Positionspapier

10. Februar 2026

Jugendschutz im digitalen Raum: Schutz durch Befähigung

Einleitung

Kinder und Jugendliche bewegen sich heute selbstverständlich im digitalen Raum. Für mehr als die Hälfte von ihnen sind Online-Dienste bereits ein fester Bestandteil des Alltags – Tendenz steigend[i]. Lernplattformen, soziale Netzwerke, kreative Plattformen, Gaming-Umgebungen und digitale Kommunikationsformen prägen längst ihr soziales, kulturelles und edukatives Leben. Mit der fortschreitenden Digitalisierung wächst zugleich die Erwartung, dass Online-Dienste sicher, vertrauenswürdig und verantwortungsbewusst gestaltet sind. Der Schutz Minderjähriger im Netz ist daher zu Recht ein zentraler Bestandteil der gesellschaftlichen und politischen Debatte. Dabei braucht es Lösungen, die nicht auf Abschottung oder Verbote setzen, sondern auf praktikable, nachhaltige und anschlussfähige Ansätze. Ein moderner Jugendmedienschutz muss Schutzbedarfe ernst nehmen, ohne Informationsfreiheit und Teilhabe einzuschränken.

Für den Bundesverband Digitale Wirtschaft (BVDW) e.V. ist der Schutz von Kindern und Jugendlichen im Netz von zentraler Bedeutung. Als Stimme einer verantwortungsvollen Digitalwirtschaft engagieren wir uns gemeinsam mit unseren Mitgliedern aktiv für einen starken Verbraucher*innenschutz und Maßnahmen, die eine sichere Teilhabe ermöglichen. Wir setzen uns für intelligente, praxistaugliche und zukunftsfähige Lösungen ein, weil wirksamer Jugendmedienschutz nur durch das Zusammenspiel von Verantwortung, Aufklärung und Innovation erreicht werden kann. Dazu gehören technische Schutzmechanismen, klare und einheitliche Rahmenbedingungen, eine zielgruppenorientierte Moderation sowie eine verantwortungsvolle Gestaltung von Websites und Apps. Ebenso zentral ist es, die digitalen und medialen Kompetenzen von Kindern, Jugendlichen und ihren Erziehungsberechtigten gezielt zu stärken. Entscheidend ist aus Sicht des BVDW, praktikable Lösungen zu schaffen, die – aufbauend auf Maßnahmen, Selbstregulierung und bestehenden Regulierung – einerseits Sicherheit gewährleisten und Risiken minimieren, andererseits aber auch Unternehmen die notwendige Gestaltungsfreiheit erlauben.

In diesem Positionspapier legt der BVDW daher seine Eckpunkte für einen wirksamen, praxistauglichen und zukunftsfähigen Jugendmedienschutz dar und zeigt auf, welche Rahmenbedingungen dafür notwendig sind.

Positionspapier

1. Rechtlicher Rahmen für Sicherheit im Netz

Der Schutz von Kindern und Jugendlichen ist eine zentrale staatliche Aufgabe, die sowohl völkerrechtlich verbindlich als auch verfassungsrechtlich verankert ist. Mit der Verabschiedung der UN-Kinderrechtskonvention im Jahr 1989 wurde der internationale Grundstein gelegt. Sie garantiert jungen Menschen umfassende Rechte auf Schutz (insbesondere Art. 17 UN-KRK) und Teilhabe (Art. 13 UN-KRK) und betont zugleich die Verantwortung der Eltern bei der Wahrnehmung dieser Rechte (Art. 18 UN-KRK). Auch das Grundgesetz verpflichtet den Staat in besonderer Weise. Art. 2 Abs. 2 GG schützt Leben und körperliche Unversehrtheit, während Art. 6 Abs. 2 GG die staatliche Wächterfunktion über das Kindeswohl festschreibt. Mit dem Aufkommen des Internets musste der Schutzrahmen gezielt angepasst und fortgeschrieben werden. Auf deutscher und europäischer Ebene ist seitdem ein differenzierter Rechtsrahmen entstanden, der den Schutz von Kindern und Jugendlichen im digitalen Raum ganzheitlich abdeckt. In Deutschland bilden unter anderem das Jugendschutzgesetz, der Jugendmedienschutz-Staatsvertrag und das Strafgesetzbuch zentrale Grundlagen.

