

Beantwortung des Fragenkatalogs durch die USK

Zum Hearing 2 – Technischer Jugendmedienschutz, Plattformgestaltung und Verantwortung digitaler Dienste – der Unabhängigen Expertenkommission „Kinder- und Jugendschutz in der digitalen Welt“

LEITFRAGE

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

***Die USK - Unterhaltungssoftware Selbstkontrolle** ist eine freiwillige Einrichtung der Games-Branche in Deutschland. Damit Kinder und Jugendliche sicher und altersgerecht an digitaler Spielkultur teilhaben können, prüft sie Games und versieht sie mit einem Alterskennzeichen. Im Bereich des JuSchG erteilen staatliche Vertreter*innen auf Empfehlung von unabhängigen Jugendschutzsachverständigen am Ende eines USK-Verfahrens die gesetzlichen Alterskennzeichen. Dabei bewertet die USK Spielinhalte und –mechaniken, die entwicklungsbeeinträchtigend sein könnten, und gibt zusätzlich Hinweise zu den Gründen für die jeweilige Alterskennzeichnung und vorhandenen Spielelementen. Die USK ist sowohl unter dem Jugendschutzgesetz des Bundes als auch unter dem Jugendmedienschutz-Staatsvertrag der Länder als zuständige Selbstkontrolle anerkannt. Zahlreiche Unternehmen haben sich der USK als Mitglieder angeschlossen, um beim Thema Jugendschutz dauerhaft und besonders eng zu kooperieren. Die USK ist zudem Mitgründerin des IARC-Systems (International Age Rating Coalition). Dieses wurde Anfang des letzten Jahres gemäß dem JuSchG als automatisiertes Bewertungssystem einer anerkannten Selbstkontrollereinrichtung durch die Obersten Landesjugendbehörden anerkannt.*

*Darüber hinaus engagiert sich die USK in der Medienbildung und ist unter anderem Mitherausgeberin des Elternratgebers und organisiert regelmäßig digitale Elternabende zum Thema Games und Jugendschutz. Die USK wird von einem Beirat beraten, der insbesondere das USK-Statut und die Leitkriterien für die Prüfungen festlegt. Dem Beirat gehören u.a. Vertreter*innen der zuständigen Ministerien von Bund und Ländern, der Medienaufsicht sowie weiterer Fachexperten an.*

Weitere Informationen: www.usk.de

Vorbemerkung:

Ein wirksamer Schutz von Kindern und Jugendlichen in digitalen Umgebungen setzt voraus, dass Regulierung die Lebenswirklichkeit junger Menschen ernst nimmt: Digitale Dienste sind heute alltägliche soziale, kulturelle und spielerische Räume, in denen Heranwachsende kommunizieren, sich ausdrücken, lernen und Gemeinschaft erfahren. Risiken entstehen dabei nicht isoliert im Bereich von einzelnen Inhalten oder Angebotstypen, sondern im Zusammenspiel von Angebotsgestaltung, Schutzmaßnahmen und Nutzungsszenarien. Entsprechend sollte der Jugendmedienschutz auch in der Zukunft nicht monolithisch, sondern **vielfältig, altersdifferenziert und risikoorientiert** gedacht werden.

Zentral ist dabei das **Verantwortungsdreieck aus Eltern, Anbietern und Staat**. Keine staatliche Regulierung kann Elternverantwortung ersetzen: „Pflege und Erziehung der Kinder [sind] das natürliche Recht der Eltern und die zuvörderst ihnen obliegende Pflicht“, da grundsätzlich davon auszugehen ist, dass das Wohl des Kindes am besten durch die Eltern verwirklicht wird (BVerfGE).¹ Demgegenüber tritt der staatliche Flankenschutz bzw. das staatliche Wächteramt grundsätzlich zurück. Erziehungsberechtigte bleiben die ersten und wichtigsten Bezugspersonen für Mediennutzung, Wertevermittlung und Schutzentscheidungen. Technische und rechtliche Instrumente entfalten ihre Wirkung nur dann, wenn sie in ein elterliches Erziehungs- und Begleitkonzept eingebettet sind. Deshalb ist es unerlässlich, dass Jugendmedienschutz nicht nur auf Verbote und Pflichten für Anbieter setzt, sondern Eltern in ihrer Rolle stärkt – durch Transparenz, verlässliche Alterskennzeichnungen wie die der USK, verständliche Schutzmaßnahmen und niedrigschwellige Unterstützung.

Gleichzeitig ist **Medienbildung eine unverzichtbare Säule des Jugendmedienschutzes**. Kinder und Jugendliche müssen befähigt werden, Risiken zu erkennen, Grenzen zu setzen, problematische Inhalte zu melden und eigene Nutzungsentscheidungen reflektiert zu treffen. In der digitalen Welt, ist Resilienz eine ebenso wichtige Schutzdimension wie technische Barrieren. Regulatorische Maßnahmen und pädagogische Kompetenzvermittlung müssen daher zusammengedacht werden.

