,

17-JÄHRIGE VERTRETERIN DER EU-PLATTFORM FÜR DIE BETEILIGUNG VON KINDERN

Sicherheit, Gesundheit und das Wohlbefinden von Kindern und Jugendlichen abgewogen werden. Hierzu zählen Risiken des unerwünschten Kontakts und der Konfrontation mit nicht altersgerechten Online-Inhalten, insbesondere Grooming und sexueller Missbrauch von Kindern.

Ein offener Austausch mit Minderjährigen über ihre Erfahrungen im Internet ist entscheidend, um Kindern und Jugendlichen das Gefühl zu vermitteln, dass sie sich an ihre Eltern oder Bezugspersonen wenden können, insbesondere wenn es um unerwünschte Kontakte oder Erfahrungen geht. Darüber hinaus müssen Betreuungspersonen und pädagogische Fachkräfte in der Lage sein, die Nutzung sozialer Medien+ durch Minderjährige zu überwachen (und erforderlichenfalls einzuschränken), und wissen, an wen sie sich wenden können, um bei Bedarf professionelle Hilfe zu erhalten.

UNTERSTÜTZUNG UND INFORMATIONEN

Viele Jugendliche nutzen soziale Medien und andere digitale Dienste, um Unterstützung bei Problemen zu suchen, mit denen sie online konfrontiert sind. Einigen Forschungsergebnissen zufolge können Jugendliche über soziale Medien+ offene Gespräche führen und online Hilfe finden²⁹⁷.

Eine unter Minderjährigen häufig geäußerte Ansicht ist, dass Online-Räume „sichere“ Alternativen für die Selbstentfaltung oder leichter zugängliche Quellen der Unterstützung bieten als „traditionelle“ Möglichkeiten, darunter Gespräche mit Eltern oder Vertrauenspersonen²⁹⁸.

Wie in Kapitel 2 dargelegt, kann es Jugendlichen mit gutem Selbstwertgefühl und Freundschaften im realen Leben gelingen, ihre Beziehungen im realen Leben zu stärken und online Unterstützung zu finden. Für Jugendliche mit geringerem Selbstwertgefühl und schwächeren sozialen Netzwerken im realen Leben können soziale Medien+ jedoch dazu führen, dass sie vermehrt unerwünschten Kontakten und dem Alter nicht angemessenen Inhalten ausgesetzt sind.

Schutzbedürftige Minderjährige, darunter auch solche, die der LGBTIQ+-Gemeinschaft angehören, sonderpädagogischen Förderbedarf haben, unter psychischen Problemen oder Essstörungen leiden oder sich selbst verletzen, neigen möglicherweise besonders dazu, soziale Medien und andere digitale Dienste zu nutzen, um mit anderen in Kontakt zu treten, die ähnliche Erfahrungen machen, oder um Unterstützung zu suchen.

Begrenzte Forschungsarbeiten deuten darauf hin, dass einige Jugendliche in Bezug auf Probleme, mit denen sie konfrontiert sind, nicht nur aufgrund direkter Online-Interaktionen, sondern auch aufgrund des Wissens, dass andere ähnliche Erfahrungen machen, Trost finden können²⁹⁹.

Wenn Minderjährige jedoch soziale Medien+ nutzen, um Unterstützung zu suchen, können Personen, die ohnehin schon schutzbedürftig sind, Gefahren wie Cybermobbing und sozialer Ausgrenzung ausgesetzt sein, die sich negativ auf ihre Gesundheit und ihr Wohlbefinden auswirken können.

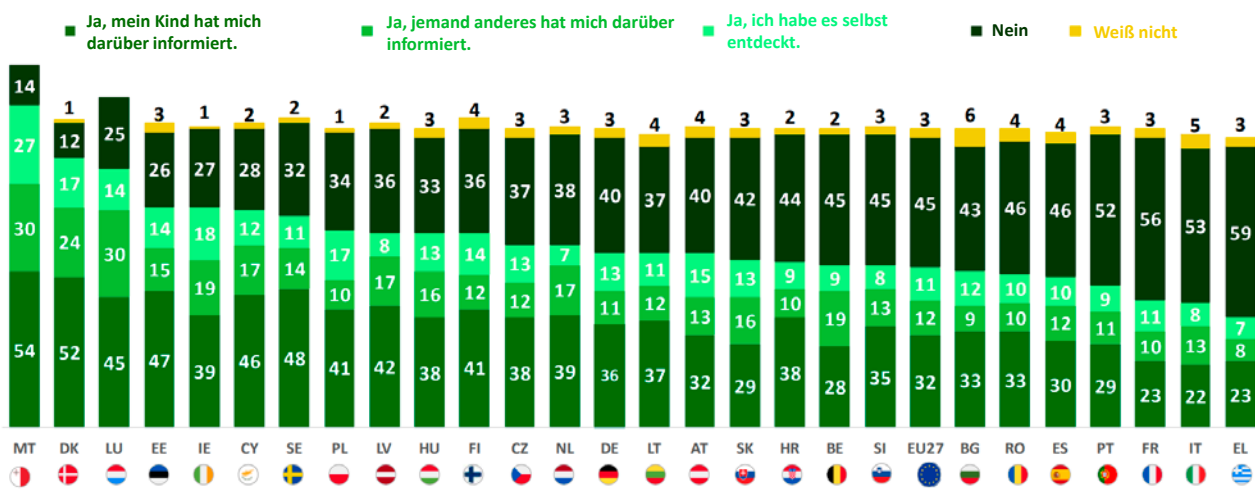
Sofern geeignete Schutzmaßnahmen getroffen werden, können Räume in den sozialen Medien+ Minderjährigen möglicherweise Unterstützung bieten. Geführte Online-Diskussionsforen, die beispielsweise von medizinischem Fachpersonal moderiert werden, könnten für Menschen, die Hilfe oder Informationen auf Social-Media-Plattformen suchen, eine Alternative darstellen.

Einiges deutet darauf hin, dass der Umgang mit dieser Art von Forum Jugendlichen dabei helfen kann, ihre Zurückhaltung bei der Inanspruchnahme professioneller Hilfe in „traditionellen“ Formen zu überwinden³⁰⁰. Dies kann auch dazu beitragen, Probleme im Zusammenhang mit der Verbreitung von Desinformation und Fehlinformationen im Internet, z. B. in Bezug auf medizinische Fragen, anzugehen.

Betreuungspersonen, pädagogische Fachkräfte und öffentliche Dienste (einschließlich Anbieter von Dienstleistungen im Bereich der psychischen und der sexuellen Gesundheit) sollten darüber nachdenken, wie sie Minderjährige am besten aufklären und dabei unterstützen können, soziale Medien und andere digitale Dienste als Informations- oder Unterstützungsquelle sicher zu nutzen.

Abbildung 1: Sensibilisierung der Familie für negative Online-Erfahrungen Minderjähriger

Frage: Ist Ihr Kind schon einmal zu Ihnen gekommen oder haben Sie schon einmal festgestellt, dass Ihr Kind im Internet eine negative Erfahrung gemacht hat?



(*) Der Gesamtwert übersteigt 100 %, da die Befragten mehrere Antworten geben konnten.

Quelle: Europäische Kommission (2026). Auswirkungen übermäßiger Bildschirmzeit und sozialer Medien auf die psychische Gesundheit junger Menschen – Juni 2026 – Eurobarometer-Umfrage.

LERNEN UND KOMPETENZENTWICKLUNG

Studien über den Einsatz digitaler Instrumente für das Lernen deuten darauf hin, dass der Einsatz digitaler Instrumente und Dienste in geringfügigem bis moderatem Umfang positive Auswirkungen auf die Lernergebnisse von Kindern in der Sekundarstufe haben können³⁰¹.

Digitale Technologien bieten Lehrkräften und Schülern zusätzliche Lehr- und Lernmöglichkeiten und scheinen dann am wirksamsten zu sein, wenn sie zur Ergänzung des herkömmlichen Unterrichts eingesetzt werden, anstatt ihn zu ersetzen³⁰².

In Fächern wie Naturwissenschaften, Mathematik und Sprachen können digitale Technologien das Lernen durch interaktive Erfahrungen bereichern. Dies schließt Simulationen, Modellierungen, Videos, digitale Spiele, Multimedia-Ressourcen und Toneffekte ein. Diese Ansätze können die aktive Mitwirkung der Schülerinnen und Schüler erhöhen und dazu beitragen, abstrakte oder komplexe Konzepte leichter zugänglich und einfacher verständlich zu machen³⁰³.

Digitale Instrumente und Dienste können auch personalisiertes Lernen unterstützen. Indem sie den Schülerinnen und Schülern ermöglichen, in ihrem eigenen Tempo voranzugehen und Themen aus verschiedenen Blickwinkeln zu erkunden, sorgen sie für mehr Flexibilität im Lernprozess. Dies kann die Motivation steigern, insbesondere bei Schülerinnen und Schülern, die besser durch wiederholtes Üben oder eigenständiges Forschen lernen³⁰⁴.

KI-basierte Technologien stellen ein zusätzliches Instrument dar, das den individualisierten Unterricht unterstützen kann. Diese Instrumente bieten Lehrkräften die Möglichkeit, ihre Unterrichtsmethoden an die schulischen Leistungen anzupassen, zeitnahes Feedback zu geben und entsprechende Anpassungen vorzunehmen sowie die individuelle Förderung entsprechend zu gestalten³⁰⁵.

Untersuchungen zeigen, dass der Einsatz generativer KI in den Lernalltag vielfach fest integriert ist³⁰⁶. Die Schülerinnen und Schüler erkennen zwar die Risiken für ihr Lernen und ihre kognitive Entwicklung an, konzentrieren sich jedoch tendenziell auf die potenziellen Möglichkeiten³⁰⁷, beispielsweise auf die Zeitersparnis durch den Einsatz eines KI-Instruments.

Durch den Einsatz von Lernplattformen in Schulen können Grund- und Sekundarschülerinnen und -schüler Zugang zu einer größeren Vielfalt an hochwertigen Lernressourcen erhalten, was selbstständiges Lernen sowie die Möglichkeit zur Selbstüberprüfung und zur gegenseitigen Überprüfung durch Mitschüler ermöglicht³⁰⁸.

Diese Chancen müssen gegen Risiken wie das Potenzial digitaler Geräte, Kinder und Jugendliche vom Lernen abzuhalten, physische Risiken (z. B. in Bezug auf das Sehvermögen von Minderjährigen) und die „Überdigitalisierung“ der Bildung abgewogen werden.

Wie in Kapitel 2 erörtert, müssen die Auswirkungen von KI-Tools auf die Bildung und Kompetenzentwicklung von Kindern und Jugendlichen eingehender analysiert werden, um potenzielle Vorteile und Risiken verstehen zu können. Ebenso sind weitere Belege für die potenziellen positiven Auswirkungen der Nutzung sozialer Medien+ in Bildungseinrichtungen erforderlich.

Digitale Bildung, einschließlich Medienkompetenz und KI-Kompetenz, ist von entscheidender Bedeutung für die Befähigung von Kindern und Jugendlichen, sich sicher online zurechtzufinden. Die wichtigste Frage ist, wie der Erwerb digitaler Fähigkeiten und Kompetenzen praktisch in die Lehrpläne integriert werden kann, und zwar in einer Weise, die dem allgemeinen Lernen und der allgemeinen Entwicklung von Minderjährigen förderlich ist.

„Junge Menschen brauchen klare Rechte, verständliche Informationen, wirksame Meldeinstrumente und eine echte Stimme bei der Gestaltung der digitalen Räume, die sie täglich nutzen. Das Internet ist nicht nur ein Ort der Gefahr. Für viele junge Menschen ist es auch ein Ort des Lernens, der Verbundenheit, der Kreativität und der Unterstützung. Statt es zu verbieten oder einzuschränken, machen Sie es lieber zu einem Ort der Inspiration, der für alle sicher ist. Deshalb ist meine Botschaft einfach: Gestaltet das Internet mit uns, nicht einfach nur für uns.“

— AYATA,

15-JÄHRIGE VERTRETERIN DER EU-PLATTFORM
FÜR DIE BETEILIGUNG VON KINDERN

Die Kulturen und Einstellungen in Bezug auf die Nutzung digitaler Geräte und Tools in Lernumgebungen sind auf nationaler Ebene in der EU durch große Unterschiede geprägt. Es wird jedoch allgemein anerkannt, dass es wichtig ist, die Kompetenzen von Minderjährigen, Betreuungspersonen und pädagogischen Fachkräften zu verbessern, sichere, altersgerechte Lerninstrumente bereitzustellen und das Konzept des digitalen Wohlbefindens in den Schulen durchgängig zu berücksichtigen.

SMARTPHONE-BESCHRÄNKUNGEN IN SCHULEN

In ganz Europa sind Mobiltelefone im Leben von Kindern und Jugendlichen inzwischen allgegenwärtig. Wie in Kapitel 1 dargelegt, können Minderjährige durch die Nutzung von Smartphones in der Schule vom Lernen abgelenkt werden, was ihre schulischen Leistungen beeinträchtigen, soziale Interaktionen einschränken und gleichzeitig das Risiko von Schäden wie Cybermobbing und sozialer Ausgrenzung erhöhen kann.

Bei Jugendlichen kann die Nutzung von Smartphones das Risiko psychischer Probleme einschließlich Angstzuständen und Depressionen steigern. Ganz allgemein kann die Nutzung von Smartphones durch Minderjährige im Klassenzimmer dazu führen, dass Lehrkräfte „Überwachungsangst“ und zusätzlichem Stress im Zusammenhang mit der Notwendigkeit, die Nutzung von Geräten zu überwachen, ausgesetzt sind.

Diese festgestellten Risiken haben in den EU-Mitgliedstaaten und darüber hinaus Diskussionen darüber ausgelöst, ob die Nutzung von Smartphones durch Kinder und Jugendliche in der Schule verboten werden sollte. Die vorgeschlagenen Maßnahmen reichen von vollständigen Verboten während der Schulzeit bis hin zu differenzierteren Beschränkungen, bei denen eine Nutzung unter bestimmten Bedingungen oder unter Aufsicht vorgesehen ist.

Ende 2025 hatten die meisten EU-Mitgliedstaaten eine Form von Beschränkungen für Mobiltelefone in Schulen eingeführt oder planten dies. Die Maßnahmen reichen von vollständigen Verboten während des Schultags (Belgien, Frankreich, Österreich, Portugal, Slowenien, Ungarn und Zypern) – oft verbunden mit einer verpflichtenden Abgabe der Geräte – bis hin zu Beschränkungen, die ausschließlich für den Unterricht gelten, wobei den Schulen ein größerer Ermessensspielraum für weitere Maßnahmen eingeräumt wird (Niederlande, Rumänien und die Slowakei). Einige Länder (Bulgarien und Schweden) sind dabei, von Beratungsrahmen zu rechtsverbindlichen Vorschriften überzugehen.

Ganztägige Verbote sind die gängigste Lösung, doch die Umsetzung variiert (so gab es beispielsweise in Schweden eine positive Resonanz von 80 % der Schulen, während 20 % Schwierigkeiten bei der Umsetzung der Verbote hatten)³⁰⁹.

Zu den ermittelten Herausforderungen und unbeabsichtigten Folgen restriktiver Maßnahmen zählen die Belastung des nicht lehrenden Personals durch das Einsammeln von Geräten, Substitutionseffekte (Minderjährige ersetzen ihre Nutzung von Smartphones, z. B. durch Tablets oder Laptops), die Verlagerung von Cybermobbing auf außerschulische Zeiten und eine Überkompensation der Smartphone-Nutzung am Abend.

Strategien und Instrumente der EU

Nachdem die Möglichkeiten der Nutzung sozialer Medien und anderer digitaler Dienste durch Kinder und Jugendliche unter Abwägung der Risiken, die diese Tätigkeiten für die Gesundheit und das Wohlbefinden von Minderjährigen mit sich bringen, untersucht wurden, werden im folgenden Abschnitt ausgewählte Maßnahmen und Instrumente der EU vorgestellt, mit denen die Selbstbestimmung und Beteiligung von Minderjährigen im Internet gefördert werden sollen.

Im Mittelpunkt der Analyse stehen Strategien und Instrumente, die nach Ansicht der Ko-Vorsitzenden durch weitere Maßnahmen ergänzt oder vervollständigt werden können.

EU-KINDERRECHTSSTRATEGIE

Die Europäische Kommission hat 2021 die EU-Kinderrechtsstrategie als umfassenden politischen Rahmen angenommen, um die Rechte des Kindes in allen Politikbereichen der EU zu wahren und sicherzustellen, dass schutzbedürftige Kinder sicheren Zugang zu grundlegenden Dienstleistungen haben.

Die Strategie baut auf den folgenden sechs Säulen auf:

1. Teilhabe von Kindern am politischen und demokratischen Leben, einschließlich der EU-Plattform für die Beteiligung von Kindern,
2. sozioökonomische Inklusion, Gesundheit und Bildung, einschließlich der Europäischen Garantie für Kinder,
3. Bekämpfung von Gewalt gegen Kinder und Gewährleistung des Schutzes von Kindern,
4. kindgerechte Justiz,
5. digitale Umgebung,
6. globale Dimension.

Die digitale Säule, mit der die weitere Unterstützung der Safer-Internet-Zentren und des Programms „Better Internet for Kids“ zugesagt wurde, stellt sicher, dass Kinder sichere digitale Umgebungen und einen gleichberechtigten Zugang zu digitalen Instrumenten genießen können.

In der Strategie wurden die EU-Mitgliedstaaten aufgefordert, für einen wirksamen gleichberechtigten Zugang zu digitalen Instrumenten zu sorgen, Maßnahmen zur Förderung der Medienkompetenz durch Bildung zu unterstützen, die Fähigkeit von Kindern zu entwickeln, Online-Inhalte kritisch zu bewerten, und Desinformation und missbräuchliches Material aufzudecken.

Darüber hinaus werden die Mitgliedstaaten aufgefordert, die von der EU kofinanzierten Safer-Internet-Zentren sowie Beratungsstellen für Kinder und Melde-Hotlines zu fördern und zu unterstützen. Schließlich werden die EU-Mitgliedstaaten in der Strategie aufgefordert, die Beteiligung von Kindern (insbesondere Mädchen) an der Bildung in den Bereichen Mathematik, Informatik, Naturwissenschaften und Technik (MINT) zu fördern.

In der EU-Kinderrechtsstrategie fordert die Europäische Kommission IKT-Unternehmen auf,

- // sicherzustellen, dass die Rechte des Kindes, einschließlich der Privatsphäre, des Schutzes personenbezogener Daten und des Zugangs zu altersgerechten Inhalten, in digitalen Produkten und Dienstleistungen durch Technikgestaltung und Voreinstellungen berücksichtigt werden; dies gilt auch im Zusammenhang mit Kindern mit Behinderungen;
- // Kinder und Eltern mit geeigneten Instrumenten auszustatten, um ihre Bildschirmzeit und ihr Verhalten zu kontrollieren und sie vor den Auswirkungen der übermäßigen Nutzung und der Abhängigkeit von Online-Produkten zu schützen;
- // Maßnahmen zur Bekämpfung schädlicher Inhalte und unangemessener kommerzieller Kommunikation zu verstärken, beispielsweise durch leicht zu nutzende Melde- und Sperrkanäle oder wirksame Altersüberprüfungsinstrumente;
- // ihre Bemühungen zur Aufdeckung, Meldung und Entfernung rechtswidriger Online-Inhalte, einschließlich des sexuellen Missbrauchs von Kindern, von ihren Plattformen und Diensten fortzusetzen, soweit diese Bemühungen rechtmäßig sind.

BETTER INTERNET FOR KIDS

Die Europäische Kommission arbeitet gemeinsam mit Expertinnen und Experten, Eltern, Betreuerinnen und Betreuern, Lehrkräften und anderen einschlägigen Interessenträgern direkt mit Kindern zusammen, um sicherzustellen, dass bei der Entwicklung und Umsetzung von Maßnahmen im Zusammenhang mit dem digitalen Umfeld unterschiedliche Perspektiven berücksichtigt werden.

Die Strategie „Better Internet for Kids“ (BIK+) bietet einen umfassenden Rahmen, der darauf abzielt, Minderjährige online, einschließlich der am stärksten gefährdeten Personen, zu schützen, zu stärken und zu achten. Die Strategie unterstützt die Umsetzung der Rechtsinstrumente der EU in diesem Bereich, indem sie die Verpflichtungen durch Sensibilisierungsmaßnahmen, Kapazitätsaufbau und Unterstützungsmaßnahmen ergänzt.

Die Plattform „Better Internet for Kids“ bietet eine umfassende Sammlung von Bildungsressourcen, die Kinder und junge Menschen bei der Entwicklung der digitalen Kompetenzen unterstützen sollen, die für eine sichere, verantwortungsvolle und selbstbewusste Teilnahme an Online-Umgebungen erforderlich sind.