Bislang ist der Jugendschutz in der EU bewusst national ausgestaltet. Damit wird den unterschiedlichen kulturellen, sprachlichen und institutionellen Gegebenheiten der Mitgliedstaaten Rechnung getragen. Zugleich zeigt sich insbesondere im digitalen Bereich zunehmend, dass rein nationale Regelungen im digitalen Binnenmarkt an ihre Grenzen stoßen. Daher sollten aus Sicht des BVDW bestehende Ansätze auf europäischer Ebene stärker verzahnt werden. Gemeinsame Leitlinien und Mindeststandards schaffen ein kohärentes Schutzniveau, verbessern die Risikominimierung und sorgen darüber hinaus für eine bessere Rechtssicherheit für europäische Unternehmen. Zugleich bleiben so Räume für flexible, praxisnahe Umsetzungen in den jeweiligen Mitgliedstaaten. Einen wichtigen Schritt hin zu einem europäischen Mindeststandard im digitalen Raum stellt der Digital Services Act dar. Mit ihm wurde der Jugendschutz erheblich gestärkt. Plattformen, die Minderjährigen zugänglich sind, werden nach Artikel 28 DSA verpflichtet, geeignete und verhältnismäßige Maßnahmen zu ergreifen, um ein hohes Maß an Sicherheit, Privatsphäre und Schutz sicherzustellen.

Der DSA kann dabei bei konsequenter Anwendung ein wirksames Mittel zum Schutz von Minderjährigen sein. Das zeigt das derzeit laufende und begrüßenswerte gemeinsame Vorgehen gegen Pornoplattformen. Dieses hat die EU-Kommission im Mai 2025 initiiert, während die Mitgliedstaaten koordiniert gegen kleinere Anbieter vorgehen. Im Fokus steht dabei der Schutz von Minderjährigen, insbesondere die fehlenden wirksamen Altersverifikationsmaßnahmen. Ergänzt wird dies durch die Verbesserung des Kinder- und Jugendschutzes im Netz durch die im Juli 2025 veröffentlichten Leitlinien zum Jugendschutz. Diese Leitlinien wurden im Rahmen des DSA (Artikel 28) von der EU-Kommission entwickelt. Sie konkretisieren das Gesetz mit einer Liste von Maßnahmen zum Schutz von Jugendlichen vor Risiken wie Grooming, schädlichen Inhalten, problematischem und süchtig-machendem Verhalten und schädlichen Geschäftspraktiken. Darüber hinaus hat die EU-Kommission auch einen Action Plan gegen Cybermobbing und Cyberbullying angestoßen. Solche Leitlinien und Aktionen sind von zentraler Bedeutung, da sie Unternehmen bei der konkreten Umsetzung des gesetzlichen Rahmens unterstützen, eine

einheitliche Interpretation gewährleisten und dadurch einen verlässlichen Schutzrahmen für Jugendliche im digitalen Raum schaffen.

2. Technologieneutralität bewahren und verhältnismäßige Altersverifikationslösungen ermöglichen

Der Schutz von Minderjährigen muss dort ansetzen, wo reale Gefahren drohen. Eine zentrale Forderung des Jugendmedienschutzes ist es daher berechtigterweise, den Zugang zu Inhalten zu beschränken, die für Kinder und Jugendliche ungeeignet sind. Dies trifft insbesondere klar definierte jugendgefährdende Inhalte, wie sie auch im Offline-Leben einer strikten Regulierung unterliegen. Die gängige Definition für jugendgefährdende Inhalte ergibt sich aus §18 Jugendschutzgesetz (JuSchG). Darunter versteht man Inhalte, welche als Gefährdung der Persönlichkeitsentwicklung von Kindern und Jugendlichen einzustufen sind.