Die Plattform verfolgt einen viele Interessenträger einbeziehenden Ansatz, der spezielle Lernbereiche für Kinder und Jugendliche, Eltern und Betreuungspersonen sowie Lehrkräfte und Erzieherinnen und Erzieher bietet. Dies spiegelt die Rolle von Betreuungspersonen und Erzieherinnen und Erziehern als Teil der unterstützenden Personenkreise von Kindern und Jugendlichen bei der Überwachung und Lenkung der Nutzung sozialer Medien+ durch Minderjährige wider.

Bereich für Kinder

Der Kinderbereich der Plattform „Better Internet for Kids“ soll Kinder und junge Menschen durch die Bereitstellung ansprechender interaktiver Lehrmaterialien in die Lage versetzen, sich in der digitalen Welt zurechtzufinden. Hierzu zählen didaktische Spiele, die das Wissen und das Bewusstsein in Bezug auf die Sicherheit von Kindern im Internet, verantwortungsvolles Online-Verhalten und die Verhinderung von übermäßiger Nutzung und Missbrauch des Internets stärken.

Der Kinderbereich bietet darüber hinaus Lehrmaterialien, die Kinder mit der Arbeit der EU und Möglichkeiten für bürgerschaftliches Engagement durch Initiativen wie die EU-Plattform für die Beteiligung von Kindern (die später in diesem Kapitel angesprochen wird) vertraut machen.

Bereich für Eltern

Der Elternbereich der Plattform „Better Internet for Kids“ unterstützt Eltern, Betreuungspersonen und Erwachsene, die Verantwortung für Kinder tragen, durch praktische Anleitung und evidenzbasierte Bildungsressourcen zu einer Reihe von Themen im Zusammenhang mit den Online-Erfahrungen von Kindern.

In speziellen Abschnitten werden Themen wie Tools für die elterliche Aufsicht, Online-Spiele und das Management der Bildschirmzeit behandelt. Darüber hinaus bietet die Plattform eine Reihe von Lernmodulen und vertiefenden Lehrveranstaltungen, die das Verständnis der Eltern sowohl für die Risiken als auch für die Chancen, die soziale Medien und digitale Technologien mit sich bringen, verbessern sollen.

Die grundlegenden Schulungsmodule umfassen Themen wie Cybersicherheit, Bekämpfung geschlechtsspezifischer Gewalt online, Online-Spiele, manipulative Marketingpraktiken in Spielen, das Verstehen von Fehlinformationen und Desinformation, Sexting, Cybermobbing und die Rolle der Eltern bei der Unterstützung und Aufklärung von Kindern in der digitalen Welt.

Jedes Modul enthält erläuternde Inhalte, vorgeschlagene Aktivitäten und ergänzende Ressourcen zur Erleichterung des selbstbestimmten Lernens.

Bereich für Lehrerinnen und Lehrer

Der Bereich für Lehrerinnen und Lehrer bietet schließlich Lehrkräften, Erzieherinnen und Erziehern sowie anderen Fachkräften, die mit Kindern und jungen Menschen arbeiten, eine Reihe von Bildungsressourcen, die ihre Fähigkeit verbessern sollen, sich mit der Sicherheit von Kindern im Internet und der digitalen Staatsbürgerschaft in Bildungseinrichtungen zu befassen.

Der Schwerpunkt der einführenden Lernmodule liegt auf grundlegenden Aspekten der Sicherheit von Kindern im Internet und der Verantwortung von Lehrkräften bei der Unterstützung von Kindern und jungen Menschen. Dabei werden Themen behandelt wie die wichtigsten Risiken für die Sicherheit im Internet, die Vermittlung von Medienkompetenz und digitaler Bürgerschaft in Grund- und weiterführenden Schulen, die Umsetzung schulweiter Konzepte zur Sicherheit von Kindern im Internet sowie die Rechte von Kindern in der digitalen Welt.

SAFER-INTERNET-ZENTREN

Im Mittelpunkt der Strategie für ein besseres Internet für Kinder (BIK+) steht ein von der EU kofinanziertes Netz von Safer-Internet-Zentren.

Allein im Jahr 2025 erreichten die Safer-Internet-Zentren mehr als 46,4 Mio. Europäerinnen und Europäer, organisierten 448 000 Schulbesuche und Schulungen und bearbeiteten über die Insafe-Helplines³¹⁰ mehr als 57 000 Kontaktaufnahmen.

Darüber hinaus fördert das Netz gemeinsam mit der Europäischen Kommission den jährlichen Tag des sicheren Internets, die weltweite Kampagne, die jedes Jahr im Februar stattfindet, um das Bewusstsein für die Sicherheit im Internet zu schärfen.

Die Safer-Internet-Zentren stellen eine Reihe von Diensten sowohl für die Prävention als auch für die Unterstützung bereit. Sie bieten Schulungen und öffentlichkeitswirksames Material für Familien und Schulen an, um die digitale Kompetenz zu stärken und verantwortungsvolles Online-Verhalten zu fördern.

Viele Safer-Internet-Zentren in ganz Europa wurden nun im Rahmen des Gesetzes über digitale Dienste als „vertrauenswürdige Hinweisgeber“ benannt, wodurch der Schutz von Minderjährigen im Internet gestärkt wird, da illegale Inhalte, die Kinder und Jugendliche betreffen, vorrangig gemeldet werden können. Die Zentren spielen eine entscheidende Rolle dabei, die Koordinatoren für digitale Dienste über Risiken zu informieren, die Kinder und Jugendliche betreffen, und die Durchsetzung des Gesetzes über digitale Dienste zu unterstützen³¹¹.

Die Zentren betreiben zudem telefonische Beratungsdienste, die Kinder und Familien, die Online-Risiken, unter anderem Cybermobbing, ausgesetzt sind, unmittelbar unterstützen, sowie Hotlines, die die anonyme Meldung mutmaßlicher Darstellungen sexuellen Kindesmissbrauchs ermöglichen.

Die Safer-Internet-Zentren führen auf nationaler und europäischer Ebene Aufklärungskampagnen durch, um die Sicherheit von Kindern im Internet zu fördern und deren Selbstbestimmung zu stärken. Diese Kampagnen schließen gezielte Initiativen wie „DSA for YOUth“ ein, in deren Rahmen das EU-Gesetz über digitale Dienste und seine Leitlinien zum Schutz Minderjähriger auf eine für junge Menschen leicht zugängliche Weise erläutert werden.

Im weiteren Sinne tragen Sensibilisierungskampagnen dazu bei, Kinder, Betreuungspersonen und pädagogische Fachkräfte über Online-Risiken für Minderjährige sowie über sichere Praktiken zu informieren. Hierzu zählen auch Initiativen, die sich mit der Belastung durch digitale Geräte in der frühen Kindheit befassen.

DIGITALE BILDUNG UND KOMPETENZEN

Die EU-Mitgliedstaaten sind für die Organisation der nationalen Systeme der allgemeinen und beruflichen Bildung, die Lehrpläne für die Schulen und die Bereitstellung von allgemeiner und beruflicher Bildung zuständig. Die EU unterstützt die Zusammenarbeit und den Austausch bewährter Verfahren zwischen den Mitgliedstaaten und stellt über EU-Programme, einschließlich Erasmus+, finanzielle Unterstützung für Initiativen im Bereich der allgemeinen und beruflichen Bildung bereit.

Im März 2025 nahm die Europäische Kommission die Strategie für eine Union der Kompetenzen an. Die Union der Kompetenzen zielt darauf ab, durch die Förderung des kontinuierlichen lebenslangen Lernens den Erwerb grundlegender und fortgeschrittener Kompetenzen, einschließlich digitaler Kompetenzen, in der gesamten EU zu verbessern. Ein Eckpfeiler der Strategie ist der Aktionsplan für Grundkompetenzen, mit dem Defizite beim Erwerb von Grundkompetenzen, einschließlich digitaler und bürgerschaftlicher Kompetenzen, behoben werden sollen^b.

Die Ergebnisse der Internationalen Studie zur Messung der Computer- und Informationskompetenzen (ICILS) aus dem Jahr 2023 deuten darauf hin, dass es 42,5 % der 13- bis 14-Jährigen an grundlegenden Informations- und Computerkompetenzen mangelt³¹². Der sozioökonomische Hintergrund ist ein wichtiger Indikator für Computer- und Informationskompetenz. Die Quote der unterdurchschnittlichen Leistungen von Schülerinnen und Schülern mit mindestens einem Elternteil, die einen Hochschulabschluss erworben haben, ist 16 Prozentpunkte niedriger als bei Kindern, deren Eltern über niedrigere Qualifikationen verfügen (32,4 % bzw. 48,6 %)³¹³.

- b.** Bürgerliche Kompetenzen beziehen sich auf die Fähigkeit, verantwortungsvoll zu handeln und uneingeschränkt am bürgerlichen Leben teilzunehmen, sowie auf Kompetenzen wie kritisches Denken (relevant für eine konstruktive Auseinandersetzung mit künstlicher Intelligenz) und Medienkompetenz.

Darüber hinaus zeigen die jüngsten Daten aus der Internationalen Erhebung der OECD zu Lehren und Lernen (OECD Teaching and Learning International Survey, TALIS), dass sich nur 45,9 % der Lehrkräfte in den EU-Mitgliedstaaten bereit fühlen, digitale Ressourcen und Instrumente für den Unterricht zu nutzen³¹⁴. Diese Erkenntnisse unterstreichen, dass nicht nur die digitalen Fähigkeiten und Kompetenzen der Schülerinnen und Schüler gestärkt werden müssen, sondern auch die Fähigkeiten von pädagogischen Fachkräften, indem die Lehrerausbildung und die Fortbildung verbessert werden, um Kinder und Jugendliche online zu schützen und zu stärken.

Auf EU-Ebene fördert die Initiative für den europäischen Bildungsraum die Entwicklung eines „das gesamte System umfassenden, gesamtschulischen Ansatzes“, um Fragen der psychischen Gesundheit und des psychischen Wohlbefindens in Schulen anzugehen und ein positives Lernumfeld zu schaffen. Die EU-Mitgliedstaaten haben erkannt, wie wichtig es ist, Eltern, Schulen und Lehrkräfte bei der Förderung der psychischen Gesundheit und des psychischen Wohlbefindens von Kindern zu unterstützen³¹⁵.

Konsultationen mit Eltern und Betreuungspersonen zeigen, dass sich Eltern oft überfordert fühlen und dass sie den neuesten technologischen Entwicklungen in den sozialen Medien+ „ständig hinterherhinken“. Gleichzeitig ist das Bewusstsein dafür, wie Kinder unterstützt werden können, wenn sie auf schädliche oder rechtswidrige Inhalte stoßen, oft begrenzt³¹⁶.

Die Mitgliedstaaten haben auch betont, dass Anbieter sozialer Medien und anderer digitaler Dienste vermeiden müssen, absichtlich auf Kinder abzielende, suchterzeugende Gestaltungspraktiken einzusetzen, und dass sie die altersgerechte Gestaltung sozialer Medien und anderer digitaler Dienste fördern müssen³¹⁷.

**„Die Lehrerausbildung
als nichtlegislative
Säule für die
Sicherheit von Kindern
im Internet
positionieren ...
Die digitale Bildung in
alle Lehrerausbildungs-
programme einbetten
und Lehrkräfte
zur wirksamen
Zusammenarbeit mit den
Eltern befähigen.“**

— LOUISE HEERAN FLYNN,

ASSISTENZPROFESSORIN FÜR
LEHRERAUSBILDUNG AM TRINITY COLLEGE
DUBLIN

AKTIONSPLAN FÜR DIGITALE BILDUNG

Digitale Bildung und Medienkompetenz sind von grundlegender Bedeutung, um Kindern und Jugendlichen die Fähigkeiten zu vermitteln, die sie benötigen, um sich sicher online zurechtzufinden. Die digitalen Kompetenzen und die Medienkompetenz von Kindern und Jugendlichen hinken jedoch dem Tempo des technologischen Wandels im Bereich der sozialen Medien und darüber hinaus hinterher – entgegen der Vorstellung, dass Minderjährige heutzutage „Digital Natives“ seien.

Es ist von entscheidender Bedeutung, digitale Kompetenzen und digitale Kompetenz in die nationalen Bildungssysteme zu integrieren. Einer Eurobarometer-Umfrage aus dem Jahr 2025 zufolge sind 92 % der Europäerinnen und Europäer der Ansicht, dass digitale Kompetenzen allen Menschen auf allen Bildungsebenen vermittelt werden sollten und dass Schülerinnen und Schüler in der Schule lernen sollten, wie sie

die Auswirkungen digitaler Technologien (einschließlich sozialer Medien) auf ihre psychische und physische Gesundheit bewältigen können³¹⁸.

Zur Unterstützung der EU-Mitgliedstaaten bei der Bereitstellung hochwertiger, inklusiver und zugänglicher digitaler Bildung legt die Europäische Kommission den Aktionsplan für digitale Bildung (2021-2027) vor. Der Plan ermöglicht es den EU-Mitgliedstaaten, ihre Bildungssysteme an den raschen technologischen Wandel und die zunehmende Bedeutung digitaler Kompetenzen anzupassen.

Die beiden wichtigsten strategischen Prioritäten des Aktionsplans für digitale Bildung sind der Aufbau eines starken europäischen Ökosystems für digitale Bildung und die Verbesserung digitaler Fähigkeiten und Kompetenzen. Konkret werden im Rahmen des Plans die Verbesserung der digitalen Lerninfrastruktur und -umgebungen, der Internetverbindung und der digitalen Ausrüstung in Schulen, die Bereitstellung hochwertiger digitaler Lerninhalte und -plattformen sowie die Fortbildung von Lehrkräften im Umgang mit digitalen Instrumenten und pädagogischen Konzepten gefördert.

Im Rahmen des Aktionsplans für digitale Bildung veröffentlichte die Kommission im März 2026 vier Leitlinienpakete³¹⁹ zur Unterstützung von pädagogischen Fachkräften bei Themen wie der Bekämpfung von Desinformation und der Förderung digitaler Kompetenzen, der ethische Nutzung von KI und Daten in der Bildung, hochwertige digitale Bildungsinhalte und Informatikunterricht.

Die Leitlinien für Lehrkräfte und andere pädagogische Fachkräfte zur Bekämpfung von Desinformation und zur Förderung der digitalen Kompetenz durch allgemeine und berufliche Bildung bieten Ressourcen für eine sachkundige und sichere Nutzung sozialer Medien, generativer KI und Prebunking^e und enthalten Unterrichtspläne für Lehrkräfte zur Bekämpfung von Cybermobbing zusammen mit Themen wie Geschlechterstereotypen und Deepfakes³²⁰.

Im Rahmen des Aktionsplans für digitale Bildung bietet die europäische Plattform für digitale Bildung eine Online-Gemeinschaft, auf der pädagogische Fachkräfte, politische Entscheidungsträger, Forschende und andere Interessenträger zusammenkommen. Über die Plattform tauschen sie Wissen und bewährte Verfahren aus und entwickeln gemeinsam Lösungen für die digitale Bildung. Die Plattform unterstützt Lehrkräfte und Erzieherinnen und Erzieher ferner bei der Vernetzung und Teilnahme an Aktivitäten wie Peer-Learning im Bereich der digitalen Bildung.

Darüber hinaus bieten das Programm Erasmus+ und das Europäische Solidaritätskorps sowie die Europäische Plattform für Schulbildung (ESEP) und die eTwinning-Gemeinschaft zusätzliche Unterstützung, um Minderjährige und Erzieherinnen und Erzieher online zu stärken. Hierzu zählen Möglichkeiten des nicht-formalen Lernens und des Engagements sowie die Unterstützung von Räumen, in denen Schulgemeinschaften interagieren, wachsen und ihre Kompetenzen entwickeln können.

Ende 2026 wird die Europäische Kommission ein Bildungspaket auf den Weg bringen. Durch das Paket wird die Zukunftsfähigkeit der nationalen Bildungsökosysteme gefördert, indem strukturelle Herausforderungen einschließlich der Notwendigkeit einer sicheren, souveränen und vertrauenswürdigen europäischen Infrastruktur für digitale Bildung angegangen werden. Das Paket wird dazu beitragen, Kinder und Jugendliche mit den wesentlichen Kompetenzen auszustatten, die sie für die konstruktive Auseinandersetzung mit KI und digitalen Technologien benötigen, indem angestrebt wird, digitales Wohlbefinden und digitale Kompetenzen sowie Sicherheit im Internet in die nationalen Bildungssysteme einzubetten.

c. Prebunking ist eine Präventivmaßnahme, die darauf abzielt, Zielgruppen darauf vorzubereiten, Informationsrisiken, einschließlich Fehlinformationen und Desinformation, zu erkennen und ihnen zu widerstehen.

KAMPAGNE „AI≠HUMAN – TALK TO A PERSON“

Sensibilisierungsinitiativen auf nationaler Ebene, einschließlich der Kampagne „AI≠Human – Talk to a person“, zeigen, wie wichtig es ist, Kinder und Jugendliche dabei zu unterstützen, die Beschaffenheit und die Grenzen KI-gestützter Instrumente, einschließlich Chatbots, zu verstehen und zu wissen, wie diese Instrumente auf kritische und verantwortungsvolle Weise eingesetzt werden können.

Solche Initiativen vermitteln Kindern und Jugendlichen eine klare Botschaft, nämlich: Künstliche Intelligenz kann zwar ein nützliches Instrument sein, wenn sie mit den richtigen Sicherheitsvorkehrungen eingesetzt wird, aber menschliche Beziehungen kann sie nicht ersetzen.

Die Kampagne fand im Frühjahr 2026 statt und wurde vom luxemburgischen Ministerium für Bildung, Kinder und Jugend in Zusammenarbeit mit dem Safer-Internet-Zentrum „BEE SECURE“, dem psychosozialen und schulischen Unterstützungszentrum (Cepas) und dem luxemburgischen Schülerverband (CNEL) entwickelt.

Sie machte auf eine Reihe potenzieller Risiken im Zusammenhang mit der unkritischen oder übermäßigen Nutzung von KI aufmerksam. Zu diesen Risiken zählen die Möglichkeit einer stärkeren sozialen Isolation, der Einsatz von KI als Ersatz für menschliche Interaktion und ein Rückgang des echten Dialogs und der persönlichen Kommunikation.

Darüber hinaus werden in der Kampagne Bedenken im Zusammenhang mit dem „kognitiven Auslagern“ hervorgehoben, die sich auf Situationen beziehen, in denen sich Nutzer zunehmend auf KI-Systeme stützen, um Gedanken zu strukturieren, Reaktionen zu erzeugen oder Entscheidungen zu treffen. Dies kann die Möglichkeiten für unabhängiges Nachdenken und aktives kognitives Engagement verringern. Im Rahmen der Kampagne werden auch Fragen des Datenschutzes und der Privatsphäre im Zusammenhang mit dem Einsatz von KI hervorgehoben.

KI-KOMPETENZRAHMEN

Im Juni 2026 legten die OECD und die Europäische Kommission einen Rahmen für KI-Kompetenzen in der allgemeinen und beruflichen Bildung ³²¹ vor. Die Initiative fördert gemeinsame Ansätze für die Entwicklung von KI-Kompetenzen in den nationalen Bildungssystemen.

Der Rahmen unterstützt Lehrkräfte, Bildungssysteme und Schulen dabei, Kindern die Kompetenzen zu vermitteln, die sie benötigen, um KI zu verstehen und sich kritisch mit ihr auseinanderzusetzen. Dabei wird das Ziel angestrebt, Kinder in die Lage zu versetzen, sicher mit KI zu interagieren, die Entwicklung von KI zu steuern und zu gestalten und die mit diesen Instrumenten verbundenen Chancen und Risiken kritisch zu bewerten.

BETEILIGUNG DER KINDER

Kinder und Jugendliche müssen sinnvolle Möglichkeiten erhalten, sich am demokratischen Leben zu beteiligen, und systematisch in Entscheidungen einbezogen zu werden, die sich auf ihr tägliches Leben auswirken. Dazu gehört auch die Gestaltung und Umsetzung politischer Maßnahmen zur Förderung des Schutzes und der Befähigung Minderjähriger im Internet.

Eine sinnvolle Beteiligung von Kindern beruht auf gegenseitigem Respekt, Transparenz und der Freiwilligkeit der Beteiligung. Bei jeder Beteiligung von Kindern sollten klare, altersgerechte Informationen über die Ziele und Abläufe ihrer Beteiligung bereitgestellt und geeignete Schutzmaßnahmen dargelegt werden. Minderjährige sollten klare Informationen über die Art und Weise, wie ihre Beiträge verwendet werden, erhalten.

Es muss dafür gesorgt werden, dass Minderjährige als Interessenträger bei Entscheidungen, die ihr Leben prägen, anerkannt werden; dies ist für die Wahrung ihrer Rechte sowohl im realen Leben als auch online von grundlegender Bedeutung. In der ersten Säule der EU-Kinderrechtsstrategie wird die Bedeutung der Beteiligung von Kindern anerkannt, die beispielsweise durch die EU-Plattform für die Beteiligung von Kindern gefördert wird.

Maßnahmen zur Förderung der Jugendbeteiligung, einschließlich des Jugend-Checks, der jugendpolitischen Dialoge, des Jugendbeirats der Präsidentin und des EU-Jugenddialogs, spielen ebenfalls eine wichtige Rolle bei der stärkeren Einbeziehung junger Menschen in die Politikgestaltung auf EU-Ebene.

Durch die aktive Einbeziehung von Kindern und Jugendlichen in Diskussionen über Sicherheit im Internet erfüllen die politischen Entscheidungsträger nicht nur rechtliche und ethische Verpflichtungen, sondern nutzen auch die einzigartigen Perspektiven Minderjähriger beim Schutz und der Wahrung ihrer Rechte online. Es sollten Maßnahmen ergriffen werden, um sicherzustellen, dass im Rahmen der Beteiligung von Kindern stets Kinder und Jugendliche mit unterschiedlichem Hintergrund und aus unterschiedlichen geografischen Gebieten einbezogen werden, damit die Inklusivität und Wirksamkeit von Maßnahmen zum Schutz und zur Stärkung Minderjähriger im Internet sichergestellt wird.

Darüber hinaus ist es von entscheidender Bedeutung, Kinder und Jugendliche in die Lage zu versetzen, Teil des Vorhabens, den Raum der sozialen Medien+ zu einem sicheren Raum zu machen, zu werden. Meldungen und Beschwerden von Kindern und Jugendlichen müssen im Rahmen der Inhaltsmoderation von Anbietern sozialer Medien und anderer digitaler Dienste vorrangig behandelt werden.

In der Empfehlung der Europäischen Kommission zur Entwicklung und Stärkung integrierter Kinderschutzsysteme werden die EU-Mitgliedstaaten aufgefordert, für einen kohärenten rechtlichen und politischen Rahmen zum Schutz von Kindern, für sichere, vertrauliche und kindgerechte Beschwerde- und Melde-mechanismen sowie für hochwertige familiäre und gemeindenähe Dienste und Fürsorge die Beteiligung von Kindern sicherzustellen³²².

„Im Mittelpunkt der Bemühungen zur Verbesserung der Sicherheit von Kindern im Internet sollte die Schaffung eines sicheren und unterstützenden digitalen Umfelds stehen, wobei gleichzeitig die Möglichkeiten der Kinder, zu lernen, zu spielen, teilzunehmen, zu kommunizieren und auf Informationen zuzugreifen, zu wahren sind.“

— ALEXANDRA WEILENMANN,
PROFESSORIN FÜR INTERAKTIONSDESIGN,
UNIVERSITÄT GÖTEBORG

EU-PLATTFORM FÜR DIE BETEILIGUNG VON KINDERN

Kinder haben das Recht, ihre Meinung frei zu äußern, und das Recht, dass ihre Meinung in Angelegenheiten, die sie betreffen, berücksichtigt wird³²³. Um diese Rechte in die Praxis umzusetzen, richtete die Europäische Kommission die EU-Plattform für die Beteiligung von Kindern ein.

Die EU-Plattform für die Beteiligung von Kindern bietet einen eigens dafür vorgesehenen Raum, in dem Kinder unter 18 Jahren direkt mit politischen Entscheidungsträgern und Verantwortlichen in Kontakt treten können. Die Plattform bietet Kindern und Jugendlichen einen sicheren Raum, in dem sie ihre Ansichten austauschen und Themen, die sie betreffen, erörtern können. Die Plattform organisiert Tätigkeiten, darunter Treffen, Workshops, Schulungen sowie Online- und persönliche Umfragen, um die Meinungen von Kindern zusammenzutragen.

Über die EU-Plattform für die Beteiligung von Kindern konsultierte die Europäische Kommission Tausende von Kindern unter anderem zu Themen wie Cybermobbing, Sicherheit im Internet und digitales Wohlbefinden sowie zum anstehenden Gesetz über digitale Fairness. Dieser Prozess hat zur Schaffung eines „Aufrufs zum Handeln an die Entscheidungsträger der EU“³²⁴ geführt, in dem Angelegenheiten angesprochen werden, die von höchster Bedeutung für Kinder sind.

Im Rahmen dieser Konsultationen hoben die Kinder ihren Wunsch hervor, sich aktiv an der Gestaltung der Vorschriften zu beteiligen, die sich auf ihre Online-Aktivitäten auswirken. Viele machten auch deutlich, dass Erwachsene – nicht Kinder – dafür verantwortlich seien, wie die Online-Welt und die sozialen Medien+ konzipiert wurden und heute funktionieren, und dass Kinder nicht für deren Versäumnisse „bestraft“ werden sollten.

Die Botschaft der Kinder ist klar: Sie wollen, dass die Online-Welt sicherer, gerechter und verständlicher wird, mit strengeren Vorschriften für Fälle, in denen Online-Dienste unfair, schädlich oder suchterzeugend sein können. Sie forderten auch Alternativen zu sozialen Medien+, einschließlich außerschulischer Aktivitäten und Sport, und forderten die Entscheidungsträger auf, sich mit Fragen des Wohlbefindens und der psychischen Gesundheit im Zusammenhang mit der Nutzung sozialer Medien durch Kinder zu befassen.

EMPFEHLUNGEN VON KINDERN

Vom 16. bis 18. April 2026 trafen sich 20 Kinder und Jugendliche aus verschiedenen EU-Mitgliedstaaten in Berlin zum Studienbesuch der EU-Plattform für die Beteiligung von Kindern zum Thema Wohlbefinden und psychische Gesundheit.

Zwei Tage lang haben sie Erfahrungen geteilt, gelernt und Empfehlungen zusammengestellt, wie sich Kinder in Fragen der psychischen Gesundheit sicher, unterstützt, respektiert und angehört fühlen können und wie Erwachsene, Schulen, Familien und Dienste das Wohlbefinden von Kindern besser fördern können.

Im Rahmen des Studienbesuchs gaben die Kinder mehrere Empfehlungen dazu ab, was sie zur Stärkung ihres Wohlbefindens benötigen:

- // Wir sollten die Freiheit haben, an einem Gespräch teilzunehmen oder es zu verlassen, einen sicheren Raum haben, um unsere Meinung zu äußern, und wissen, an wen wir uns wenden können.
- // Wir brauchen stabile, zuverlässige Unterstützungssysteme, Strukturen, um gehört zu werden, und eine Gemeinschaft, auf die wir uns verlassen können.
- // Wir sollten Zugang zu „emotionalen Ventilen“ wie Bewegung und Sport, Hobbys, Journaling, Entspannung, sichere Räume für Spiele und Aktivitäten haben.
- // Schulen sollten Gespräche über psychische Gesundheit zur Normalität machen und regelmäßige Tage, an denen Themen des psychischen Wohlbefindens behandelt werden, einführen. Es sollten sichere Umgebungen geschaffen werden, in denen wir uns wohlfühlen, wenn wir über unsere psychische Gesundheit sprechen, und Lehrkräfte sollten darin geschult werden, Unterstützung im Bereich der psychischen Gesundheit zu leisten, genauso wie sie in Erster Hilfe geschult werden. Jede Schule sollte über ausgebildetes psychologisches oder beratendes Personal verfügen, das tatsächlich zugänglich ist und dem die Schülerinnen und Schüler vertrauen.
- // Wir brauchen eine klare, offene und wirksame Kommunikation mit Erwachsenen.
- // Wir brauchen klare Kennzeichnungen, damit wir erkennen können, an welche Erwachsenen wir uns in unterschiedlichen Situationen und bei unterschiedlichen Themen wenden können;
- // Gesundheitsthemen müssen in den Schulen ausreichend abgedeckt werden, sodass wir keine Online-Räume nutzen müssen, um Lücken zu schließen^d.

- d.** In Bulgarien beispielsweise gaben Kinder an, dass sie Informationen über Gesundheitsthemen hauptsächlich über KI-Tools erhalten.

Peer-Beratung

Durch die Schaffung eines unterstützenden Umfelds für die Erörterung von Herausforderungen mit geschulten Peers kann die Peer-Beratung bei der Förderung des Wohlbefindens von Kindern und Jugendlichen sowohl online als auch offline eine wichtige Rolle spielen. Da es Kindern oft leichter fällt, sich jemandem anzuvertrauen, der etwa in ihrem Alter ist, kann die Peer-Beratung dazu beitragen, dass sie frühzeitig Hilfe in Anspruch nehmen, und verhindern, dass Probleme eskalieren. Zudem sorgt sie dafür, dass es offline einen sicheren Raum gibt, in dem sie Kontakte knüpfen und auf der Grundlage gemeinsamer Erfahrungen sinnvolle Bindungen aufbauen können.

Im Zusammenhang mit der Sicherheit von Kindern im Internet können Peer-Beraterinnen und -Berater dazu beitragen, das Bewusstsein für Risiken wie Cybermobbing, einen gesunden Umgang mit Bildschirmen und sozialen Medien, Falschinformationen und Desinformation, künstliche Intelligenz sowie die Bedeutung des Schutzes personenbezogener Daten zu schärfen. Peer-Beraterinnen und -Berater können positives digitales Verhalten fördern, einschließlich respektvoller Kommunikation, Empathie, kritischem Denken und verantwortungsvoller Online-Beteiligung.

Da die Peer-Unterstützung von etwa Gleichaltrigen geleistet wird, die ähnliche Erfahrungen gemacht haben, wird die Peer-Beratung von Kindern und Jugendliche häufig als nachvollziehbarer und glaubwürdiger empfunden und wirkt auf Kinder und Jugendliche weniger formell oder einschüchternd. Sie kann innerhalb von Schulen oder Gemeinschaften das Zugehörigkeitsgefühl, die Inklusion und die gegenseitige Unterstützung fördern und Minderjährige in die Lage versetzen, bei der gegenseitigen Unterstützung im Hinblick auf sichere Online-Erfahrungen eine aktive Rolle zu spielen.

**„Echte Sicherheit
im Internet geht
über Regulierung
hinaus. Sie erfordert
digitale Kompetenz,
barrierefreie
Unterstützung und
Investitionen in
Offline-Räume.“**

— MARTINA TÓTHOVÁ,
JUGENDBEIRAT DER PRÄSIDENTIN,
JUGENDRAT DER SLOWAKEI

BEISPIELE FÜR BEWÄHRTE VERFAHREN DER PEER-BERATUNG

Das Referenzzentrum für psychosoziale Unterstützung der Internationalen Föderation der Rotkreuz- und Rothalbmondgesellschaften (IFRC) hat das Toolkit „**Psychologische Erste Hilfe für junge Peers**“ entwickelt, um jungen Menschen bei der Unterstützung Gleichaltriger in schwierigen Zeiten Hilfestellung zu leisten³²⁵.

Dieses Toolkit stärkt die Handlungskompetenz junger Menschen, indem es ihnen die Kompetenzen und Kenntnisse vermittelt, die sie benötigen, um ihren Altersgenossen zu helfen, wobei gleichzeitig das Bewusstsein für die Bedeutung der Selbstfürsorge geschärft wird³²⁶. Das übergeordnete Ziel des Toolkits besteht darin, die Resilienz junger Menschen gegenüber widrigen Ereignissen und Krisensituationen zu stärken und sie mit Kenntnissen und Kompetenzen im Bereich der psychologischen Ersten Hilfe auszustatten³²⁷. Das Toolkit umfasst ein Handbuch, in dem das Konzept der psychologischen Ersten Hilfe vorgestellt wird und praktische Beispiele dafür gegeben werden, wie junge Menschen dieses Konzept anwenden können, um Gleichaltrigen zu helfen³²⁸.

Das Toolkit bietet auch ein Schulungspaket für Schulen, Jugend- und Sportvereine und Pfadfinderorganisationen. Die Teilnehmenden erfahren, welche Herausforderungen Menschen ihres Alters betreffen, welche Krisenereignisse und -reaktionen es gibt und wie die Grundprinzipien der psychologischen Ersten Hilfe und Verfahren der Selbstfürsorge angewendet werden³²⁹. Die Teilnehmer lernen auch zu erkennen, wann jemand möglicherweise Hilfe benötigt, die über das hinausgeht, was sie leisten können³³⁰.

Ein weiteres Beispiel für bewährte Verfahren ist die portugiesische Initiative „**Líderes Digitais**“ (digitale Vorreiter), die vom SeguraNet-Sensibilisierungszentrum³³¹ entwickelt wurde. Durch einen Peer-to-Peer-Ansatz werden die Schülerinnen und Schüler im Rahmen dieser Initiative dazu befähigt, als digitale Botschafter an ihren Schulen zu agieren.

Teilnehmende Schülerinnen und Schüler werden zu Themen wie digitale Bürgerschaft, Sicherheit im Internet, Cybermobbing, Privatsphäre und Datenschutz, Falschinformationen, Medienkompetenz sowie dem verantwortungsvollen Umgang mit neuen Technologien, einschließlich künstlicher Intelligenz, geschult. Anschließend teilen sie mittels Sensibilisierungsmaßnahmen, Workshops, Diskussionen im Unterricht und informelle Unterstützung dieses Wissen mit Gleichaltrigen, was zu einer sichereren und positiveren digitalen Kultur in der Schulgemeinschaft beiträgt.

Von Gleichaltrigen geleitete Initiativen wie „Líderes Digitais“ zeigen, wie Kinder aktiv dazu beitragen können, das Wohlbefinden online und die digitale Resilienz zu fördern. Durch die Förderung des Dialogs unter Gleichaltrigen stärken diese Initiativen positive digitale Verhaltensweisen, darunter respektvolle Online-Kommunikation, kritisches Denken, Empathie und verantwortungsbewusste Teilnahme an digitalen Umgebungen, und stärken gleichzeitig das Zugehörigkeitsgefühl der Kinder sowie ihre gegenseitige Unterstützung.

Der langfristige Erfolg und die Skalierbarkeit von Peer-Beratungsinitiativen hängen jedoch von einer nachhaltigen Finanzierung und institutionellen Unterstützung ab, um für ihren Fortbestand zu sorgen und es mehr Schulen und Kindern zu ermöglichen, von diesen Initiativen zu profitieren. In Anbetracht des von ihnen geleisteten erheblichen Beitrags zur Sicherheit im Internet und zum Wohlbefinden von Kindern ist es daher unerlässlich, ihren Wert anzuerkennen und in ihre Weiterentwicklung zu investieren.

Empfehlungen

EMPFEHLUNG 1

Minderjährigen mehr Möglichkeiten bieten, die Welt der sozialen Medien+ in einem geschützten Rahmen aktiv mitzugestalten

Kinder und Jugendliche sollten sinnvolle Möglichkeiten erhalten, Rechtsvorschriften, Strategien und Bildungsinitiativen zur Förderung der Sicherheit und Befähigung von Kindern online aktiv mitzugestalten. Dementsprechend sollten mehr Maßnahmen für die Beteiligung von Kindern und Jugendlichen an einschlägigen Vorhaben ergriffen werden. So sollten Kinder beispielsweise bei der Gestaltung von Sicherheitsstrategien, Lernprogrammen, Evaluierungen und Leitfäden einbezogen werden. Die Auswirkungen dieser Maßnahmen auf die Sicherheit und die Rechte von Kindern sollten kontinuierlich beobachtet und evaluiert werden.

Bei Verfahren zur Beteiligung von Kindern sollte sichergestellt werden, dass die Kinder klare Informationen erhalten, dass sie verstehen, wie ihre Beiträge weiterverwendet werden, und dass sie über die weiteren Entwicklungen am Laufenden gehalten werden. Es sollten besondere Anstrengungen unternommen werden, um Kinder aus benachteiligten, marginalisierten und schutzbedürftigen Gruppen einzubeziehen. Für alle Aktivitäten, an denen Kinder beteiligt sind, müssen geeignete Schutzmaßnahmen vorgesehen werden.

EMPFEHLUNG 2

Beschwerde- und Meldemechanismen sowie Verbraucherrechte von Kindern und Jugendlichen ausweiten

Meldungen und Beschwerden von Kindern und Jugendlichen sollten bei der Moderation von Inhalten durch Anbieter sozialer Medien und anderer digitaler Dienste vorrangig behandelt werden. Die Anbieter müssen intensiver in die Pflicht genommen werden, damit für Beratungs- und Hilfsangebote und Beschwerdemechanismen ausreichende Mittel zur Verfügung stehen. Diese Mechanismen müssen altersgerecht, benutzerfreundlich, zugänglich und wirksam sein und die Privatsphäre wahren.

EMPFEHLUNG 3

Aufbau und Nutzung von sozialen Medien und anderen digitalen Diensten, die auf den Werten der EU aufbauen, und wo Minderjährige sicher miteinander in Kontakt treten können, finanzieren und bewerben

Unterstützung der Einrichtung und der allgemeinen Verbreitung von auf EU-Werten basierenden, auf Sicherheit durch Technikgestaltung ausgelegten und altersgerechten sozialen Medien sowie anderer digitaler Dienste durch öffentliche Investitionen. Durch solche Dienste sollten zuverlässige Informationen bereitgestellt werden, die es Kindern und Jugendlichen (aber auch Erwachsenen) ermöglichen, sichere Online-Interaktionen zu führen, ohne schädlichen Inhalten ausgesetzt zu sein.

EMPFEHLUNG 4**Programme für digitale Bildung und zur Förderung digitaler Kompetenzen für Minderjährige, Eltern und Betreuungspersonen, Lehrkräfte und pädagogische Fachkräfte etablieren**

Digitale Bildung und digitale Kompetenz sollten auf allen Bildungsebenen als zentrale Grundfertigkeit für Minderjährige, Eltern und Lehrkräfte verankert werden. Wohlbefinden im digitalen Raum sollte Teil der digitalen Bildung für alle sein.

Bildung sollte Kinder und Jugendliche in die Lage versetzen, Informationen und Quellen online kritisch zu bewerten und Manipulationstechniken wie z. B. Desinformation, Deepfakes und personalisierte Werbung zu erkennen. Außerdem sollten Minderjährige, Eltern und Lehrkräfte darüber aufgeklärt werden, wie digitale Inhalte erstellt und geteilt werden und wie Algorithmen das Wahrnehmen und Erleben in der Welt der sozialen Medien+ beeinflussen.

Durch strukturierte Bildungsangebote für die Sicherheit im Internet sollten praktische Kompetenzen in Bezug auf den Schutz personenbezogener Daten, die Verwaltung von Datenschutzeinstellungen, die Wahrung sicherer digitaler Identitäten und die Ermittlung von Risiken insbesondere in sozialen Medien+, bei Nachrichtenübermittlungsdiensten und in Spielumgebungen aufgebaut werden. Diese Kompetenzen sollten laufend ausgebaut werden, ausgehend von einfachen Verhaltensweisen für mehr Sicherheit hin zu einem Verstehen komplexerer Konzepte wie digitaler Fußabdruck, Einwilligungserklärungen und Risiken auf Plattformen. Für ein gesundes Bildschirmverhalten sollten Kinder angeleitet werden, eine ausgewogene Nutzung zu erlernen, ihre Aufmerksamkeit zu regulieren und übermäßiges oder schädliches Nutzungsverhalten zu erkennen.

Die Safer-Internet-Zentren sollten weiterhin eine Schlüsselrolle bei der Bereitstellung von Schulungen, Sensibilisierungsmaßnahmen, Ressourcen und Unterstützung für Kinder, Eltern, Betreuungspersonen und Lehrkräfte spielen. Die Entwicklung leicht zugänglicher Online-Kurse für Eltern, Lehrkräfte und junge Nutzerinnen und Nutzer sollte finanziert werden.

Neben der Sicherheit sollte in der Bildung auch ein Schwerpunkt auf die Chancen und die Stärkung der Handlungskompetenz gelegt werden, d. h., wie Schülerinnen und Schüler digitale Instrumente zum Lernen sowie für Kreativität, Zusammenarbeit und staatsbürgerliche Beteiligung nutzen können.

EMPFEHLUNG 5**Mehr Angebot und geeignete Infrastruktur für Offline-Aktivitäten schaffen**

Die Mitgliedstaaten und die lokalen Behörden sollten das Angebot an erschwinglichen Sport-, Kunst- und Kulturstätten, Jugendclubs, Bibliotheken und Gemeinschaftsräumen erhalten und erweitern und den Zugang dazu erleichtern, um Minderjährige verstärkt für gesunde Offline-Aktivitäten zu gewinnen und attraktive Alternativen zur übermäßigen Bildschirmnutzung zu schaffen. Dafür bedarf es Investitionen in sichere, inklusive und altersgerechte Räume, in denen Minderjährige miteinander in Kontakt treten, lernen, spielen und positive Beziehungen in ihrem Umfeld aufbauen können.