Offline unterliegen jugendgefährdende Inhalte strengen Zugangsbeschränkungen und sind im Handel nur für Erwachsene erhältlich. Dazu gehören insbesondere pornografische und gewalthaltige Darstellungen, Angebote aus dem Bereich Glücksspiel oder Online-Casinos sowie Inhalte, die riskante oder potenziell gefährdende Verhaltensweisen zeigen oder bewerben. Auch Inhalte, die zur Teilnahme an kostenpflichtigen Online-Verträgen oder Finanzgeschäften animieren, zählen dazu. Der Grundsatz des Digital Services Act (DSA), dass alles, was offline illegal ist, auch online illegal sein muss, ist hier ein wichtiger Leitgedanke.

Aus Sicht des BVDW ist zur Erreichung des Ziels ein risikobasierter Ansatz entscheidend. Verpflichtende Altersverifikationen sollten dort eingesetzt werden, wo konkrete und hohe Gefahren für Minderjährige bestehen, wie z. B. bei den oben genannten pornografischen oder vergleichbar jugendgefährdenden Inhalten. In anderen Bereichen, in denen keine oder nur geringe Risiken vorliegen, sind alternative Schutzmaßnahmen wie altersgerechtes Design, kindgerechte Voreinstellungen (z. B. Privacy by Default für Minderjährige oder altersbasierte Zugangsbeschränkungen zu bestimmten Funktionen) oder elterliche Begleitfunktionen (Parental Controls) oft wirksamer und verhältnismäßiger. Dieser risikobasierte Ansatz entspricht auch dem Grundgedanken des DSA, was durch die Leitlinien des Europäischen Datenschutzausschusses zum Zusammenspiel des DSA mit der DSGVO betont wird. Zahlreiche Unternehmen der Digitalen Wirtschaft entwickeln hierfür bereits proaktiv technische, organisatorische und pädagogische Lösungen, nicht nur als Einzelunternehmen, sondern auch übergreifend.

Nach Artikel 28 und 34 DSA sollen Plattformen geeignete und verhältnismäßige Maßnahmen ergreifen, um Risiken für Minderjährige zu minimieren. Entscheidend ist dabei, dass redaktionelle Angebote und werbefinanzierte Plattformen, die sich nicht speziell an Kinder und Jugendliche richten, sondern ein Angebot für alle Altersschichten sind, nicht unbeabsichtigt durch pauschale Verifikationspflichten zu sehr benachteiligt werden. So sollten beispielsweise die Publisher mit ihren redaktionellen Angeboten auch künftig die Möglichkeit haben, Inhalte auf Grundlage datenschutzkonformer und verantwortungsvoller Werbeformen zu finanzieren. Ein risikobasierter Ansatz sollte daher berücksichtigen, dass sich die Gefährdungslage je nach Art des Angebots und Nutzerstruktur deutlich unterscheidet. Ist dann aufgrund der Bereitstellung ausschließlich

jugendgefährdender Inhalte eine Altersverifizierung angemessen und verhältnismäßig, ist die Umsetzung dieser Verifizierung entscheidend.

Derzeit existieren dazu zahlreiche Ansätze. Das Vereinigte Königreich etwa hat bereits im Rahmen des „Online Safety Act" eine verpflichtende Alterskontrolle für zahlreiche Plattformen eingeführt. Dieser Ansatz erweist sich in der Praxis jedoch als problematisch. Die Kontrollen können durch den Einsatz von VPN-Diensten trivial umgangen werden. VPN-Anbieter berichten von einem Anstieg um bis zu 1800 Prozent seit Einführung des Gesetzes[ii]. Gerade kostenlose VPN-Dienste, die von Jugendlichen bevorzugt genutzt werden, bergen eigene Risiken durch intransparente Datensammlungen. Darüber hinaus sind viele der dort eingesetzten Verfahren entweder datenschutzrechtlich bedenklich (siehe dazu auch Leitlinien des EDSA 3/2025 zum Zusammenspiel zwischen dem DSA und der DSGVO), diskriminierend (z. B. biometrische Ansätze) oder technisch wenig belastbar (z. B. Kreditkarten- oder Ausweisüberprüfungen, die leicht mit elterlichen Daten übergangen werden können). Die Skepsis zur Wirksamkeit und Datenschutzkonformität wird von der französischen CNIL[iii] und dem US-amerikanischen NIST[iv] bestätigt. Der europäische Weg unterscheidet sich bewusst hiervon. Der DSA schreibt keine konkrete Technologie vor, sondern verlangt Verfahren, die „genau, zuverlässig, robust und nicht-diskriminierend" sind. Dort wo die Altersverifikation dringend notwendig ist, darf sie nicht zu einem technischen Scheininstrument verkommen, das in der Praxis leicht zu umgehen ist und neue Gefahren für Datenschutz und Datensicherheit schafft. Sie sollte allerdings auch nur da eingesetzt werden, wo sie tatsächlich notwendig und wirksam ist und dort eben konsequent und verlässlich.

Entscheidend ist entsprechend, dass zukünftige Systeme technisch robust, datensparsam und nutzerfreundlich ausgestaltet werden. Eine zukunftsfähige Lösung liegt aus Sicht des BVDW in einem dualen Ansatz, der privatwirtschaftliche Innovation mit robuster öffentlicher Infrastruktur verbindet. Einerseits muss es Raum für innovative, privatwirtschaftliche Lösungen geben. Ohne praxisferne und bürokratische Hürden, aber mit nachvollziehbaren Mindestanforderungen, die Vertrauen schaffen und Missbrauch verhindern. Um Vertrauen, Sicherheit und Datenschutzkonformität sicherzustellen, könnten diese Lösungen nach bestimmten europäischen Mindeststandards entwickelt werden. Andererseits könnten perspektivisch europäische Lösungen wie die EU Digital Identity Wallet oder darauf basierende nationale eID-Systeme einen entscheidenden Beitrag als vertrauenswürdige Basisinfrastruktur bieten. Bis diese europäischen Systeme allerdings flächendeckend einsatzbereit sind, bleibt es entscheidend, auf Technologieneutralität zu setzen und unterschiedliche oder sich ergänzende Altersverifikationsmaßnahmen zu ermöglichen. Wichtig hierbei ist, dass auch Jugendliche, die noch kein amtliches Ausweisdokument haben, ohne große Barrieren digital partizipieren können. Gerade Teenager zwischen 13-15 Jahren dürfen hier nicht benachteiligt werden.

Darüber hinaus ist der kontinuierliche Austausch zwischen den verschiedenen Akteuren essenziell für die Entwicklung robuster und praxisnaher Lösungen. Gerade in der Phase der Lösungsfindung auf europäischer und nationaler Ebene müssen Unternehmen die Möglichkeit haben, sich aktiv einzubringen, um wirksame, verhältnismäßige und breitflächig einsetzbare Alternativlösungen gemeinsam zu entwickeln und zu etablieren.

3. Inhalte-Moderation und Verantwortung der Plattformen

Die Analyse der bisherigen Verfahren zeigt, dass Altersverifikationen wichtige und notwendige Instrumente für einen kohärenten Jugendschutz sein können. Entscheidend ist dabei ihr verhältnismäßiger Einsatz auf Basis eines risikobasierten Ansatzes sowie die Entwicklung technologieneutraler und datensparsamer Lösungen. Darüber hinaus braucht es allerdings auch Standards, wenn Kinder und Jugendliche online aktiv sind. So gibt es bestimmte Angebote für kindgerechte Inhalte, Videos oder Austauschformate. Gerade auf Plattformen mit hoher Reichweite und hoher Beteiligung von Kindern oder Jugendlichen wie sozialen Netzwerken sind zusätzliche Maßnahmen essenziell. Jugendschutz im digitalen Raum umfasst nicht nur den Schutz vor unerlaubtem Zugang, sondern auch vor schädlichen, unerwünschten und ausdrücklich für Erwachsene bestimmten Inhalten. Dazu sind auch die Plattformen in der Pflicht, Kinder und Jugendliche so weit wie möglich vor diesen Inhalten zu schützen.