EMPFEHLUNG 6**Gemeinsam Leitfäden für Eltern ausarbeiten**

Gemeinsam mit Elternvereinigungen sollten sich die EU und die Mitgliedstaaten dafür einsetzen, dass Leitfäden für Eltern ausgearbeitet werden. Die Leitfäden würden Eltern und Betreuungspersonen als klare und leicht zugängliche Ratgeber dabei unterstützen, Minderjährige im sicheren, verantwortungsvollen und positiven Umgang mit den sozialen Medien+ zu begleiten. Die Leitfäden sollten praktische Hilfestellungen zu wichtigen Themen wie Sicherheit im Internet und Datenschutz, digitales Wohlbefinden, ethische und verantwortungsvolle Nutzung und Hilfsangeboten bieten.

EMPFEHLUNG 7**Eltern und Betreuungspersonen mit den modernsten Hilfsmitteln für Kontrolle und Aufsicht unterstützen, die laufend an den neuesten Stand der Technik angepasst werden**

Die Anstrengungen zur Befähigung von Minderjährigen sollten durch kontinuierliche Unterstützung für Eltern und Betreuungspersonen ergänzt werden; dabei sollte es nicht nur um digitale Fähigkeiten und Kompetenzen gehen, sondern auch um Instrumente, mit denen Betreuungspersonen Minderjährige bei der Nutzung sozialer Medien und anderer digitaler Dienste anleiten können, ohne ihre Rechte unverhältnismäßig einzuschränken. Dazu gehört auch die Bereitstellung praktischer Instrumente für die elterliche Aufsicht und die Sensibilisierung für diese Instrumente, ergänzt durch zuverlässige Informationen über Risiken, sichere Praktiken und die Art und Weise, wie der Kontakt mit Kindern gestaltet werden kann. Die Sensibilisierung der Eltern sollte persönlich erfolgen (beispielsweise bei Gesprächen mit Lehrkräften in der Schule, Besuchen beim Kinderarzt oder bei der Kinderärztin, sowie während des Mutterschutzes oder der Elternzeit).

Die Instrumente der elterlichen Aufsicht sollten wirksam, benutzerfreundlich, interoperabel und altersgerecht sein; sie sollten den sich entwickelnden Fähigkeiten Minderjähriger entsprechen und so konzipiert sein, dass sie Kommunikation, Lernen und Befähigung fördern und nicht Kontrolle. Dies ist entscheidend, um Minderjährigen schrittweise den Umgang mit sozialen Medien zu ermöglichen. Mit diesen Instrumenten soll dafür gesorgt werden, dass Änderungen nur mit derselben Berechtigungsstufe vorgenommen werden können, die für ihre Aktivierung erforderlich ist; sie sollen unabhängig vom Gerät oder Betriebssystem gelten und Schutzmaßnahmen umfassen, die Minderjährige vor einem möglichen Missbrauch durch Eltern warnen (beispielsweise durch einen deutlichen Hinweis für Minderjährige, wenn Überwachungsinstrumente aktiviert sind).

EMPFEHLUNG 8**Ausreichende öffentliche Finanzierung und gemeinsame Standards für Organisationen der Zivilgesellschaft und Peer-Beratung sichern**

Die EU und die Mitgliedstaaten sollten sicherstellen, dass die Safer-Internet-Zentren und ähnliche Organisationen der Zivilgesellschaft auch künftig mit ausreichenden finanziellen Mitteln ausgestattet werden und dass ihre Arbeit sich nach gemeinsamen, von Fachleuten entwickelten Standards richtet. Nur so können sie weiter Sensibilisierungs-, Schulungs- und Unterstützungsdienste anbieten und ihr Angebot weiterentwickeln.

Öffentliche Mittel sind von entscheidender Bedeutung, damit sie weiter unabhängig agieren können und das Angebot kohärent bleibt.

Auch Peer-Beratung, Beratungs- und Hilfsangebote, Bildungsressourcen, Sensibilisierungskampagnen und Maßnahmen für Kapazitätsaufbau sollten von der öffentlichen Hand finanziert werden. Mit weiteren Investitionen sollten die Sichtbarkeit, Zugänglichkeit und Reichweite dieser Einrichtungen – auch für schutzbedürftige Minderjährige – erhöht und Initiativen zur Förderung sichererer Umgebungen in den sozialen Medien+ unterstützt werden.

EMPFEHLUNG 9

Das Gesundheitssystem in die Lage versetzen, Suchterkrankungen und andere psychische Erkrankungen im Zusammenhang mit der Nutzung sozialer Medien und anderer digitaler Dienste zu diagnostizieren und zu behandeln

Die Gesundheitssysteme sollten diagnostische ICD-11-Standards für verhaltensabhängige Suchterkrankungen, einschließlich Spielsucht und zwanghafter Nutzung sozialer Medien+, umsetzen. Eine evidenzbasierte Behandlung dieser Erkrankungen sollte im Rahmen des Gesundheitssystems zugänglich gemacht werden. Medizinische Fachkräfte und Psychotherapeuten sollten sich der potenziellen Folgen von Schäden bewusst sein, die durch „digitale Vernachlässigung“ und unfreiwillige Konfrontation mit nicht altersgerechten Inhalten, Cybermobbing, Online-Grooming, Sextortion und andere Schäden verursacht werden.

Die Gesundheitssysteme sollten evidenzbasierte Behandlungen für PTBS und andere psychopathologische Folgen anbieten. Darüber hinaus könnte die digitale Risikobewertung in Kinderuntersuchungen und in gezielte Präventionsmaßnahmen für schutzbedürftige Minderjährige integriert werden. Präventionsmaßnahmen und verhaltensbezogene Herausforderungen, darunter „Online-Fasten“ oder „Digital Detox“ (Auszeit vom Internet), könnten zu mehr Erlebnissen außerhalb des Internets beitragen und einen kulturellen Wandel hinsichtlich der Internetnutzung von Minderjährigen bewirken.

EMPFEHLUNG 10

Aus- und Weiterbildung von Lehrkräften im Bereich digitaler Kompetenzen und Medienkompetenz fördern und Eltern einbeziehen

Die EU und die Mitgliedstaaten sollten sicherstellen, dass die digitale Kompetenzen einschließlich KI-Kompetenzen sowie digitales Wohlbefinden systematisch in die anfängliche und weitere berufliche Aus- und Weiterbildung von Lehrkräften einbezogen werden. Lehrkräfte müssen in der Lage sein, die Fähigkeit zum kritischen Denken und die Medienkompetenz von Kindern und Jugendlichen sowie digitale Kompetenzen für eine sichere Nutzung sozialer Medien+ zu entwickeln.

Lehrkräfte sollten für das Risiko einer „Überdigitalisierung“ in Schulen sensibilisiert werden. Neue digitale Instrumente wie KI sollten gegebenenfalls für spezifische pädagogische Zwecke eingesetzt werden. Im Rahmen der Lehrerbildung sollte mit den Eltern eng zusammengearbeitet werden, um die gesunde und ausgewogene Bildschirmnutzung von Minderjährigen besser zu fördern, zu verstehen, wie Kinder und Jugendliche mit sozialen Medien und anderen digitalen Diensten umgehen, und altersgerechte Strategien zu entwickeln, um im Unterricht und zu Hause über Online-Risiken und -Erfahrungen zu sprechen.

EMPFEHLUNG 11**KI-Kompetenz als integralen Bestandteil der digitalen Bildung aufnehmen**

KI-Kompetenz sollte in die digitale Bildung in Schulen und anderen Einrichtungen der allgemeinen und beruflichen Bildung integriert werden. Minderjährige sollten die Chancen, Grenzen und Risiken im Zusammenhang mit KI-Technologien (d. h. KI-Chatbots/-begleiter, Empfehlungssysteme und generative KI) verstehen, einschließlich der Möglichkeit fehlerhafter Informationen, Manipulation und synthetischer Inhalte.

Die Förderung der Medienkompetenz könnte sich am Rahmen für KI-Kompetenzen in der Primär- und Sekundarschulbildung orientieren, der von der Europäischen Kommission und der OECD entwickelt wurde. Ohne entsprechende Aufsicht sollten Minderjährige keinen anthropomorphen KI-Begleitpersonen ausgesetzt werden, die menschenähnliche Beziehungen imitieren.

EMPFEHLUNG 12**Schulen sollten strukturierte Möglichkeiten zur Verbesserung der psychischen Gesundheit und des digitalen Wohlbefindens anbieten**

Schulen müssen eine aktive Rolle bei der Minderung von Risiken in den sozialen Medien+ spielen und sich für die geistige Gesundheit und das Wohlbefinden von Kindern und Jugendlichen einsetzen. Schulen sollten Informations- und Schulungsmöglichkeiten für Eltern sowie für Minderjährige gemeinsam mit ihren Eltern organisieren, um über Sicherheit im Internet, geistige Gesundheit und Wohlbefinden zu informieren.

Schulen sollten im Hinblick auf Probleme im Zusammenhang mit der Nutzung sozialer Medien+ durch Minderjährige den Zugang zu schulbasierter Beratung und anderen Unterstützungsleistungen im Bereich der psychischen Gesundheit ausweiten. Es sollten sichere, vor Stigmatisierung geschützte physische und digitale Räume zur Verfügung stehen, in denen Schülerinnen und Schüler das Gefühl haben, über Schwierigkeiten (z. B. psychische Gesundheit, Wohlbefinden usw.) sprechen zu können, die sie im Rahmen ihrer Nutzung sozialer Medien+ und ähnlicher Umgebungen erleben. Schulen sollten Zugang zu qualifizierten Fachkräften im Bereich der Gesundheitsberufe haben, einschließlich einer abgestuften Versorgung im Bereich der psychischen Gesundheit. Fachkräfte für psychische Gesundheit sollten spezielle Schulungen auf den Gebieten des digitalen Wohlbefindens und der Online-Gefahren erhalten.

Die Schulen sollten ferner zugängliche, vertrauliche und kindgerechte Meldemechanismen für Minderjährige, die online Problemen ausgesetzt sind, einrichten. Zur weiteren Stärkung des Schutzes sollten Schulen über Wege zur Weiterverweisung an externe Kinderschutzdienste, Dienste im Bereich der psychischen Gesundheit und spezialisierte Unterstützungsdienste verfügen.

EMPFEHLUNG 13**Bei bildungspolitischen Maßnahmen besonderes Augenmerk auf schutzbedürftige Gruppen legen**

Minderjährige, die mit sozioökonomischen Benachteiligungen, sonderpädagogischem Förderbedarf, negativen Kindheitserfahrungen, Diskriminierung oder psychischen Problemen konfrontiert sind, können erhöhten Risiken im Zusammenhang mit sozialen Medien ausgesetzt sein. Bildungs- und Unterstützungsmaßnahmen sollten inklusiv und gegebenenfalls gezielt ausgerichtet sein; ferner sollten sie so konzipiert sein, dass sie Ungleichheiten sowohl in den sozialen Medien als auch bei der digitalen Teilhabe und dem digitalen Wohlergehen verringern.

In Schulen könnten proaktive, gezielte Maßnahmen ergriffen werden, um den unverhältnismäßigen Auswirkungen von Online-Gefahren auf schutzbedürftige und marginalisierte Minderjährige zu begegnen und schutzbedürftige Gruppen unterstützen. Der gleichberechtigte Zugang zu Geräten, Konnektivität und technischen Hilfsmitteln sollte ausgeweitet werden und auch Kinder mit Behinderungen einschließen.

EMPFEHLUNG 14**In eine sichere, präventive, robuste und vertrauenswürdige digitale Bildungsinfrastruktur investieren**

Schulen benötigen sichere, robuste und vertrauenswürdige digitale Infrastrukturen und Instrumente, um die digitalen Kompetenzen Minderjähriger zu stärken und die digitale Souveränität Europas zu gewährleisten. Europäische Schulen sind in hohem Maße auf Anwendungen aus Drittländern angewiesen, wobei europäische Lösungen auf anhaltende Herausforderungen stoßen. Die EU sollte der Entwicklung und dem Einsatz sicherer, interoperabler digitaler Infrastrukturen und Tools für die Bildung Vorrang einräumen und diese unterstützen sowie strategische Abhängigkeiten verringern.

Danksagungen

Unsere Aufgabe als Ko-Vorsitzende und Sonderberater bestand darin, den vielschichtigen Prozess zu lenken und zu steuern, indem wir durch die Zusammenarbeit mit Expertinnen und Experten während der Sitzungen des Sonderausschusses Wissen zusammengetragen, bei Expertinnen und Experten Erkenntnisse gewonnen und den Austausch und Kontakt mit zahlreichen Interessenträgern gepflegt haben.

Dieser Bericht entstand dank des Engagements zahlreicher Menschen, die sich dafür einsetzen, dass Kinder und Jugendliche sich sicher in der Welt der sozialen Medien+ und darüber hinaus bewegen können. Zwar liegt die Verantwortung für die Empfehlungen ausschließlich bei uns, doch sind wir für die Beiträge anderer renommierter Sachverständiger, von Eltern- und Jugendvertretern und -vertreterinnen sowie der Europäischen Kommission äußerst dankbar.

Zuallererst möchten wir der Präsidentin der Europäischen Kommission, **Ursula von der Leyen**, für ihr stetiges Interesse und ihre Unterstützung für unsere Arbeit danken. Ihre Teilnahme und ihr Engagement bei den Sitzungen des Sonderausschusses unterstreichen ihr Engagement für die Sicherheit von Kindern im Internet und wurden von uns und allen Teilnehmenden sehr geschätzt. Wir danken der Präsidentin für ihr langjähriges Interesse und ihr Engagement für die Sicherheit von Kindern, die es ermöglichten, diese Arbeit durchzuführen und konkrete Empfehlungen für das Wohlergehen von Kindern und Jugendlichen in ganz Europa auszuarbeiten. Wir möchten auch dem Kabinettschef der Präsidentin, **Björn Seibert**, der den gesamten Prozess von Anfang an begleitete, und **Patricia Reilly**, Mitglied des Kabinetts der Präsidentin, für ihre beständige Unterstützung danken.

Darüber hinaus möchten wir allen Teilnehmenden der Sitzungen des Sonderausschusses danken. Wir sind allen dankbar, die uns zum Wohle der europäischen Jugend ihr umfangreiches Wissen, ihre Erfahrung und ihr Engagement zur Verfügung gestellt haben. Wir möchten **Julie Inman Grant**, der australischen eSafety-Kommissarin, und **Lucas Borges**, Fachbereichsleiter Regulierung bei der brasilianischen Datenschutzbehörde, unseren besonderen Dank dafür aussprechen, dass sie uns Einblicke und Erkenntnisse aus ihren Ländern zur Sicherheit von Kindern im Internet zur Verfügung gestellt haben.

Wir haben allen aufmerksam zugehört, doch wir sind allein für die Schlussfolgerungen dieses Berichts verantwortlich.

WIR DANKEN DEN TEILNEHMENDEN DES SONDERAUSSCHUSSES*:

* Liste nicht vollständig

- // **Ayata**, 15-jährige Vertreterin der EU-Plattform für die Beteiligung von Kindern
- // **Zuzanna**, 17-jährige Vertreterin der EU-Plattform für die Beteiligung von Kindern
- // **Kimmo Alho**, Psychologe und emeritierter Professor, Universität Helsinki
- // **Mehdi Arfaoui**, Soziologin, Commission nationale de l'informatique
- // **Leanda Barrington-Leach**, Exekutivdirektorin, 5Rights Foundation
- // **Gabriele Battimelli**, Botschafterin von „Better Internet for Kids+“ aus Italien
- // **Owen Bennett**, unabhängiger Sachverständiger für die Regulierung digitaler Technologien
- // **Elena Bozzola**, Kinderärztin und Mitglied des nationalen Rates der italienischen Gesellschaft für Kinderheilkunde
- // **Matthias Brand**, Professor und Leiter der Abteilung Allgemeine Psychologie, Universität Duisburg
- // **Urs Buscke**, leitender Rechtsreferent, Europäischer Verbraucherverband
- // **Ana Caballero**, Vorsitzende der Expertengruppe für einen besseren Schutz Minderjähriger im digitalen Bereich, Spanien
- // **Alex Cooney**, Geschäftsführerin und Mitbegründerin von CyberSafeKids
- // **Lies Craeynest**, Gründerin von KidsUnplugged
- // **Jutta Croll**, Vorsitzende der Stiftung Digitale Chancen
- // **María del Mar España Martí**, Direktorin der Plattform Control Z
- // **Sigge Eriksson**, Vorsitzende des Nationalen Rates schwedischer Kinder- und Jugendorganisationen
- // **Marina Fernández**, Präsidentin, Adolescència Lliure de mòbils
- // **Louise Flynn**, Assistenzprofessorin, Trinity College Dublin
- // **Tobiáš Bruno Galia**, tschechischer Kinder- und Jugendrat
- // **Catalina Goanta**, Dozentin für Privatrecht und Technologie, Universität Utrecht
- // **Konstantinos Karachalios**, Berater des Exekutivdirektors des IEEE und Vorstandsmitglied der 5Rights Foundation
- // **Maija Katkovska**, Leiterin des lettischen Safer-Internet-Zentrums
- // **Rasmus Kjedahl**, Direktor, Børns Vilkår

- // **Petra Kogelnig**, Generalsekretärin, Europäische Elternvereinigung
- // **Pavel Kordik**, Dozent, Tschechische Technische Universität
- // **Marta Gonçalves**, Botschafterin von „Better Internet for Kids+“ aus Portugal
- // **Beckett Leclair**, Leiter Technologie, 5Rights Foundation
- // **Sonia Livingstone**, Professorin für Sozialpsychologie, London School of Economics
- // **Aisling Maloney**, Nationaler Jugendrat Irlands
- // **Giovanna Mascheroni**, Professorin, Katholische Universität Mailand
- // **Helen Mason**, Exekutivdirektorin, Child Helpline International
- // **Elvira Mentzelioti**, Vorsitzende des griechischen nationalen Jugendrates
- // **Eva Möhler**, Vorsitzende und Chefärztin für Kinder- und Jugendpsychiatrie, Universität Saarland
- // **Alberto Monge Roffarello**, Assistenzprofessor, Politecnico di Torino
- // **Théo Mouhoud**, Kinderpsychiater, Hopitaux de Paris
- // **Servane Mouton**, Ärztin, Neurologin und Neuropsychologin
- // **Mie Oehlenschläger**, unabhängige Forscherin und Beraterin für KI, Ethik und öffentliche Ordnung
- // **James O'Higgins Norman**, Professor für Bildung und Gesellschaft, Dublin City University
- // **Maja Olszewska**, Botschafterin von „Better Internet for Kids+“ aus Polen
- // **Brian O'Neill**, emeritierter Professor, Technological University of Dublin
- // **Kerstin Paschke**, Fachärztin für Kinder- und Jugendpsychiatrie und Psychotherapie, Universitätsklinikum Hamburg-Eppendorf
- // **Leo Pekkala**, stellvertretender Direktor, Finnisches Institut für audiovisuelle Medien
- // **María Soledad Pera**, Assistenzprofessorin, TU Delft
- // **Tanja Petelin**, Assistenzprofessorin, Université de Poitiers
- // **Christoph Pieh**, Leiter der Abteilung Psychosomatische Medizin und Psychotherapie, Universität für Weiterbildung Krems
- // **Jessica Piotrowski**, Professorin, Universität Amsterdam
- // **Declan Qualter**, Praktikumsleiter und Doktorand am University College Dublin
- // **Kai Rannenber**g, Professor und Lehrstuhlinhaber für Mobile Business und multilaterale Sicherheit, Goethe-Universität Frankfurt

- // **Anna Schwabegger**, Vorsitzende des österreichischen Nationalen Jugendrates
- // **Judith Simon**, Professorin für Ethik in Informationstechnologien, Universität Hamburg
- // **Lore Sleeckx**, Europäische Jugenddelegierte, Flämischer Jugendrat
- // **Petr Slovak**, Assistenzprofessor für Mensch-Computer-Interaktion, King's College London
- // **Elisabeth Staksrud**, Professorin, Abteilung Medien und Kommunikation, Universität Oslo
- // **Sophie Stalla-Bourdillon**, Forschungsleiterin, Forschungsgruppe Recht, Wissenschaft, Technologie und Gesellschaft, VUB
- // **Argyris Stringaris**, klinischer Wissenschaftler und Vorsitzender, Kinder- und Jugendpsychiatrie, University College London
- // **Lisa Thorell**, Professorin, Abteilung für klinische Neurowissenschaften, Karolinska Institutet
- // **Hanne-Mari Schiøtz Thorud**, Physiologin und Professorin, Universität Südostnorwegen
- // **Piotr Toczyski**, Assistenzprofessor, APS Maria Grzegorzewska Universität
- // **Antonia Torrens**, Präsidentin, COFACE – Families Europe
- // **Martina Tóthová**, leitende Delegierte, Jugendrat der Slowakei
- // **Dimitris Tsalavos**, Jugendbotschafter von „Better Internet for Kids+“ aus Zypern
- // **Laura Vandenbosch**, Assistenzprofessorin und Direktorin des Media Psychology Lab, KU Leuven
- // **Sørine Vesth Rasmussen**, Beraterin für Kinderrechte und Technologiepolitik, Børns Vilkår
- // **Mieke Visser-Schuurman**, Direktorin für Kinderrechte und Kapazitätsaufbau, Eurochild
- // **Rareș Voicu**, Vorsitzender des Europäischen Jugendforums
- // **Alexandra Weilenmann**, Professorin am Fachbereich Angewandte IT, Universität Göteborg
- // **Niels Zagema**, niederländischer Jugendvertreter, Nationale Jeugdraad

Für uns war es entscheidend, nicht nur dafür zu sorgen, dass junge Menschen bei den Sitzungen des Sondergremiums beteiligt waren, sondern sie auch in die gemeinsame Erstellung dieses Berichts einzubeziehen. Deshalb möchten wir **Marta Gonçalves** danken, die nicht nur als Botschafterin von Better Internet for Kids+ aus Portugal an der Podiumsdiskussion teilgenommen, sondern auch an der Ausarbeitung dieses Berichts mitgewirkt hat.

Dieser Bericht wäre ohne die Unterstützung vieler Bediensteter der Europäischen Kommission nicht möglich gewesen.

Zunächst möchten wir IDEA und ihrem stellvertretenden Leiter **David Müller** für die freundliche Aufnahme und die ausgezeichneten Arbeitsbedingungen danken.

Unsere Arbeit wurde durch die Unterstützung eines engagierten Teams innerhalb IDEA enorm bereichert: Wir möchten uns bei **Undine Ruge** für die Begleitung und Unterstützung dieses Prozesses bedanken. Wir danken **Asen Dimitrov** sehr, der als leitender Koordinator der Ko-Vorsitzenden des Sonderausschusses für die Online-Sicherheit von Kindern unser zuverlässiger Ansprechpartner war. Er stand uns mit Rat und Tat zur Seite, sowohl in inhaltlicher als auch in verfahrenstechnischer Hinsicht, trieb die Umsetzung unserer Pläne voran, organisierte alle Sitzungen und den Austausch und übernahm die Koordinierung der Arbeit am Bericht innerhalb von IDEA sowie – gemeinsam mit Kolleginnen und Kollegen aus dem Generalsekretariat – auch innerhalb der Kommission.

Ohne die zusätzliche Unterstützung von IDEA wäre dieser Bericht nicht zustande gekommen: Wir danken **Thomas Hopkins**, der ein ausgezeichnete Redakteur der englischen Fassung des Berichts war, **Anna Magdalena Comploi**, die ihr Fachwissen, ihre Forschung und ihre Unterstützung an allen organisatorischen Fronten beisteuerte, sowie **Quinlan Rijks**, der an der Entwicklung der visuellen Darstellungen beteiligt war. Wir danken **Alexander Hempfing** für seine Analyse und **Yee-Sol Chang** und **Konrad Rose** für ihre Beteiligung.

Gemeinsam mit IDEA haben Kolleginnen und Kollegen des Generalsekretariats die Arbeit innerhalb der Kommission koordiniert und wertvolle Einblicke sowohl in den Prozess als auch in den Inhalt gegeben. Wir danken daher dem stellvertretenden Generalsekretär **Nils Behrndt** für seine Zeit und sein Engagement sowie **Nacira Boulehouat**, **Ioana-Maria Gligor**, **Alessandra Falcinelli**, **Tarik Draidj**, **Louis Dancourt** und **Armande Lorentz**.

Zunächst haben wir uns zum Ziel gesetzt, die bestehenden Rechtsvorschriften und Instrumente, die der EU und den Mitgliedstaaten der EU zum Schutz von Kindern und Jugendlichen im Internet zur Verfügung stehen, sowie deren bisherige Umsetzung besser zu verstehen. Dieser Kontext bot uns die Grundlage, um gemeinsam mit Expertinnen und Experten aktuelle Defizite und das weitere Vorgehen zu erörtern. Dafür danken wir der Leitung der GD CNECT und ihrem Generaldirektor **Roberto Viola** und ihrer stellvertretenden Generaldirektorin **Renate Nikolay** sowie der GD JUST und ihrer Generaldirektorin **Ana Gallego Torres** und ihrem stellvertretenden Generaldirektor **Hubert Gambs**.

Wir danken den Expertinnen und Experten der GD CNECT, die wertvolles Fachwissen und Erkenntnisse beigetragen haben: **Prabhat Agarwal**, **Julia Van Best**, **Martin Harris Hess**, **Andrea Tognoni**, **Manon Baert**, **Emma O'Mahony** und **Irene Roche Laguna**.

Wir danken den Expertinnen und Experten der GD JUST, die ebenfalls wertvolles Fachwissen und Erkenntnisse beigetragen haben: **Maria-Myrto Kanellopoulou**, **Benedicte Van Ormelingen**, **Denisa Alexandroaiei**, **Caoimhe Sheridan**, **Marie-Cécile Rouillon** und **Marta Kuljon**.

Dieser Bericht stützt sich ferner auf Forschungsergebnisse und Beiträge von Sachverständigen aus verschiedenen Dienststellen der Europäischen Kommission (JRC, GD SANTE, GD EAC, GD HOME, GD RTD, GD GROW, SJ und anderen): **Andrea Ceglia**, **Yves Punie**, **Marianne Takki**, **Martine Ingvorsen**, **Francesca Maltauro**, **Marta Touykova**, **Chiara Colella**, **Marta Markowska**, **Leonie Wahlmann**, **Katarzyna Janicka-Pawlowska**, **Veronica Travisani**, **Alessia Donna**, **Eva Gerhards**, **María del Pilar González Pantaleón**, **Amaryllis Verhoeven**, **Philipp Runge**, **Lorna Armati** und **Paul-John Loewenthal**.

Wir danken allen für das Einbringen ihrer Expertise und ihre Geduld bei der Beantwortung unserer unzähligen Fragen sowie für ihre Fähigkeit, komplexe rechtliche und technische Fragen zusammenzufassen und verständlich zu machen.

Wir danken auch den Expertinnen und Experten der GD COMM und des Generalsekretariats, die in Bezug auf Kommunikationsaspekte ausgezeichnete Unterstützung leisteten: **Chloe Lahousse Juarez, Anguel Konstantinov Beremliysky, Emma Kristina Kvennberg** und anderen. Unser Dank gilt auch den sehr kreativen und geduldigen Grafikdesignern und Übersetzungsexpertinnen und -experten: **Laurie Janssen, Camille Palandjian und Benedetta Benedetto** und anderen.

Unsere Arbeit wäre ohne die organisatorische Unterstützung zahlreicher Kolleginnen und Kollegen der Kommission bei den Sitzungen des Sonderausschusses, den Dienstreisen und anderen Treffen mit Interessenträgerinnen und -trägern nicht möglich gewesen: **Carmen Tresguerres, Rozaliya Petkova, Martina Gunda, Nuria Paredes, Alexandre Verin, Mariola De Las Heras Ojeda, Anne Catherine Louppe, Margarita Biacho Varela, Hafize Balci und Vaia Tsiampazi.**

Auch wir als Ko-Vorsitzende durften uns auf die Unterstützung unserer Heimatinstitutionen und unserer engsten Kooperationspartner in diesem Bereich verlassen:

Prof. Dr. Fegerts Team am Universitätsklinikum Ulm - **PD Dr. Franziska Köhler-Dauner, Juniorprofessorin Dr. Ann-Christin Haag, Emily Sitarski, Lena Peter, Karen Schlaegel, Claudia Rau, Annette Claus und Ariane Saccarello.**

Wir danken auch dem Team von Dr. Maria Melchior am Sorbonne Institut für öffentliche Gesundheit in Zusammenarbeit mit der Universität der Sorbonne und dem französischen Institut für Gesundheit und medizinische Forschung (INSERM): **Fabienne El Khoury, Camille Davisse-Paturet, Hamid Massoumi, Bertrand Redonnet und Mays Kabakibi.**

Endnoten

- 01.** Aries, P. (1962). Centuries of childhood: A social history of family life. Knopf Doubleday Publishing Group.
- 02.** Berk, L.E. (1994). Infants and Children Prenatal Through Early Childhood.
- 03.** Kessler, R. C., Magee, W. J. (1993). Childhood adversities and adult depression: basic patterns of association in a US national survey. *Psychological Medicine*, 23(3), 679–690.
- 04.** Taylor, G., Sala, G., Kolak, J., Gerhardstein, P., Lingwood, J. (2024). Does adult-child co-use during digital media use improve children's learning aged 0–6 years? A systematic review with meta-analysis. *Educational Research Review*, 44, 100614.
- 05.** Rideout, V. (2020). The Common Sense Census: Media Use by Kids Age Zero to Eight.
- 06.** Taylor, G., Sala, G., Kolak, J., Gerhardstein, P., Lingwood, J. (2024). Does adult-child co-use during digital media use improve children's learning aged 0–6 years? A systematic review with meta-analysis. *Educational Research Review*, 44, 100614.
Uhls, Y. T., Ellison, N. B., Subrahmanyam, K. (2017). Benefits and costs of social media in adolescence. *Pediatrics*, 140 (Supplement 2), S67–S70.
- 07.** Odgers, C. L., Jensen, M. R. (2020). Annual research review: Adolescent mental health in the digital age: Facts, fears, and future directions. *Journal of Child Psychology and Psychiatry*, 61(3), 336–348.
Nesi, J., Telzer, E. H., Prinstein, M. J. (2020). Adolescent Development in the Digital Media Context. *Psychological Inquiry*, 31(3), 229–234.
- 08.** Montag, C., Lachmann, B., Herrlich, M., Zweig, K. (2019). Addictive features of social media/messenger platforms and freemium games against the background of psychological and economic theories. *International journal of environmental research and public health*, 16(14), 2612.
- 09.** Steinberg, L. D. (2014). Age of opportunity: Lessons from the new science of adolescence. Houghton Mifflin Harcourt.
Casey, B. J., Getz, S., Galvan, A. (2008). The adolescent brain. *Developmental review*, 28(1), 62–77.
- 10.** Li, C., Cheng, G., Sha, T., Cheng, W., Yan, Y. (2020). The relationships between screen use and health indicators among infants, toddlers, and preschoolers: A meta-analysis and systematic review. *International Journal of Environmental Research and Public Health*, 17(19), 7324.
Teague, S., Somoray, K., Shatte, A. Miller, D., Moss, K., Crawford, A. et al. (2026). Digital Media Use and Child Health and Development. Deakin University. Journal contribution.
- Jing, X., et al. (2023). Effects of foreground screen media use on vocabulary development in young children: A meta-analysis. *Child Development*, 94(5), 1398–1415.
- 11.** Johnston MV. Neurotransmitters and vulnerability of the developing brain. *Brain Dev.* 1995 Sep-Oct;17(5):301-6.
- 12.** Ahmer, A., Raza, M., Azhar, M., Rahman, A., Das, J. K., Jafri, S. K. (2025). A systematic review and meta-analysis on the impact of screen-time on the social-emotional development of children under five years. *Journal of the College of Physicians and Surgeons Pakistan*, 35(3), 351–358.
Vasconcellos, R. P., Sanders, T., Lonsdale, C., Parker, P., Conigrave, J., Tang, S., Noetel, M. (2025). Electronic screen use and children's socioemotional problems: A systematic review and meta-analysis of longitudinal studies. *Psychological Bulletin*, 151(5), 513–543.
- 13.** Boxer, P., Groves, C. L., Docherty, M. (2015). Video games do indeed influence children and adolescents' aggression, prosocial behavior, and academic performance: A clearer reading of Ferguson (2015). *Perspectives on psychological science*, 10(5), 671–673.
Coyne, S. M., Radesky, J., Collier, K. M., Gentile, D. A., Linder, J. R., Nathanson, A. I., Rogers, J. (2017). Parenting and digital media. *Pediatrics*, 140(Supplement 2), S112–S116.
- 14.** Calvert, S. L. (2017). Parasocial relationships with media characters: Imaginary companions for young children's social and cognitive development. In *Cognitive development in digital contexts* (pp. 93–117). Academic Press.
Mallawaarachchi S., Burley J., Mavilidi M., et al (2024). Early Childhood Screen Use Contexts and Cognitive and Psychosocial Outcomes: A Systematic Review and Meta-analysis. *JAMA Pediatr.* 2024;178(10):1017–1026.
- 15.** Mallawaarachchi S., Burley J., Mavilidi M., et al (2024). Early Childhood Screen Use Contexts and Cognitive and Psychosocial Outcomes: A Systematic Review and Meta-analysis. *JAMA Pediatr.* 2024;178(10):1017–1026.
- 16.** Calvert, S. L. (2017). Parasocial relationships with media characters: Imaginary companions for young children's social and cognitive development. In *Cognitive development in digital contexts* (pp. 93–117). Academic Press.
Mallawaarachchi S., Burley J., Mavilidi M., et al (2024). Early Childhood Screen Use Contexts and Cognitive and Psychosocial Outcomes: A Systematic Review and Meta-analysis. *JAMA Pediatr.* 2024;178(10):1017–1026.

17. Taylor, G., Sala, G., Kolak, J., Gerhardstein, P., Lingwood, J. (2024). Does adult-child co-use during digital media use improve children's learning aged 0–6 years? A systematic review with meta-analysis. *Educational Research Review*, 44, 100614.
18. American Academy of Pediatrics (2024). Screen time guidelines. Center of Excellence on Social Media and Youth Mental Health.
19. Qian, H., Wang, C., Li, H. (2024). Parental risk factors and moderators of prolonged digital use in preschoolers: a meta-analysis. *Education and Information Technologies*, 29(13), 17601-17619. Jackson, D. B., Testa, A., Fox, B. (2021). Adverse childhood experiences and digital media use among US children. *American journal of preventive medicine*, 60(4), 462–470.
20. Li, C., Cheng, G., Sha, T., Cheng, W., Yan, Y. (2020). The relationships between screen use and health indicators among infants, toddlers, and preschoolers: A meta-analysis and systematic review. *International Journal of Environmental Research and Public Health*, 17(19), 7324. Ahmer, A., Raza, M., Azhar, M., Rahman, A., Das, J. K., Jafri, S. K. (2025). A systematic review and meta-analysis on the impact of screen-time on the social-emotional development of children under five years. *Journal of the College of Physicians and Surgeons Pakistan*, 35(3), 351–358.
21. Boichicchio, V., Keith, K., Montero, I., Scandurra, C., Winsler, A. (2022). Digital media inhibit self-regulatory private speech use in preschool children: The “digital bubble effect”. *Cognitive development*, 62, 101180.
22. Yang, C. C., Holden, S. M., Ariati, J. (2021). Social media and psychological well-being among youth: The multidimensional model of social media use. *Clinical child and family psychology review*, 24(3), 631–650. Vasconcellos, R. P., Sanders, T., Lonsdale, C., Parker, P., Conigrave, J., Tang, S., Noetel, M. (2025). Electronic screen use and children's socioemotional problems: A systematic review and meta-analysis of longitudinal studies. *Psychological Bulletin*, 151(5), 513–543.
23. Qian, H., Wang, C., Li, H. (2024). Parental risk factors and moderators of prolonged digital use in preschoolers: a meta-analysis. *Education and Information Technologies*, 29(13), 17601-17619. Jackson, D. B., Testa, A., Fox, B. (2021). Adverse childhood experiences and digital media use among US children. *American journal of preventive medicine*, 60(4), 462–470.
24. Madigan, S., Browne, D., Racine, N., Mori, C., Tough, S. (2019). Association between screen time and children's performance on a developmental screening test. *JAMA pediatrics*, 173(3), 244–250. Teague, S., Somoray, K., Shatte, A., Miller, D., Moss, K., Crawford, A. et al. (2026). Digital Media Use and Child Health and Development. Deakin University. Journal contribution.
25. Calvert, S. L. (2017). Parasocial relationships with media characters: Imaginary companions for young children's social and cognitive development. In *Cognitive development in digital contexts* (pp. 93–117). Academic Press. Marshall, S. J., Biddle, S. J., Gorely, T., Cameron, N., Murdey, I. (2004). Relationships between media use, body fatness and physical activity in children and youth: a meta-analysis. *International journal of obesity*, 28(10), 1238–1246.
26. Madigan, S., Browne, D., Racine, N., Mori, C., Tough, S. (2019). Association between screen time and children's performance on a developmental screening test. *JAMA pediatrics*, 173(3), 244–250. Mallawaarachchi S., Burley J., Mavilidi, M., et al (2024). Early Childhood Screen Use Contexts and Cognitive and Psychosocial Outcomes: A Systematic Review and Meta-analysis. *JAMA Pediatr.* 2024;178(10):1017–1026.
27. Korat, O., Shamir, A., Heibal, S. (2013). Expanding the boundaries of shared book reading: E-books and printed books in parent–child reading as support for children's language. *First language*, 33(5), 504–523. Taylor, G., Sala, G., Kolak, J., Gerhardstein, P., Lingwood, J. (2024). Does adult-child co-use during digital media use improve children's learning aged 0–6 years? A systematic review with meta-analysis. *Educational Research Review*, 44, 100614.
28. Kidron, B., Evans, A., Afia, J., Adler, J. R., Bowden-Jones, H., Hackett, L., Juj, A., Przybylski, A. K., Rudkin, A., Young Scot. (2018). Disrupted childhood: The cost of persuasive design. 5Rights Foundation. Stoilova, M., Bulger, M., Livingstone, S. (2024). Do parental control tools fulfil family expectations for child protection? A rapid evidence review of the contexts and outcomes of use. *Journal of Children and Media*. Chao, M., Lei, J., He, R., Jiang, Y., Yang, H. (2023). TikTok use and psychosocial factors among adolescents: Comparisons of non-users, moderate users, and addictive users. *Psychiatry Research*, 325, 115247.
29. Taylor, G., Sala, G., Kolak, J., Gerhardstein, P., Lingwood, J. (2024). Does adult-child co-use during digital media use improve children's learning aged 0–6 years? A systematic review with meta-analysis. *Educational Research Review*, 44, 100614. Zgambo, M., Anyango, E., Arabiat, D. H., Ngune, I., Mörelius, E., Zhang, M., Whitehead, L. C. (2025). Effect of Digital Safety Interventions on Parental Practices in Safeguarding Children's Digital Activities: Systematic Review and Meta-Analysis. *JMIR Pediatrics and Parenting*, 8(1), e70745.
30. Qian, H., Wang, C., Li, H. (2024). Parental risk factors and moderators of prolonged digital use in preschoolers: a meta-analysis. *Education and Information Technologies*, 29(13), 17601-17619. Jackson, D. B., Testa, A., Fox, B. (2021). Adverse childhood experiences and digital media use among US children. *American journal of preventive medicine*, 60(4), 462–470.