Der Digital Services Act (DSA) schafft erstmals einen einheitlichen europäischen Rechtsrahmen für den Jugendschutz und etabliert damit Regeln für Sicherheit und Privatsphäre sowie sichere Meldewege und schützt vor bestimmten Inhalten im digitalen Raum. Viele Plattformen hatten bereits zuvor eigene Standards und Schutzmaßnahmen etabliert. Der DSA hat diese nun in verbindliche Regeln umgesetzt. Konkret verpflichtet der DSA Plattformen zum Ausschluss personalisierter Werbung für Minderjährige, die Bewertung und Minimierung von Risiken wie Manipulation oder Cybergrooming sowie den Zugangsschutz vor illegalen oder ungeeigneten Inhalten.

Kinder und Jugendliche werden höchstwahrscheinlich immer neue Wege finden, sich Zugang zu verbotenen Inhalten zu verschaffen. Auch hierauf muss der Jugendschutz eine Antwort haben. Deswegen ist die Umsetzung des DSA mit seinen „Trust & Safety"-Strukturen wie schnelle „Notice-and-Action"-Verfahren, niedrigschwellige und transparente Meldewege, nachvollziehbare Begründungen bei der Moderation und Entfernung von Inhalten sowie zugänglichen Beschwerdemechanismen ein wichtiger Baustein. Auch der im DSA verankerte Einsatz von „Trusted Flaggers" kann dabei helfen, Meldungen mit besonderem Gewicht effizient zu bearbeiten und kritische Inhalte zügiger zu entfernen. Entscheidend ist nicht allein das Verbot problematischer Inhalte, sondern auch die Geschwindigkeit und Qualität der Reaktion, wenn diese dennoch auftauchen.

Neben dem gesetzlichen Rahmen tragen auch die Plattformen selbst Verantwortung. Bereits heute existieren branchenweite Standards und Initiativen, die Orientierung bieten. Dazu gehören etwa der EU-Verhaltenskodex gegen Hassrede, der Code of Practice on Disinformation oder die „Alliance to Better Protect Minors Online". Auch nationale Systeme wie die Selbstkontrolleinrichtungen in Deutschland (FSK[v], FSM[vi], USK[vii]) dienen als Referenzpunkte.

Zu guter Letzt ist auch der Einsatz von neuen Technologien wie Künstliche Intelligenz notwendig, um die Prüfung und Filterung von Inhalten zunehmend effizienter zu machen, wodurch Plattformen ihre Schutzpflichten noch wirksamer erfüllen können. Durch die kontinuierliche Investition in KI-basierte, automatisierte Technologien können potenziell problematische Inhalte schneller erkannt und entfernt werden, bevor sie angesehen werden.

4. Digital- und Medienkompetenz konsequent weiter fördern

Auch die wirksamsten technischen Schutzsysteme und die strengsten Inhaltsmoderationen können keinen lückenlosen Schutz garantieren. Selbst bei konsequenter Aufsicht werden Kinder und Jugendliche mit problematischen Inhalten in Kontakt kommen können. Deshalb ist die Digital- und Medienkompetenz die unverzichtbare zweite Säule eines nachhaltigen Jugendschutzes. Digitale Kompetenzen befähigen junge Menschen, Risiken zu erkennen, diese kritisch einzuordnen und verantwortungsvoll mit digitalen Angeboten und Diensten umzugehen.

Die Förderung sollte frühestmöglich beginnen. Angesichts des sehr frühen Geräte- und Internetzugangs müssen bereits Vorschul- und Grundschulkinder altersgerecht an Themen wie Datenschutz, Cybersicherheit und den Umgang mit Informationen herangeführt werden. Kinder und Jugendliche müssen nicht nur über die Risiken der digitalen Welt informiert werden, sondern auch über ihre Chancen. Eine reflektierte Einschätzung digitaler Teilhabe bereitet sie auf zukünftige Arbeitsweisen, Technologien und Beteiligungsformen vor. Schulen tragen dabei eine herausragende Verantwortung: Medien- und Digitalkompetenz gehört verbindlich in den Unterricht, unterstützt durch eine gezielte Fortbildung der Lehrkräfte.

Dazu existieren bereits einige bewährte Programme und Initiativen. Nationale Projekte wie „Frag FINN“, „Deutschland sicher im Netz“, „klicksafe“ oder „SCHAU HIN!“ leisten wertvolle Beiträge zur Aufklärung. Auf europäischer Ebene bietet die Strategie „Better Internet for Kids+ (BIK+)“ einen wichtigen Rahmen, um Maßnahmen zu koordinieren, altersgerechtes Design zu fördern und europaweit eine gemeinsame Basis zu schaffen.

Neben der Verantwortung der jeweiligen Online-Angebote und Dienste, den Schulen und den Kindern und Jugendlichen selbst, stehen natürlich auch die Eltern oder Erziehungsberechtigten der Kinder in der Pflicht. Sie stehen vor der Herausforderung, ihren Kindern eine Welt verständlich zu machen, in der sie selbst nicht groß geworden sind. Eltern benötigen deswegen eine möglichst niedrigschwellige Orientierung, ein solides Grundverständnis sowie alltagstaugliche Werkzeuge, flankiert von der Bereitschaft, die Mediennutzung ihrer Kinder aktiv zu begleiten und mit Interesse zu verfolgen.

Medienkompetenz ist demnach immer ein Zweiklang aus Schutz und Befähigung. Ziel sollte nicht nur sein, Risiken zu reduzieren, sondern auch die Resilienz zu stärken und Teilhabe zu ermöglichen. Realistischer Jugendschutz muss daher technologische Maßnahmen mit Aufklärung, Begleitung und praktischen Alltagskompetenzen verbinden. Für einen sicheren, bewussten und chancengerechten Umgang mit digitalen Technologien.

5. Jugendschutz durch klare Grenzen und echte Teilhabe

Soziale Medien sind für Kinder und Jugendliche inzwischen zentraler Bestandteil gesellschaftlicher Teilhabe. Rund 92 Prozent der 6- bis 18-Jährigen nutzen soziale Netzwerke regelmäßig[viii]. Sie dienen nicht nur dem Austausch und der Identitätsentwicklung, sondern auch der politischen Bildung und der Möglichkeit, sich aktiv an gesellschaftlichen Prozessen zu beteiligen. Für marginalisierte Gruppen oder Minderheiten bieten digitale Plattformen oft die einzige Möglichkeit, in einer Weise zu partizipieren, die offline nur eingeschränkt zugänglich ist.

Anliegen, Probleme und Wünsche der Jugendlichen müssen auch digital von der jungen Generation vorgebracht werden können. Ihre Stimmen, die in der analogen Welt selten gehört werden, dürfen digital nicht verstummen. Altersdifferenzierte Zugänge auf soziale Medien können ein sinnvolles Instrument sein, um Jugendliche zu schützen. So können reduzierte Funktionen wie eingeschränkte Chat- und Kontaktmöglichkeiten, begrenzte Sichtbarkeit von Profilen oder strengere Voreinstellungen für Interaktionen dazu beitragen, Risiken wirksam zu reduzieren. Jüngere Nutzer*innen könnten in einem stärker abgesicherten Funktionsraum agieren, während ältere Jugendliche schrittweise mehr Autonomie erhalten. Diese Schritte müssen immer begleitet werden von transparenten Regeln und klaren Schutzmechanismen. Ziel muss es sein, Kinder und Jugendliche nicht auszuschließen, sondern ihnen innerhalb sozialer Medien sichere Entwicklungsräume bereitzustellen, die ihren jeweiligen Bedürfnissen und Risikolagen gerecht werden.

Kinder und Jugendliche brauchen daher einen sicheren Zugang zu sozialen Medien, damit sie ihre Teilhabe verantwortungsvoll wahrnehmen können. Sie müssen altersgerecht lernen, mit der digitalen Welt zu interagieren. In geschützten Räumen und im Dialog mit der Schule, den Eltern sowie Gleichaltrigen müssen Kinder und Jugendliche lernen, was man online glauben kann und was nicht. Deswegen sollte der Fokus nicht auf ein allumfassendes Verbot von Sozialen Medien liegen, sondern auf der Frage, wie wir Kindern und Jugendlichen Zugang zu diesen Schutzräumen ermöglichen. Entscheidend ist daher nicht der Ausschluss, sondern die Befähigung. Kinder und Jugendliche brauchen sichere Rahmenbedingungen, wirksame Schutzmechanismen und echte Mitgestaltungsmöglichkeiten. Nur so lässt sich ein Jugendschutz verwirklichen, der ihre Rechte wahrt, ihre Resilienz stärkt und ihre gesellschaftliche Teilhabe fördert.