31. Yang, C. C., Holden, S. M., Ariati, J. (2021). Social media and psychological well-being among youth: The multidimensional model of social media use. *Clinical child and family psychology review*, 24(3), 631-650.
- Uhls, Y. T., Ellison, N. B., Subrahmanyam, K. (2017). Benefits and costs of social media in adolescence. *Pediatrics*, 140 (Supplement 2), S67-S70.
32. Teague, S., Somoray, K., Shatte, A. Miller, D., Moss, K., Crawford, A. et al. (2026). Digital Media Use and Child Health and Development. Deakin University. Journal contribution.
33. Vasconcellos, R. P., Sanders, T., Lonsdale, C., Parker, P., Conigrave, J., Tang, S., Noetel, M. (2025). Electronic screen use and children's socioemotional problems: A systematic review and meta-analysis of longitudinal studies. *Psychological Bulletin*, 151(5), 513-543.
34. Qian, H., Wang, C., Li, H. (2024). Parental risk factors and moderators of prolonged digital use in preschoolers: a meta-analysis. *Education and Information Technologies*, 29(13), 17601-17619.
- Jackson, D. B., Testa, A., Fox, B. (2021). Adverse childhood experiences and digital media use among US children. *American journal of preventive medicine*, 60(4), 462-470.
35. Qian, H., Wang, C., Li, H. (2024). Parental risk factors and moderators of prolonged digital use in preschoolers: a meta-analysis. *Education and Information Technologies*, 29(13), 17601-17619.
- Zgambo, M., Anyango, E., Arabiat, D. H., Ngune, I., Mörelus, E., Zhang, M., Whitehead, L. C. (2025). Effect of Digital Safety Interventions on Parental Practices in Safeguarding Children's Digital Activities: Systematic Review and Meta-Analysis. *JMIR Pediatrics and Parenting*, 8(1), e70745.
36. Calvert, S. L. (2017). Parasocial relationships with media characters: Imaginary companions for young children's social and cognitive development. In *Cognitive development in digital contexts* (pp. 93-117). Academic Press.
- Marshall, S. J., Biddle, S. J., Gorely, T., Cameron, N., Murdey, I. (2004). Relationships between media use, body fatness and physical activity in children and youth: a meta-analysis. *International journal of obesity*, 28(10), 1238-1246.
37. Böttger, T., Zierer, K. (2024). To ban or not to ban? A rapid review on the impact of smartphone bans in schools on social well-being and academic performance. *Education Sciences*, 14(8), 906.
38. Boztas, S. (2025, July 4). Smartphone bans in Dutch schools have improved learning, study finds. The Guardian.
39. Wedekind, K. (2026, March 11). So abgelenkt sind Schüler, wenn es kein Handyverbot gibt. n-tv.
40. Korat, O., Shamir, A., Heibal, S. (2013). Expanding the boundaries of shared book reading: E-books and printed books in parent-child reading as support for children's language. *First language*, 33(5), 504-523.
41. Calvert, S. L. (2017). Parasocial relationships with media characters: Imaginary companions for young children's social and cognitive development. In *Cognitive development in digital contexts* (pp. 93-117). Academic Press.
- Marshall, S. J., Biddle, S. J., Gorely, T., Cameron, N., Murdey, I. (2004). Relationships between media use, body fatness and physical activity in children and youth: a meta-analysis. *International journal of obesity*, 28(10), 1238-1246.
42. Purba, A. K., Thomson, R. M., Henery, P. M., Pearce, A., Henderson, M., Katikireddi, S. V. (2023). Social media use and health risk behaviours in young people: systematic review and meta-analysis. *bmj*, 383.
43. Nesi, J., Telzer, E. H., Prinstein, M. J. (2020). Adolescent Development in the Digital Media Context. *Psychological Inquiry*, 31(3), 229-234.
- Uhls, Y. T., Ellison, N. B., Subrahmanyam, K. (2017). Benefits and costs of social media in adolescence. *Pediatrics*, 140 (Supplement 2), S67-S70.
44. Schwartz, D., Zhang, M., Troop-Gordon, W., Taylor, L. M., Chung, J. (2025). Are social media use and popularity in the peer group linked during adolescence? A meta-analytic review. *Journal of Adolescence*, 97(3), 575-592.
45. Madigan, S., Browne, D., Racine, N., Mori, C., Tough, S. (2019). Association between screen time and children's performance on a developmental screening test. *JAMA pediatrics*, 173(3), 244-250.
- Teague, S., Somoray, K., Shatte, A. Miller, D., Moss, K., Crawford, A. et al. (2026). Digital Media Use and Child Health and Development. Deakin University. Journal contribution.
46. Children's Hospital of Philadelphia (2026). Age Limits Alone Won't Fix Smartphone Risks, Suggests Children's Hospital of Philadelphia Study. Accessed on 12 July 2026.
47. Vasconcellos, R. P., Sanders, T., Lonsdale, C., Parker, P., Conigrave, J., Tang, S., Noetel, M. (2025). Electronic screen use and children's socioemotional problems: A systematic review and meta-analysis of longitudinal studies. *Psychological Bulletin*, 151(5), 513-543.
- Teague, S., Somoray, K., Shatte, A. Miller, D., Moss, K., Crawford, A. et al. (2026). Digital Media Use and Child Health and Development. Deakin University. Journal contribution.
48. Nesi, J., Choukas-Bradley, S., Prinstein, M. J. (2018). Transformation of adolescent peer relations in the social media context: Part 1 – A theoretical framework and application to dyadic peer relationships. *Clinical child and family psychology review*, 21(3), 267-294.
- Uhls, Y. T., Ellison, N. B., Subrahmanyam, K. (2017). Benefits and costs of social media in adolescence. *Pediatrics*, 140 (Supplement 2), S67-S70.
49. Werling, A. M., Kuzhippallil, S., Emery, S., Walitza, S., Drechsler, R. (2022). Problematic use of digital media in children and adolescents with attention-deficit/hyperactivity disorder compared to controls: A meta-analysis. *Journal of Behavioral Addictions*, 11(2), 305-325.

50. Nesi, J., Telzer, E. H., Prinstein, M. J. (2020). Adolescent Development in the Digital Media Context. *Psychological Inquiry*, 31(3), 229–234.
Uhls, Y. T., Ellison, N. B., Subrahmanyam, K. (2017). Benefits and costs of social media in adolescence. *Pediatrics*, 140 (Supplement 2), S67–S70.
51. Orben, A., Przybylski, A. K. (2019). The association between adolescent well-being and digital technology use. *Nature Human Behaviour*, 3, 173–182.
52. Orben, A., Meier, A., Dalgleish, T., Blakemore, S. J. (2024). Mechanisms linking social media use to adolescent mental health vulnerability. *Nature Reviews Psychology*, 3(6), 407–423.
53. Vasconcellos, R. P., Sanders, T., Lonsdale, C., Parker, P., Conigrave, J., Tang, S., Noetel, M. (2025). Electronic screen use and children's socioemotional problems: A systematic review and meta-analysis of longitudinal studies. *Psychological Bulletin*, 151(5), 513–543.
54. Keles, B., McCrae, N., Grealish, A. (2020). A systematic review: The influence of social media on depression, anxiety and psychological distress in adolescents. *International Journal of Adolescence and Youth*, 25(1), 79–93.
Liu, M., Kamper-DeMarco, K. E., Zhang, J., Xiao, J., Dong, D., Xue, P. (2022). Time spent on social media and risk of depression in adolescents: A dose-response metaanalysis. *International Journal of Environmental Research and Public Health*, 19.
55. Orben, A., Meier, A., Dalgleish, T., Blakemore, S. J. (2024). Mechanisms linking social media use to adolescent mental health vulnerability. *Nature Reviews Psychology*, 3(6), 407–423.
56. Vasconcellos, R. P., Sanders, T., Lonsdale, C., Parker, P., Conigrave, J., Tang, S., Noetel, M. (2025). Electronic screen use and children's socioemotional problems: A systematic review and meta-analysis of longitudinal studies. *Psychological Bulletin*, 151(5), 513–543.
Qian, H., Wang, C., Li, H. (2024). Parental risk factors and moderators of prolonged digital use in preschoolers: a meta-analysis. *Education and Information Technologies*, 29(13), 17601–17619.
57. Yang, C. C., Holden, S. M., Ariati, J. (2021). Social media and psychological well-being among youth: The multidimensional model of social media use. *Clinical child and family psychology review*, 24(3), 631–650.
58. Vasconcellos, R. P., Sanders, T., Lonsdale, C., Parker, P., Conigrave, J., Tang, S., Noetel, M. (2025). Electronic screen use and children's socioemotional problems: A systematic review and meta-analysis of longitudinal studies. *Psychological Bulletin*, 151(5), 513–543.
59. Pagano, M., Bacaro, V., Crocetti, E. (2023). "Using digital media or sleeping... that is the question". A meta-analysis on digital media use and unhealthy sleep in adolescence. *Computers in Human Behavior*, 146, 107813.
Orben, A., Przybylski, A. K. (2019). The association between adolescent well-being and digital technology use. *Nature Human Behaviour*, 3, 173–182.
60. Orben, A., Meier, A., Dalgleish, T., Blakemore, S. J. (2024). Mechanisms linking social media use to adolescent mental health vulnerability. *Nature Reviews Psychology*, 3(6), 407–423.
61. Uhls, Y. T., Ellison, N. B., Subrahmanyam, K. (2017). Benefits and costs of social media in adolescence. *Pediatrics*, 140 (Supplement 2), S67–S70.
62. Orben, A., Meier, A., Dalgleish, T., Blakemore, S. J. (2024). Mechanisms linking social media use to adolescent mental health vulnerability. *Nature Reviews Psychology*, 3(6), 407–423.
63. Vasconcellos, R. P., Sanders, T., Lonsdale, C., Parker, P., Conigrave, J., Tang, S., Noetel, M. (2025). Electronic screen use and children's socioemotional problems: A systematic review and meta-analysis of longitudinal studies. *Psychological Bulletin*, 151(5), 513–543.
Teague, S., Somoray, K., Shatte, A., Miller, D., Moss, K., Crawford, A. et al. (2026). Digital Media Use and Child Health and Development. Deakin University. Journal contribution.
64. Vasconcellos, R. P., Sanders, T., Lonsdale, C., Parker, P., Conigrave, J., Tang, S., Noetel, M. (2025). Electronic screen use and children's socioemotional problems: A systematic review and meta-analysis of longitudinal studies. *Psychological Bulletin*, 151(5), 513–543.
65. Madigan, S., Browne, D., Racine, N., Mori, C., Tough, S. (2019). Association between screen time and children's performance on a developmental screening test. *JAMA pediatrics*, 173(3), 244–250.
Teague, S., Somoray, K., Shatte, A., Miller, D., Moss, K., Crawford, A. et al. (2026). Digital Media Use and Child Health and Development. Deakin University. Journal contribution.
66. Qian, H., Wang, C., Li, H. (2024). Parental risk factors and moderators of prolonged digital use in preschoolers: a meta-. *Education and Information Technologies*, 29(13), 17601–17619.
67. Pagano, M., Bacaro, V., Crocetti, E. (2023). "Using digital media or sleeping... that is the question". A meta-analysis on digital media use and unhealthy sleep in adolescence. *Computers in Human Behavior*, 146, 107813.
68. Odgers, C. L., Jensen, M. R. (2020). Annual research review: Adolescent mental health in the digital age: Facts, fears, and future directions. *Journal of Child Psychology and Psychiatry*, 61(3), 336–348.
Sala, A., Porcaro, L., Gómez, E. (2024). Social Media Use and adolescents' mental health and well-being: An umbrella review. *Computers in Human Behaviours Report*, volume 14.
69. Sala, A., Porcaro, L., Gómez, E. (2024). Social Media Use and adolescents' mental health and well-being: An umbrella review. *Computers in Human Behaviours Report*, volume 14.
70. Staksrud, E., Livingstone, S. (2009). Children and online risk. *Information, Communication and Society*, 12 (3).

71. Fegert, J.M. (2026). European child and adolescent psychiatry in a digital world. *European Child and Adolescent Psychiatry*, 35, 309–315.
72. WeProtect (2021). Estimates of childhood exposure to online sexual harms and their risk factors, p.5.
73. European Commission (2026). Action Plan against Cyberbullying.
74. Hamm, M. P., Newton, A. S., Chisholm, A., Shulhan, J., Milne, A., Sundar, P., Ennis, H., Scott, S. D., Hartling, L. (2015). Prevalence and effect of cyberbullying on children and young people: A scoping review of social media studies. *Journal of the American Medical Association Southeast Asia. Supplement. Pediatrics*, 169, 770–777.
Ronis, S., Slaunwhite, A. (2017). Gender and Geographic Predictors of Cyberbullying Victimization, Perpetration, and Coping Modalities Among Youth. *Canadian Journal of Psychology*, 34 (1).
75. European Commission (2021). Study to support the preparation of the European Commission's initiative to extend the list of EU crimes in Article 83 of the Treaty on the Functioning of the EU to hate speech and hate crime. Final report.
76. European Institute for Gender Equality (EIGE). 2026. Growing up online: how violence follows girls across platforms. Accessed on 29 June 2026.
77. Abendroth Dias, K., Arias Cabarcos, P., Bacco, F.M., Bassani, E., Bertoletti, A., et al. (2025). Generative AI Outlook Report – Exploring the Intersection of Technology, Society and Policy. Navajas Cawood, E., Vespe, M., Kotsev, A., van Bavel, R. (editors). Publications Office of the European Union, Luxembourg, JRC142598.
78. Ofcom. (2024). A deep dive into deepfakes that demean, defraud and disinform. Accessed on 29 June 2026.
79. Rousay, V. (2023). Sexual Deepfakes and Image-Based Sexual Abuse: Victim-Survivor Experiences and Embodied Harms. Master's thesis, Harvard University Division of Continuing Education.
80. Cataldo, I., Lepri, B., Neoh, M. J. Y., Esposito, G. (2021). Social Media Usage and Development of Psychiatric Disorders in Childhood and Adolescence: A Review. *Frontiers in Psychiatry*, 11.
81. McCrae, N., Gettings, S., Pursell, E. (2017). Social media and depressive symptoms in childhood and adolescence: A systematic review. *Adolescent Research Review*, Vol. 2, pp. 315–330.
82. Cataldo, I., Lepri, B., Neoh, M. J. Y., Esposito, G. (2021). Social Media Usage and Development of Psychiatric Disorders in Childhood and Adolescence: A Review. *Frontiers in Psychiatry*, 11.
83. Svensson, R., Johnson, B. Olsson, A. (2022). Does gender matter? The association between different digital media activities and adolescent well-being. *MC Public Health*, 10 (22), 273.
84. Svensson, R., Johnson, B. Olsson, A. (2022). Does gender matter? The association between different digital media activities and adolescent well-being. *MC Public Health*, 10 (22), 273.
85. Twenge J.M., Martin G.N. (2020). Gender differences in associations between digital media use and psychological well-being: Evidence from three large datasets. *Journal of Adolescence*, 79, 91-102.
86. Svensson, R., Johnson, B. Olsson, A. (2022). Does gender matter? The association between different digital media activities and adolescent well-being. *MC Public Health*, 10 (22), 273.
87. Dreßing, H., Hoell, A., Scharmann, L., Simon, A. M., Haag, A. C., Dölling, D., Meyer-Lindenberg, A., Fegert, J. M. (2025). Sexual Violence Against Children and Adolescents: A German Nationwide Representative Survey on Its Prevalence, Situational Context, and Consequences. *Deutsches Ärzteblatt International*, 122(11), 285.
88. Ronis, S., Slaunwhite, A. (2017). Gender and Geographic Predictors of Cyberbullying Victimization, Perpetration, and Coping Modalities Among Youth. *Canadian Journal of Psychology*, 34 (1).
89. Sala, A., Porcaro, L., and Gómez, E. (2024). Social Media Use and adolescents' mental health and well-being: An umbrella review. *Computers in Human Behaviours Report*, 14.
90. eSafety Commissioner (2025). How common are experiences of seeing online hate among children in Australia? Accessed 16 June 2026.
91. Kowalski, R.M., Limber, S.P., McCord, A. (2019). A developmental approach to cyberbullying: Prevalence and protective factors. *Aggression and Violent Behavior*, 45.
92. 5Rights Foundation (2020). Why digital platforms must be designed with LGBTQ children in mind. Accessed on 29 June 2026.
93. 5Rights Foundation (2020). Why digital platforms must be designed with LGBTQ children in mind. Accessed on 29 June 2026.
94. FRA (2024). LGBTIQ equality at a crossroads: Progress and challenges, p.72.
95. 5Rights Foundation (2020). Why digital platforms must be designed with LGBTQ children in mind. Accessed on 29 June 2026.
96. Ybarra, M.L., Mitchell, K.J., Palmer, N.A., Reisner, S.L. (2015). Online social support as a buffer against online and offline peer and sexual victimization among U.S. LGBT and non-LGBT youth. *Child Abuse Neglect*, 39.
97. Ronis, S., Slaunwhite, A. (2017). Gender and Geographic Predictors of Cyberbullying Victimization, Perpetration, and Coping Modalities Among Youth. *Canadian Journal of Psychology*, 34 (1).

98. Koch, T., Laaber, F., Florack, A. (2024). Socioeconomic status and young people's digital maturity: The role of parental mediation. *Computers in Human Behaviour*, 154.
Li, H., Luo, M., Duan, B., Kawulia, A., Su, M., Di, H. (2024). Family socioeconomic status and young children digital addiction: a moderated mediation model. *Frontiers in Psychology*, 27 (5).
99. Lu, Z. (2026). Mapping adolescent problematic social media use patterns across 41 countries/ regions: A multilevel latent class analysis with social determinants. *Addictive Behaviors*, 172.
Gracia, P., Fernandez-Urbano, R., Rubio-Cabañez, M., Celik, S., Cineli, B. (2026). World Happiness Report 2026. Chapter 7: Problematic social media use and adolescent wellbeing: the role of family socioeconomic status across 43 countries. Helliwell, J.F., Layard, R., Sachs, J. D., De Neve, J.-E., Aknin, L. B., Wang, S. (editors). Wellbeing Research Centre, University of Oxford.
100. Prkno, D., Grafe, N., Schulz, M.S., Kiess, W., Poulain, T. (2025). Children's and adolescents' negative internet experiences and the association with quality of life and behavioural difficulties: a cross-sectional study. *BMJ Paediatrics Open*, 17:9 (1).
101. Ofcom. (2022). Research into risk factors that may lead children to harm online.
102. Koch, T., Laaber, F., Florack, A. (2024). Socioeconomic status and young people's digital maturity: The role of parental mediation. *Computers in Human Behaviour*, 154.
103. World Happiness Report (2026). Chapter 7: Problematic social media use and adolescent wellbeing: the role of family socioeconomic status across 43 countries.
Lu, Z. (2026). Mapping adolescent problematic social media use patterns across 41 countries/ regions: A multilevel latent class analysis with social determinants. *Addictive Behaviors*, 172.
104. Ronis, S., Slaunwhite, A. (2017). Gender and Geographic Predictors of Cyberbullying Victimization, Perpetration, and Coping Modalities Among Youth. *Canadian Journal of Psychology*, 34 (1).
105. Hong, J.S., et al. (2016). Understanding the correlates of face-to-face and cyberbullying victimization among U.S. adolescents: A social-ecological analysis. *Violence and Victims*, 31(4), 638–663.
Thomas, A., Yeqing, L. (2025). Helping teens navigate online racism – study shows which parenting strategy works best.
106. FRA (2023). Online content moderation – Current challenges in detecting hate speech.
107. Bermudez-Villalva, A., Mehrnezhad, M., Toreini, E. (2025). Measuring Online Hate on 4chan using Pre-trained Deep Learning Models. *IEEE Transactions on Technology and Society*, 6 (2), June 2025.
108. FRA (2024). Being Muslim in the EU – Experiences of Muslims.
109. FRA (2023). Being Black in the EU – Experiences of people of African descent.
110. Council of Europe (2026). Hate speech levels across Europe alarming, stronger action needed. Accessed on 25 June 2026.
111. United Nations (2021). Report of the Special Rapporteur on minority issues, Fernand de Varennes. Human Rights Council, Forty-sixth session, 22 February–19 March 2021.
112. FRA (2022). Bias in Algorithms – Artificial Intelligence and Discrimination.
113. Ofcom. (2022). Research into risk factors that may lead children to harm online. p. 27.
114. eSafety Commissioner, 2023. A new playground: The digital lives of young people with disability.
Childlight Global Safety Institute (2023). The nature of online CSEA among children living with disabilities.
115. WeProtect (2025). How do we protect disabled young people from abuse and exploitation in digital spaces?
116. Childlight Global Safety Institute (2023). The nature of online CSEA among children living with disabilities.
117. eSafety Commissioner (2023). Young people with disability more likely to express themselves online despite higher rates of abuse.
118. eSafety Commissioner (2023). A new playground: The digital lives of young people with disability.
119. Werling, A.M., Kuzhippallil, S., Emery, S., Walitza, S., Drechsler, R. (2022). Problematic use of digital media in children and adolescents with a diagnosis of attention-deficit/hyperactivity disorder compared to controls. A meta-analysis. *Journal of Behavioral Addictions*, 11 (2).
120. Villar Onrubia, D., Barreda Angeles, M., Cachia, R., Economou, A., Lopez Cobo, M., (2025). Cyberbullying: Insights from science, policy and legislation. Publications Office of the European Union, Luxembourg, JRC144335.
121. Shou, Q., Yamashita, M., Mizuno, Y. (2025). Association of screen time with attention-deficit/hyperactivity disorder symptoms and their development: the mediating role of brain structure. *Translational Psychiatry*, 15:447.
122. eSafety Commissioner (2023). A new playground: The digital lives of young people with disability.
123. World Health Organization (2025). Mental health of adolescents. Accessed on 29 June 2026.
124. European Commission (2023). Flash Eurobarometer 530: Mental health.

125. World Health Organization (2025). Mental health of adolescents. Accessed on 29 June 2026.
126. World Health Organization (2025). Over a billion people living with mental health conditions – services require urgent scale-up. Accessed on 29 June 2026.
127. World Health Organization (2025). Suicide. Accessed on 16 June 2026:
128. OECD (2021). *Fitter Minds, Fitter Jobs: From Awareness to Change in Integrated Mental Health, Skills and Work Policies*. OECD Publishing, Paris.
129. Bertoni, E., Centeno, C., Cachia, R. (2025). Social media usage and adolescents' mental health in the EU. European Commission, Joint Research Centre (JRC), Ispra.
130. Bertoni, E., Centeno, C., Cachia, R. (2025). Social media usage and adolescents' mental health in the EU. European Commission, Joint Research Centre (JRC), Ispra.
131. Beullens, K., Bozzola, E., Cataldo, I., Hale, L., Kent, M., Montag, C., Nivins, S., O'reilly, M., Rubæk, L., Schiøtz Thorud, H.-M., Sterpenich, V., Vandenbosch, L. (2025). Minors' health and social media: an interdisciplinary scientific perspective. Manolios, S., Sala, A., Sundorph, E., Chaudron, S., Gomez, E. (editors), Publications Office of the European Union, Luxembourg. P.8.
132. Vidal, C., Lhaksampa, T., Miller, L., Platt, R. (2020). Social media use and depression in adolescents: A scoping review. *International Review of Psychiatry* (Abingdon, England), 32(3), 235-253.
133. Prkno, D., Grafe, N., Schulz, M.S., Kiess, W., Poulain, T. (2025). Children's and adolescents' negative internet experiences and the association with quality of life and behavioural difficulties: a cross-sectional study. *BMJ Paediatrics Open*, 17;9 (1).
134. Sarmiento, I., Olson, C., Yeo, G., Chen, Y., Toma, C., Brown, B., Bellmore, A., Mares, M. L. (2020). How does social media use relate to adolescents' internalizing symptoms? Conclusions from a systematic narrative review. *Adolescent Research Review*, 5, 381-404.
135. Sala, A., Porcaro, L., Gómez, E. (2024). Social Media Use and adolescents' mental health and well-being: An umbrella review. *Computers in Human Behavior Reports*, Vol 14. McCrae, N., Gettings, S., Pursell, E. (2017). Social media and depressive symptoms in childhood and adolescence: A systematic review. *Adolescent Research Review*, Vol 2, 315-330.
136. Li, H., Zhang, R., Lee, Y.C., et al. (2023). Systematic review and meta-analysis of AI-based conversational agents for promoting mental health and well-being. *NPJ Digital Medicine*, 6, 236.
137. Kooli, C., Chakraoui, R. (2025). AI-driven assistive technologies in inclusive education: benefits, challenges, and policy recommendations. *Sustainable Futures*, 10.
138. Unicef (2025). Guidance on AI and Children. Accessed on 29 June 2026.
139. Hudon, A., Stip, E. (2025) Delusional Experiences Emerging From AI Chatbot Interactions or "AI Psychosis". *JMIR Mental Health*, 3 (12). European Parliament (2026). The spread of AI companions and the challenges they generate. European Parliamentary Research Service (EPRS). Nature (2025). Can AI chatbots trigger psychosis? What the science says. Accessed on 16 June 2026.
140. Vice (2023). 'He Would Still Be Here': Man Dies by Suicide After Talking with AI Chatbot, Widow Says. Accessed on 16 June 2026.
141. Kurian, N. (2024). 'No, Alexa, no!': designing child-safe AI and protecting children from the risks of the 'empathy gap' in large language models. *Learning, Media and Technology*, 50.
142. Kurian, N. (2023). AI's empathy gap: the risks of conversational artificial intelligence for young children's well-being and key ethical considerations for early childhood education and care. *Contemporary Issues in Early Childhood*, 26(1), 132-139.
143. Commission nationale de l'informatique et des libertés (CNIL) (2026). L'impact des usages de l'AI sur la santé mentale des jeunes européens.
144. Ganapini, M., Panai, E. (2023). An Audit Framework for Adopting AI-Nudging on Children. Tech Ethics Lab.
145. Kurian, N. (2024). 'No, Alexa, no!': designing child-safe AI and protecting children from the risks of the 'empathy gap' in large language models. *Learning, Media and Technology*, 50.
146. Fegert, J. M. (2026). European child and adolescent psychiatry in a digital world. *European Child and Adolescent Psychiatry*, 35, 309-315.
147. Sala, A., Porcaro, L., Gómez, E. (2024). Social Media Use and adolescents' mental health and well-being: An umbrella review. *Computers in Human Behavior Reports*, Vol. 14.
148. Cataldo, I., Lepri, B., Neoh, M. J. Y., Esposito, G. (2021). Social Media Usage and Development of Psychiatric Disorders in Childhood and Adolescence: A Review. *Frontiers in Psychiatry*, 11.
149. Liu, L. (2024). Research on the relationship between virtual social interaction and the degree of loneliness based on algorithm matching technologies: A quantitative analysis on the SOUL APP-A virtual social software for strangers. *PLoS One*, 3:19.
150. eSafety Commissioner (2025). Online risks for children in your community. Accessed on 17 June 2026.
151. 5Rights Foundation (2021). Pathways: How digital design puts children at risk. p.5.

152. Cataldo, I., Lepri, B., Neoh, M. J. Y., Esposito, G. (2021). Social Media Usage and Development of Psychiatric Disorders in Childhood and Adolescence: A Review. *Frontiers in Psychiatry*, 11.
Bottaro, R., Faraci, P. (2022). The use of social networking sites and its impact on adolescents' emotional well-being: A scoping review. *Current Addiction Reports*, 9, 518–539.
153. Keles, B., McCrae, N., Grealish, A. (2020). A systematic review: The influence of social media on depression, anxiety and psychological distress in adolescents. *International Journal of Adolescence and Youth*, 25 (1), 79–93.
Ivie, E. J., Pettitt, A., Moses, L. J., Allen, N. B. (2020). A meta-analysis of the association between adolescent social media use and depressive symptoms. *Journal of Affective Disorders*, 275, 165–174.
154. Cataldo, I., Lepri, B., Neoh, M. J. Y., Esposito, G. (2021). Social Media Usage and Development of Psychiatric Disorders in Childhood and Adolescence: A Review. *Frontiers in Psychiatry*, 11.
155. Bozzola, E., Spina, G., Agostiniani, R., Barni, S., Russo, R., Scarpato, E., Di Mauro, A., Di Stefano, A. V., Caruso, C., Corsello, G., Staiano, A. (2022). The use of social media in children and adolescents: Scoping review on the potential risks. *International Journal of Environmental Research and Public Health*, 19.
156. Course-Choi, J., Hammond, L. (2021). Social media use and adolescent well-being: A narrative review of longitudinal studies. *Cyberpsychology, Behavior, and Social Networking*, 24, 223–236.
157. Consumer Science and Analytics (2022). Les adolescents et l'info. Research by Milan Presse and YouTube.
Notley, T., Zhong, H.F., Dezuanni, M., et al. (2023) Comparing children's and teens' news engagement practices and affective news experiences. *Journal of Youth Studies*, 26 (7): 878–893.
158. University of Southern Denmark (2025). Children and misinformation on social media. Accessed on 25 June 2026.
159. University of Southern Denmark (2025). Children and misinformation on social media. Accessed on 17 June 2026.
160. Calvin, A., Lenhart, A., Mann, S., and Robb, M. (2025). Teens, Trust, and Technology in the Age of AI: Navigating Trust in Online Content. *Common Sense Media*.
161. European Parliament (2025). Youth survey 2024.
162. Ali, S., DiPaola, D., Lee, I., et al. (2021). Children as creators, thinkers and citizens in an AI-driven future. *Computers and Education: Artificial Intelligence*, 2.
163. Howard, P.N., et al. (2021). Digital Misinformation / disinformation and children. UNICEF.
Melchior, C., Oliveira, M. (2024) A systematic literature review of the motivations to share fake news on social media platforms and how to fight them. *New Media and Society*, 26 (2): 1127–1150.
164. Howard, P.N., et al. (2021). Digital Misinformation / disinformation and children. UNICEF.
165. Ma, I., Mubashir, S., Kozyreva, A., van den Bos, W. (2025). Understanding the impact of misinformation on adolescents. *Nature Human Behaviour*, 10, 18–28.
166. NewsGuard (2021). Toxic TikTok: Popular social-media video app feeds vaccine misinformation to kids within minutes after they sign up. Accessed on 17 June 2026.
167. Ludwig-Walz, H., Bujard, M., Fegert, J.M., et al. (2025). Integrating European contexts and needs into WHO guiding principles on online mental health content for young people: Five recommendations. *European Child and Adolescent Psychiatry*, Vol. 34, 1221–1224.
168. Moss, C., Wibberley, C., Witham, G. (2023). Assessing the impact of Instagram use and deliberate self-harm in adolescents: A scoping review. *International Journal of Mental Health Nursing*, 32, 14–29.
169. World Health Organization (2025). Suicide worldwide in 2021: Global health estimates.
170. Arendt, F., Scherr, S., Romer, D. (2019). Effects of exposure to self-harm on social media: Evidence from a two-wave panel study among young adults. *New Media and Society*, Vol. 21 (11-12).
Nesi, J., et al. (2022). Social Media Use and Self-Injurious Thoughts and Behaviors: A Systematic Review and Meta-Analysis. *Clinical Psychology Review*, 8;87.
171. Nesi, J., et al. (2022). Social Media Use and Self-Injurious Thoughts and Behaviors: A Systematic Review and Meta-Analysis. *Clinical Psychology Review*, 8;87.
172. Memon, A. M., Sharma, S. G., Mohite, S. S., Jain, S. (2018). The role of online social networking on deliberate self-harm and suicidality in adolescents: A systematized review of literature. *Indian Journal of Psychiatry*, 60 (4).
173. Nesi, J., et al. (2022). Social Media Use and Self-Injurious Thoughts and Behaviors: A Systematic Review and Meta-Analysis. *Clinical Psychology Review*, 8;87.
174. Beullens, K., Bozzola, E., Cataldo, I., Hale, L., Kent, M., Montag, C., Nivins, S., O'reilly, M., Rubæk, L., Schiøtz Thorud, H.-M., Sterpenich, V., Vandenbosch, L. (2025). Minors' health and social media: an interdisciplinary scientific perspective. Manolios, S., Sala, A., Sundorph, E., Chaudron, S., Gomez, E. (editors), Publications Office of the European Union, Luxembourg.

175. Yue, C., Wenyao, G., Xudong, Y., Shuang, S., Zhuying, S., Yizheng, Z., Linlin, Z., Jinxin, C., Xingqi, W., Yujia, L. (2023). Dose-response relationship between daily screen time and the risk of low back pain among children and adolescents: A meta-analysis of 57831 participants. *Environmental Health and Preventive Medicine*, 28, 64–64.
176. American Optometric Association. (Undated). Computer vision syndrome (Digital eye strain). American Optometric Association. Accessed 29 June 2026. Thorud, H.-M. S., Aurjord, R., Falkenberg, H. K. (2021). Headache and musculoskeletal pain in school children are associated with uncorrected vision problems and need for glasses: A case-control study. *Scientific Reports*, 11(1). Thorud, H.-M. S., Mork, R., Bjørset, C. O., Gilson, S. J., Hagen, L. A., Langaas, T., Pedersen, H. R., Svarverud, E., Vikesdal, G. H., Baraas, R. C. (2022). Laboured reading and musculoskeletal pain in school children - the role of lifestyle behaviour and eye wear: A cross-sectional study. *BMC Pediatrics*, 22(1). Thorud, H.-M. S., Mudvari, P. R., Falkenberg, H. K. (2024). Academic performance and musculoskeletal pain in adolescents with uncorrected vision problems. *BMC Pediatrics*, 24(1).
177. Bozzola, E., Irrera, M., Hellmann, R., Crugliano, S., Fortunato, M. (2024). Media Device Use and Vision Disorders in the Pediatric Age: The State of the Art. *Children (Basel, Switzerland)*, 11(11).
178. Morningstar, B., Clayborne, Z., Wong, S.L., Roberts, K.C., Prince, S.A., Gariépy, G., Goldfield, G.S., Janssen, I., Lang, J.J. (2023). The association between social media use and physical activity among Canadian adolescents: a Health Behaviour in School-aged Children (HBSC) study. *Canadian Journal of Public Health*, 114(4): 642-650. Foreman, J., Salim, A.T., Praveen, A., Fonseka, D., Ting, D.S.W., Guang He, M., Bourne, R.R.A., Crowston, J., Wong, T.Y., Dirani, M. (2021). Association between digital smart device use and myopia: a systematic review and meta-analysis. *Lancet Digit Health*, 3(12). Ahmed, O., Walsh, E.I., Dawel, A., Alateeq, K., Espinoza Oyarce, D.A., Cherbuin, N. (2024) Social media use, mental health and sleep: A systematic review with meta-analyses. *Journal of Affective Disorders*, 15;367: 701-712. Purba, A.K., Thomson, R.M., Henery, P.M., Pearce, A., Henderson, M., Katikireddi, S.V. (2023) Social media use and health risk behaviours in young people: systematic review and meta-analysis. *BMJ*, 383.
179. Czeisler, C. A. (2015). Duration, timing and quality of sleep are each vital for health, performance and safety. *Sleep Health*, 1(1), 5–8. Matricciani, L., Paquet, C., Galland, B., Short, M., Olds, T. (2019). Children's sleep and health: A meta-review. *Sleep Medicine Reviews*, 46, 136–150. Short, M. A., Blunden, S., Rigney, G., Matricciani, L., Coussens, S., M Reynolds, C., Galland, B. (2018). Cognition and objectively measured sleep duration in children: A systematic review and meta-analysis. *Sleep Health*, 4(3), 292–300.
180. Wheaton, A. G., Claussen, A. H. (2021). Short Sleep Duration Among Infants, Children, and Adolescents Aged 4 Months-17 Years – United States, 2016-2018. *MMWR. Morbidity and Mortality Weekly Report*, 70(38). Gariépy, G., et al. (2020). How Are Adolescents Sleeping? Adolescent Sleep Patterns and Sociodemographic Differences in 24 European and North American Countries. *Journal of Adolescent Health*, 66 (6) Supplement.
181. Chang, A.M., Aeschbach, D., Duffy, J. F., Czeisler, C. A. (2015). Evening use of light-emitting eReaders negatively affects sleep, circadian timing, and next-morning alertness. *Proceedings of the National Academy of Sciences*, 112(4), 1232–1237. Hale, L., Guan, S. (2015). Screen time and sleep among school-aged children and adolescents: A systematic literature review. *Sleep Medicine Reviews*, 21, 50–58.
182. Tähkämö, L., Partonen, T., Pesonen, A.K. (2019). Systematic review of light exposure impact on human circadian rhythm. *Chronobiology International*, 36(2): 151-170.
183. Lund, L., Sølvhøj, I. N., Danielsen, D., Andersen, S. (2021). Electronic media use and sleep in children and adolescents in western countries: A systematic review. *BMC Public Health*, 21(1), 1598.
184. Mammeri, K., Riontino, L., Schwartz, S., Sterpenich, V. (2025). Influence of parental rules about screen electronic device use in the evening on sleep in adolescents. *Discover Public Health*, 22:517
185. Perrault, A. A., Bayer, L., Peuvrier, M., Afyouni, A., Ghisletta, P., Brockmann, C., Spiridon, M., Hulo Vesely, S., Haller, D. M., Pichon, S., Perrig, S., Schwartz, S., Sterpenich, V. (2019). Reducing the use of screen electronic devices in the evening is associated with improved sleep and daytime vigilance in adolescents. *Sleep*, 42(9). Bartel, K., Scheeren, R., Gradisar, M. (2019). Altering Adolescents' Pre-Bedtime Phone Use to Achieve Better Sleep Health. *Health Communication*, 34(4), 456–462.
186. World Health Organization. Regional Office for Europe (2024) A focus on adolescent social media use and gaming in Europe, central Asia and Canada: Health Behaviour in School-aged Children international report from the 2021/2022 survey.
187. Digital Services Act.
188. European Commission (2023). Consumer protection: manipulative online practices found on 148 out of 399 online shops screened.
189. Flayelle, M., et al. (2023). A taxonomy of technology design features that promote potentially addictive online behaviours. *Nature Reviews Psychology*, 2: 136–150. Perales, J.C., et al. (2020). Learning to lose control: A process-based account of behavioral addiction. *Neuroscience and biobehavioural reviews*, 108: 771-780.

190. van der Wal, A., Beyens, I., Janssen, L.H.C., Valkenburg, P.M. (2025). Diverse platforms, diverse effects: Evidence from a 100-day study on social media and adolescent mental health. *Current Psychology*, 45 (36).
191. Owenz, M., Freed, R. (2021). The ethics of persuasive design in technology used by children and adolescents. *Ethical Human Psychology Psychiatry*, 23, 89–99.
192. Andreassen, C.S., et al. (2016). The Relationship between Addictive Use of Social Media and Video Games and Symptoms of Psychiatric Disorders: A Large-Scale Cross-Sectional Study. *Psychology of Addictive Behaviors*. 30(2): 252–62.
193. European Commission (2024). Commission Staff Working Document Fitness Check on EU consumer law on digital fairness.
194. Saura, J.R., Palacios-Marqués, D., Iturricha-Fernández, A. (2021). Ethical design in social media: Assessing the main performance measurements of user online behavior modification. *Journal of Business Research*, 129.
195. United Nations (2021). General comment No. 25 (2021) on children's rights in relation to the digital environment. Committee on the Rights of the Child. European Commission (2025). Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28(4) of Regulation (EU) 2022/2065.
196. Curtis, B. L., Lookatch, S. J., Ramo, D. E., McKay, J. R., Feinn, R. S., Kranzler, H. R. (2018). Meta-Analysis of the Association of Alcohol-Related Social Media Use with Alcohol Consumption and Alcohol-Related Problems in Adolescents and Young Adults. *Alcoholism: Clinical and Experimental Research*, 42(6), 978–986. Vannucci, A., Simpson, E. G., Gagnon, S., Ohannessian, C. M. (2020). Social media use and risky behaviors in adolescents: A meta-analysis. *Journal of Adolescence*, 79(1), 258–274.
197. Beullens, K., Schepers, A. (2013). Display of alcohol use on Facebook: A content analysis. *Cyberpsychology, Behavior and Social Networking*, 16(7), 497–503. Vanherle, R., Hendriks, H., Beullens, K. (2023). Only for Friends, Definitely Not for Parents: Adolescents' Sharing of Alcohol References on Social Media Features. *Mass Communication and Society*, 26(1), 47–73. Vranken, S., Kurten, S., Beullens, K. (2024). Time to 'Wine': A Content Analysis Investigating How Social Media Influencers Refer to Alcohol Use in Instagram's Feed Posts and Stories. *Mass Communication and Society*, 27(6), 1468–1494.
198. Geusens, F., Beullens, K. (2018). The Association Between Social Networking Sites and Alcohol Abuse Among Belgian Adolescents: The Role of Attitudes and Social Norms. *Journal of Media Psychology*, 30(4), 207–216. Geusens, F., Beullens, K. (2021). Triple spirals? A three-wave panel study on the longitudinal associations between social media use and young individuals' alcohol consumption. *Media Psychology*, 24(6), 766–791. Vanherle, R., Hendriks, H., Beullens, K. (2023). Only for Friends, Definitely Not for Parents: Adolescents' Sharing of Alcohol References on Social Media Features. *Mass Communication and Society*, 26(1), 47–73.
199. Geusens, F., Beullens, K. (2018). The Association Between Social Networking Sites and Alcohol Abuse Among Belgian Adolescents: The Role of Attitudes and Social Norms. *Journal of Media Psychology*, 30(4), 207–216. Geusens, F., Beullens, K. (2019). A Longitudinal Examination of the Moderating Influence of Peer and Parental Socialization on Alcohol-Related Social Media Self-Effects Among Late Adolescents. *Media Psychology*, 22(2), 273–297. Geusens, F., Beullens, K. (2021). Triple spirals? A three-wave panel study on the longitudinal associations between social media use and young individuals' alcohol consumption. *Media Psychology*, 24(6), 766–791. Vanherle, R., Hendriks, H., Beullens, K. (2023). Only for Friends, Definitely Not for Parents: Adolescents' Sharing of Alcohol References on Social Media Features. *Mass Communication and Society*, 26(1), 47–73.
200. Geusens, F., Beullens, K. (2019). A Longitudinal Examination of the Moderating Influence of Peer and Parental Socialization on Alcohol-Related Social Media Self-Effects Among Late Adolescents. *Media Psychology*, 22(2), 273–297.
201. Rutherford, B.N., et al. (2025). #TurntTrending: a systematic review of substance use portrayals on social media platforms. *Addiction*, 8;118 (2).
202. Liu, J., Charmaraman, L., Bickham, D. (2024). Association between social media use and substance use among middle and high school-aged youth. *Substance Use and Misuse*, 59 (7).
203. Europol (2025). Europol coordinates operation against terrorist content online targeting minors. Accessed on 29 June 2026.
204. Europol (2026). 2025 Serious and Organised Crime Threat Assessment (SOCTA): The changing DNA of serious and organised crime.
205. Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., Hasebrink, U. (2020). EU Kids Online 2020: Survey results from 19 countries. EU Kids Online. Dreßing, H., Hoell, A., Scharmann, L., Simon, A. M., Haag, A. C., Dölling, D., Meyer-Lindenberg, A., Fegert, J. M. (2025). Sexual Violence Against Children and Adolescents: A German Nationwide Representative Survey on Its Prevalence, Situational Context, and Consequences. *Deutsches Ärzteblatt International*, 122(11), 285.
206. Chauviré-Geib, K., et al. (2025). The increase in online child sexual solicitation and abuse: Indicator 16.2.3 of the UN Sustainable Development Goals (SDG) documents a hidden and growing pandemic. Population-based surveys fail to capture the full