Fazit

Ein wirksamer Jugendschutz im digitalen Raum muss Risiken minimieren und gleichzeitig echte Teilhabe ermöglichen. Kinder und Jugendliche sind heute selbstverständlich online. Politik, Gesellschaft und Wirtschaft stehen gemeinsam in der Verantwortung, für die Sicherheit von Kindern und Jugendlichen zu sorgen. Schutzmaßnahmen müssen praxisnah sein, ohne Innovation und Gestaltungsfreiheit zu ersticken. Es braucht daher einen rechtlichen Rahmen, der mit klaren Pflichten arbeitet, gleichzeitig aber auch Raum für Selbstregulierung und Verantwortung der Unternehmen sowie die Förderung von Medienkompetenz lässt. Damit dies gelingt, braucht es hierbei einen risikobasierten Ansatz:

Der bereits bestehende Rechtsrahmen in Deutschland und Europa bietet eine solide Grundlage. Der Digital Services Act stärkt den Schutz Minderjähriger europaweit durch klare Vorgaben zu Sicherheit, Privatsphäre und Inhaltsmoderation. Gleichzeitig zeigt sich: Jugendschutz darf nicht auf rigide Listen oder schnell veraltete Technologien setzen. Dort wo nötig, muss Altersverifikation technologieneutral, datenschutzfreundlich und praxistauglich gestaltet werden, um echten Schutz zu gewährleisten. Perspektivisch bieten europäische Lösungen wie die EU Digital Identity Wallet Chancen. Aktuell bleibt jedoch die Offenheit für unterschiedliche technische Ansätze entscheidend.

Positionspapier

Anbieter von digitalen Diensten und Angeboten selbst tragen eine zentrale Verantwortung, Inhalte angemessen zu moderieren und Kinder und Jugendliche vor schädlichen Angeboten zu schützen. Der DSA verpflichtet sie zu klaren Prozessen, schnellen Reaktionen und sicheren Meldewegen. Ergänzend sind branchenweite Standards und technische Innovationen, etwa durch KI, notwendig, um Risiken effektiv zu begegnen. Doch kein System kann allein verhindern, dass junge Menschen problematischen Inhalten begegnen.

Deshalb ist die Förderung von Digital- und Medienkompetenzen die zweite unverzichtbare Säule eines nachhaltigen Jugendschutzes. Kinder, Eltern, Schulen und Anbieter müssen hier gemeinsam Verantwortung übernehmen. Ziel darf nicht ausschließlich sein, Risiken zu reduzieren. Es muss auch darum gehen, Resilienzen zu stärken und Chancen zu eröffnen. Anstatt Ausschlüsse oder Verbote in den Vordergrund zu stellen, gilt es, Kinder und Jugendliche durch Schutzräume, Orientierung und echte Mitgestaltungsmöglichkeiten zu befähigen. Nur so gelingt ein Jugendschutz, der sowohl Sicherheit als auch gesellschaftliche Teilhabe gewährleistet. Wichtig bleibt: Jugendschutz ist kein statischer Endpunkt, sondern eine kontinuierliche, sich stets weiterentwickelnde Aufgabe aller Beteiligten.

Referenzen

[i] https://mpfs.de/studie/kim-studie-2024/
[ii] https://www.bbc.com/news/articles/cn72ydj70g5o
[iii] https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors
[iv] https://www.nist.gov/news-events/news/2024/05/nist-reports-first-results-age-estimation-software-evaluation
[v] Freiwillige Selbstkontrolle der Filmwirtschaft
[vi] Freiwillige Selbstkontrolle Multimedia-Diensteanbieter
[vii] Unterhaltungssoftware Selbstkontrolle
[viii] https://www.klicksafe.de/news/kinder-und-jugendliche-verbringen-taeglich-gut-zwei-stunden-am-smartphone