- picture. Child Abuse and Neglect, 164.
Dreßing, H., Hoell, A., Scharmann, L., Simon, A. M., Haag, A. C., Dölling, D., Meyer-Lindenberg, A., Fegert, J. M. (2025). Sexual Violence Against Children and Adolescents: A German Nationwide Representative Survey on Its Prevalence, Situational Context, and Consequences. Deutsches Ärzteblatt International, 122(11), 285.
- 207.** Internet Watch Foundation (2026). [2025 Internet Watch Foundation Annual Data and Insights Report](#).
- 208.** Insoll, T., Ovaska, A., Vaaranen-Valkonen, N. (2024). CSAM Users in the Dark Web: Protecting Children Through Prevention. Protect Children.
- 209.** Internet Watch Foundation (2026). 2025 Internet Watch Foundation Annual Data and Insights Report.
- 210.** Our Voice (2025) Survey for survivors of sexual violence in childhood – voices of the Nordic survivors.
- 211.** Haag, A. C., Bonanno, G. A., Chen, S., Herd, T., Strong-Jones, S., S, S., Noll, J. G. (2023). Understanding posttraumatic stress trajectories in adolescent females: A strength-based machine learning approach examining risk and protective factors including online behaviors. Development and Psychopathology, 35 (4).
- 212.** Chauviré-Geib, K., Fegert, J. M. (2023). Victims of Technology-Assisted Child Sexual Abuse: A Scoping Review. Trauma, Violence, & Abuse, 25(2).
- 213.** Haag, A. C., Bonanno, G. A., Chen, S., Herd, T., Strong-Jones, S., S, S., Noll, J. G. (2023). Understanding posttraumatic stress trajectories in adolescent females: A strength-based machine learning approach examining risk and protective factors including online behaviors. Development and Psychopathology, 35 (4).
- 214.** Chauviré-Geib, K., Fegert, J. M. (2023). Victims of Technology-Assisted Child Sexual Abuse: A Scoping Review. Trauma, Violence, & Abuse, 25(2).
- 215.** Haag, A. C., Bonanno, G. A., Chen, S., Herd, T., Strong-Jones, S., S, S., Noll, J. G. (2023). Understanding posttraumatic stress trajectories in adolescent females: A strength-based machine learning approach examining risk and protective factors including online behaviors. Development and Psychopathology, 35 (4).
Chauviré-Geib, K., Fegert, J. M. (2023). Victims of Technology-Assisted Child Sexual Abuse: A Scoping Review. Trauma, Violence, & Abuse, 25(2).
- 216.** Haag, A. C., Bonanno, G. A., Chen, S., Herd, T., Strong-Jones, S., S, S., Noll, J. G. (2023). Understanding posttraumatic stress trajectories in adolescent females: A strength-based machine learning approach examining risk and protective factors including online behaviors. Development and Psychopathology, 35 (4).
Chauviré-Geib, K., Fegert, J. M. (2023). Victims of Technology-Assisted Child Sexual Abuse: A Scoping Review. Trauma, Violence, & Abuse, 25(2).
- 217.** Chauviré-Geib, K., Gerke, J., Haag, A. C., Sachser, C., Finkelhor, D., Rassenhofer, M., Fegert, J. M. (2025). The increase in online child sexual solicitation and abuse: Indicator 16.2.3 of the UN Sustainable Development Goals (SDG) documents a hidden and growing pandemic. Child Abuse Neglect, 164.
- 218.** Eurostat (2025). [EU Terrorism Situation and Trend Report](#).
- 219.** Krahé, B., Möller, I., Huesmann, L.R., Kirwil, L., Felber, J., Berger, A. (2011). Desensitization to Media Violence: Links With Habitual Media Violence Exposure, Aggressive Cognitions, and Aggressive Behavior. Journal of Personality and Social Psychology, 100(4).
- 220.** Article 17 GDPR.
- 221.** European Data Protection Board (2022). [Guidelines 9/2022 on personal data breach notification under GDPR. Version 2](#).
- 222.** Schlegel, L., (2022). [Playing Against Radicalization: Why extremists are gaming and how P/CVE can leverage the positive effects of video games to prevent radicalization](#).
- 223.** European Commission (2023). [Understanding the value of a European video games society – Final report](#). Directorate-General for Communications Networks, Content and Technology (DG CNECT), ECORYS and KEA, section. 5.1.2.
Kowert, R., et al. (2026). Editorial: Extremism in games. Frontiers in Psychology, Vol. 16, p. 12.
- 224.** European Commission (2025). [The European media industry outlook – September 2025](#). Directorate-General for Communications Networks, Content and Technology (DG CNECT), p. 99.
- 225.** Radicalisation Awareness Network (2021). [Digital Grooming Tactics on Video Gaming & Video Gaming Adjacent Platforms: Threats and Opportunities – Conclusion paper](#).
- 226.** Brooks, G.A., Clark, L. (2019). Associations between loot box use, problematic gaming and gambling, and gambling-related cognitions. Addictive Behaviors, 96.
- 227.** Boniel-Nissim, M., Marino, C., Galeotti, T., Blinka, L., Ozoliņa, K., Craig, W., et al. (2024). [A focus on adolescent social media use and gaming in Europe, central Asia and Canada. Health Behaviour in School-aged Children international report from the 2021/2022 survey. Volume 6](#). WHO Regional Office for Europe.
- 228.** PEGI (2026). [PEGI expands age rating criteria with interactive risk categories](#). Accessed on 17 June 2026.
- 229.** OECD (2021). [Children in the digital environment – Revised typology of risks](#).
- 230.** Livingstone, S., Stoilova, M. (2021). The 4Cs: Classifying Online Risk to Children (1.0.0).
- 231.** European Commission, Joint Research Centre

232. Beullens, K., Bozzola, E., Cataldo, I., Hale, L., Kent, M., Montag, C., Nivins, S., O'reilly, M., Rubæk, L., Schiøtz Thorud, H.-M., Sterpenich, V., Vandenbosch, L. (2025). Minors' health and social media: an interdisciplinary scientific perspective. Manolios, S., Sala, A., Sundorph, E., Chaudron, S., Gomez, E. (editors), Publications Office of the European Union, Luxembourg.
233. Bursztyn, L., Duckworth, A., JiménezDurán, R., Leonard, A., Milojević, F., Roth, C., Sunstein, C. R. (2026). Why bans fail: Tipping points and Australia's socialmedia ban. (BFI Working Paper No. 202657). Becker Friedman Institute for Economics.
234. Article 28 DSA.
235. Articles 34 and 35 DSA.
236. Article 25 GDPR.
237. Article 6(1) GDPR.
238. Article 4(11) GDPR.
239. EDPB Guidelines 05/2020 on consent under Regulation 2016/679, pp. 62.
240. Case C-252/21, Meta v. Bundeskartellamt (ECLI:EU:C:2023:537), paragraph 106.
241. CJEU C-252/21 Bundeskartellamt, paragraph 111.
242. EDPB guidelines on legitimate interest, para 96.
243. EDPB Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, §54. Case C-252/21, Meta v. Bundeskartellamt (ECLI:EU:C:2023:537), paragraph 111.
244. EDPB Guidelines 8/2020 on the targeting of social media users, paragraph 16.
245. EDPB guidelines on legitimate interest, paragraph 95.
246. Article 17 and recital 65 GDPR.
247. Article 22 and recital 71 GDPR.
248. Recital 38 GDPR.
249. Article 29 Data Protection Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.
250. Article 35 and 36 GDPR.
251. European Commission (2026). Draft Commission guidelines on the classification of high-risk AI systems.
252. European Commission (2025). Commission publishes the Guidelines on prohibited artificial intelligence (AI) practices, as defined by the AI Act. Accessed on 2 July 2026.
253. European Commission (2026). The General-Purpose AI Code of Practice.
254. Article 50 AI Act.
255. European Commission (2026). Code of Practice on marking and labelling of AI-generated content.
256. European Commission (2026). Draft of the guidelines on the implementation of the transparency obligations for certain AI systems under Article 50 of the AI Act.
257. European Commission (2021). UCPD Guidelines.
258. Digital Fairness Fitness Check
259. European Commission (2026). Action Plan against Cyberbullying.
260. European Commission (2024). Commission Recommendation on developing and strengthening integrated child protection systems in the best interests of the child.
261. European Commission (2024). TikTok commits to permanently withdraw TikTok Lite Rewards programme from the EU to comply with the Digital Services Act. Accessed on 2 July 2026.
262. Article 82 DSA.
263. European Commission (2026). Commission preliminarily finds TikTok's addictive design in breach of the Digital Services Act. Accessed on 2 July 2026.
264. European Commission (2026). Commission preliminarily finds Pornhub, Stripchat, XNXX and XVideos in breach of the Digital Services Act for allowing minors to access their services. Accessed on 2 July 2026.
265. European Commission (2025). The European Board for Digital Services launches a coordinated action to reinforce the protection of minors as regards pornographic platforms. Accessed on 2 July 2026.
266. European Commission (2026). Commission preliminarily finds Meta in breach of Digital Services Act for failing to prevent minors under 13 from using Instagram and Facebook. Accessed on 2 July 2026.
267. European Commission (2026). Commission investigates Snapchat's compliance with child protection rules under the Digital Services. Accessed on 2 July 2026.
268. European Commission (2025). Commission accepts commitments offered by AliExpress under the DSA and takes further action. Accessed on 2 July 2026. European Commission (2026). Commission launches investigation into Shein under the Digital Services Act. Accessed on 2 July 2026. European Commission (2025). Commission preliminarily finds Temu in breach of the Digital Services Act. Accessed on 2 July 2026.
269. Authority for Consumers and Markets (2026). ACM launches investigation into Roblox in connection with risks that minors are facing. Accessed on 2 July 2026.
270. European Commission (2026). Commission investigates Grok and X's recommender systems under the Digital Services Act. Accessed on 2 July 2026.

271. European Commission (2026). Commission launches investigation into Shein under the Digital Services Act. Accessed on 2 July 2026.
272. European Commission (2024). Commission opens formal proceedings against Temu under the Digital Services Act. Accessed on 2 July 2026.
273. Article 53 AI Act.
274. Article 55 AI Act.
275. DLA Piper (2026). DLA Piper GDPR Fines and Data Breach Survey: January 2026.
276. Data Protection Commission (2023). Annual Report 2023.
277. Data Protection Commission (2023). Irish Data Protection Commission announces €345 million fine of TikTok. Accessed on 2 July 2026.
278. Data Protection Commission (2022). Data Protection Commission announces decision in Instagram Inquiry. Accessed on 2 July 2026.
279. Garante per la Protezione dei Dati Personali (2021). Provvedimento del 22 gennaio 2021.
280. Data Protection Commission (2026). Data Protection Commission opens investigation into X (XIUC). Accessed on 2 July 2026.
281. Art 15 EMFA.
282. European Commission (undated). Social media, online games and search engines. Accessed on 24 June 2026.
283. European Commission (undated). Social media, online games and search engines. Accessed on 24 June 2026.
284. European Commission (undated). Sweeps. Accessed on 24 June 2026.
285. European Commission (undated). Influencer Legal Hub. Accessed on 24 June 2026.
286. European Commission (undated). Social media, online games and search engines. Accessed on 24 June 2026.
287. Article 37 DSA.
288. Article 38 DSA.
289. FRA (2025). Towards Integrated Child Protection Systems – Challenges, promising practices and ways forward, p.79.
290. Popat, A., Tarrant, C. (2023). Exploring adolescents' perspectives on social media and mental health and well-being – A qualitative literature review. Special Issue: Social Media and Mental Health, 28 (1), p. 329.
291. Singleton, A., Abeles, P., Smith, I.C. (2016). Online social networking and psychological experiences: The perceptions of young people with mental health difficulties. Computers in Human Behavior, vol. 61.
292. Sala, A., Porcaro, L., and Gómez, E. (2024). Social Media Use and adolescents' mental health and well-being: An umbrella review. Computers in Human Behavior Reports, vol. 14, p. 8.
293. Sala, A., Porcaro, L., and Gómez, E. (2024). Social Media Use and adolescents' mental health and well-being: An umbrella review. Computers in Human Behavior Reports, vol. 14, p. 8.
294. Sala, A., Porcaro, L., and Gómez, E. (2024). Social Media Use and adolescents' mental health and well-being: An umbrella review. Computers in Human Behavior Reports, vol. 14, p. 8.
295. Sala, A., Porcaro, L., and Gómez, E. (2024). Social Media Use and adolescents' mental health and well-being: An umbrella review. Computers in Human Behavior Reports, vol. 14, p. 8.
296. Anderson, M., Vogels, E.A., Perrin, A., Lee, R. (2022). Connection, Creativity and Drama: Teen Life on Social Media in 2022. Pew Research Center. As cited in: Manolios, S., Chaudron, S., Fortuna, P., Sala, A., Gomez, E. (2026). Opportunities for young users on social media. European Commission, Joint Research Centre (JRC), Seville, JRC147510.
297. Sala, A., Porcaro, L., and Gómez, E. (2024). Social Media Use and adolescents' mental health and well-being: An umbrella review. Computers in Human Behavior Reports, vol. 14, p. 8.
298. Shankleman, M., Hammond, L., Jones, F.W. (2021). Adolescent Social Media Use and Well-Being: A Systematic Review and Thematic Meta-synthesis. Adolescent Research Review, vol. 6.
299. Shankleman, M., Hammond, L., Jones, F.W. (2021). Adolescent Social Media Use and Well-Being: A Systematic Review and Thematic Meta-synthesis. Adolescent Research Review, vol. 6.
300. Popat, A., Tarrant, C. (2023). Exploring adolescents' perspectives on social media and mental health and well-being – A qualitative literature review. Special Issue: Social Media and Mental Health, 28 (1), p. 329.
301. Hillmayr, D., Ziernwald, L., Reinhold, F., Hofer, S.I., Reiss, K.M. (2020). The potential of digital tools to enhance mathematics and science learning in secondary schools: A context-specific meta-analysis. Computers & Education, vol. 153.
302. Timotheou, S., Miliou, O., Dimitriadis, Y., Villagrà Sobrino, S., Giannoutsou, N., Cachia, R., Martínez Monés, A., Ioannou, A. (2022). Impacts of digital technologies on education and factors influencing schools' digital capacity and transformation: A literature review. Education and Information Technologies, vol. 28.
303. Forsström, S., Njå, M., Munthe, E., Houldsworth, L., Álvarez-Galván, J.-L. (2025). Key findings and integration strategies on the impact of digital technologies on students' learning: Results from a literature review. OECD Education Working Paper No. 336.

- Barrot, J.S. (2022). Social media as a language learning environment: A systematic review of the literature (2008-2019). *Computer Assisted Language Learning*, 35 (9).
- Zachos, G., Paraskevopoulou-Kollia, E.-A., Anagnostopoulos, I. (2018). Social Media Use in Higher Education: A Review. *Education Sciences*, 8 (4), Article 4.
- 304.** Forsström, S., Njå, M., Munthe, E., Houldsworth, L., Álvarez-Galván, J.-L. (2025). Key findings and integration strategies on the impact of digital technologies on students' learning: Results from a literature review. OECD Education Working Paper No. 336.
- 305.** Villar Onrubia, D., Cachia, R., Rietz, C., Feltrero, R., Niemi, H. et al. (2025). Generative Artificial Intelligence in secondary education – Uses and perceptions from the perspective of early adopters across five EU Member States. Luxembourg, JRC144345.
- Forsström, S., Njå, M., Munthe, E., Houldsworth, L., Álvarez-Galván, J.-L. (2025). Key findings and integration strategies on the impact of digital technologies on students' learning: Results from a literature review. OECD Education Working Paper No. 336.
- 306.** Villar Onrubia, D., Cachia, R., Rietz, C., Feltrero, R., Niemi, H. et al. (2025). Generative Artificial Intelligence in secondary education – Uses and perceptions from the perspective of early adopters across five EU Member States. Luxembourg, JRC144345.
- 307.** Villar Onrubia, D., Cachia, R., Rietz, C., Feltrero, R., Niemi, H. et al., (2025). Generative Artificial Intelligence in secondary education – Uses and perceptions from the perspective of early adopters across five EU Member States. Luxembourg, JRC144345.
- 308.** Timotheou, S., Miliou, O., Dimitriadis, Y., Villagrà Sobrino, S., Giannoutsou, N., Cachia, R., Martínez Monés, A., Ioannou, A. (2022). Impacts of digital technologies on education and factors influencing schools' digital capacity and transformation: A literature review. *Education and Information Technologies*, vol. 28.
- 309.** Crêteur, S., Dunajeva, J., Frydman, B., Berg Mulvik, I., Del Cogliano, D., Nada, C., Siarova, H., Sankalaite, S. (2026). Mobile phone bans in schools across the EU: ENESET analytical report. European Commission, Directorate-General for Education, Youth, Sport and Culture (DG EAC).
- 310.** European Commission (2026). Better Internet for Kids: Review of the year 2025. Accessed on 2 July 2026.
- 311.** European Commission (2026). Better Internet for Kids: Review of the year 2025. Accessed on 2 July 2026.
- 312.** European Commission (2024). International Computer and Information Literacy Study (ICILS) in Europe, 2023: Main findings and educational policy implications. Directorate-General for Education, Youth, Sport and Culture (DG EAC).
- 313.** European Commission (2025). Education and Training Monitor: Comparative Report. Chapter 2 – Young people's basic skills.
- 314.** European Commission (2026). The teaching profession in the EU – A comparative analysis building upon the TALIS 2024 results. Directorate-General for Education, Youth, Sport and Culture (DG EAC).
- 315.** Council conclusions on promoting and protecting the mental health of children and adolescents in the digital era.
- 316.** COFACE Families Europe (2026). Towards digital safety and well-being for children and their families: Moving beyond social media age restrictions as the sole solution.
- 317.** Council conclusions on promoting and protecting the mental health of children and adolescents in the digital era.
- 318.** European Commission (2025). Flash Eurobarometer survey: Future needs in digital education.
- 319.** European Commission (2026). New guidelines to help teachers lead Europe's digital education. Accessed on 1 July 2026.
- 320.** European Commission (2026). Guidelines for teachers and educators on tackling disinformation and promoting digital literacy through education and training. Directorate-General for Education, Youth, Sport and Culture (DG EAC).
- 321.** OECD / European Union (2026). Empowering Learners for the Age of AI: An AI Literacy Framework for Primary and Secondary Education. OECD Publishing, Paris.
- 322.** Commission Recommendation (EU) 2024/1238 of 23 April 2024 on developing and strengthening integrated child protection systems in the best interests of the child.
- 323.** Article 24 Charter of Fundamental Rights of the European Union.
- 324.** European Commission (2025). Call to Action: from children to EU decision-makers. Accessed on 1 July 2026.
- 325.** O'Connell, R. (2021). Psychological first aid for Young Peers. Training manual. IFRC Reference Centre for Psychosocial Support, Copenhagen.
- 326.** O'Connell, R. (2021). Psychological first aid for Young Peers. Training manual. IFRC Reference Centre for Psychosocial Support, Copenhagen.

- 327.** O'Connell, R. (2021). Psychological first aid for Young Peers. Training manual. IFRC Reference Centre for Psychosocial Support, Copenhagen.
- 328.** O'Connell, R. (2021). Psychological first aid for Young Peers. Training manual. IFRC Reference Centre for Psychosocial Support, Copenhagen.
- 329.** European Commission (Undated). Promising practices – Summary. Denmark – Psychological First Aid for Young Peers.
- 330.** European Commission (2024). Best Practices Portal – Psychological First Aid for Young Peers. Accessed on 1 July 2026.
- 331.** Seguranet (2026) Digital Leaders | SeguraNet. Accessed on 7 July 2026.



**Amt für Veröffentlichungen
der Europäischen Union**

Recht | Daten | Veröffentlichungen