Vor diesem Hintergrund braucht es **differenzierte, verhältnismäßige, regulatorische Antworten**, die der Vielfalt digitaler Dienste und der unterschiedlichen Gefährdungslagen gerecht werden. Ein pauschaler Ansatz wird der Vielfältigkeit der heutigen Medienangebote nicht gerecht. Entscheidend ist vielmehr eine **konkrete Gefahrenprognose**, die Eintrittswahrscheinlichkeit und Schadenspotenzial von Risiken ebenso berücksichtigt wie vorhandene strukturelle Vorsorgemaßnahmen eines Dienstes. Diese Grundgedanken sind bereits seit der Änderung des Jugendschutzgesetzes im Jahr 2021 verankert und werden im Rahmen der Alterskennzeichnung der USK bei digitalen Spielen bereits erfolgreich in der Praxis umgesetzt. Auch international zeigt sich, dass Deutschland mit diesem Ansatz eine Vorreiterrolle eingenommen hat.

Das System der **regulierten Selbstkontrolle**, wie es in Deutschland seit langem Bestand hat, hat sich bei der Inhaltebewertung aber auch zur Vermeidung von Verstößen gegen den Jugendmedienschutz als besonders wirksam erwiesen. Es verbindet staatlich gesetzte Schutzziele mit fachlich fundierter, unabhängiger Einzelfallprüfung und ermöglicht eine dynamische Anpassung an technische und gesellschaftliche Entwicklungen. Die USK bewertet digitale Spiele nicht nur nach ihren Inhalten, sondern –

¹ vgl. BVerfGE 24, 119 (150) = BVerfG NJW 1968, 2233; BVerfGE 76, 1 (51) = BVerfG NJW 1988, 626; BVerfGE 99, 145 (156) = BVerfG NJW 1999, 631; vgl. BVerfGE 99, 216 (232) = BVerfG NJW 1999, 557.

im Sinne eines modernen, risikoorientierten Jugendmedienschutzes – auch nach nutzungsbezogenen Risiken wie Kommunikationsfunktionen, Monetarisierungsmechanismen oder exzessiver Nutzung. Die rechtliche Grundlage hierfür bildet insbesondere § 10b Abs. 2 und 3 JuSchG.

Die folgenden Ausführungen zu einzelnen Risikokategorien sind daher nicht als isolierte Problemfelder zu verstehen, sondern als Teil eines integrierten Schutzkonzepts, das Anbieterpflichten, elterliche Verantwortung, pädagogische Befähigung und regulierte Selbstkontrolle miteinander verbindet. Für eine Vielzahl der Fragestellungen sind bereits konkrete Lösungen in der Umsetzung vorhanden, die in der Praxis eingesetzt werden. Nur durch dieses Zusammenspiel lässt sich ein nachhaltiger, wirksamer und zugleich verhältnismäßiger Jugendmedienschutz in digitalen Diensten gewährleisten.

I. Risiken, Schutzmaßnahmen und Gestaltung digitaler Dienste

1. Welche Maßnahmen sind aus Ihrer Sicht am wirksamsten, um die folgenden Risiken für Kinder und Jugendliche in digitalen Diensten zu verhindern, zu erschweren oder in ihren Folgen zu begrenzen:
 - a) digitale sexualisierte Gewalt (z.B. Cybergrooming, Sextortion, Missbrauchsdarstellungen),
 - b) suchtbegünstigende/hochgradig bindende Gestaltungspraktiken (z.B. Mikrotransaktionen, Lootboxen/Zufallsmechaniken, Dark Patterns),
 - c) Hate Speech, Desinformation sowie verschwörungsideologische und extremistische Inhalte,
 - d) Belästigung/Cybermobbing und weitere Interaktionsrisiken (z. B. Doxxing, Stalking, koordinierte Angriffe),
 - e) Selbstgefährdungsrisiken (z. B. Selbstschädigung/Suizid, Essstörungen, gefährliche Challenges),
 - f) kommerzielle Ausnutzung sowie Daten- und Privatsphäre-Risiken (z. B. Profiling/Tracking, irreführende Werbung, Scams)?

Aus Sicht der USK basiert ein wirksamer Jugendmedienschutz in digitalen Diensten auf dem **Verantwortungsdreieck zwischen Eltern, Anbietern und Staat**. In Deutschland sind die regulatorischen Vorgaben für Medienanbieter im internationalen Vergleich sehr tiefgreifend und umfassend. Der Paradigmenwechsel im Rahmen der letzten Novellierung des Jugendschutzgesetzes adressiert bereits eine Vielzahl dieser Thematiken – insbesondere im Bereich digitaler Spiele. Dabei hat sich ein **differenzierter und risikoorientierter Ansatz im Rahmen der regulierten Selbstregulierung als Konzept bewährt**. Im Rahmen der Altersbewertung werden nicht nur die Inhalte, sondern auch die nutzungsbezogenen Risiken systematisch geprüft. Entscheidend ist eine konkrete Gefahrenprognose im Einzelfall, bei der die Eintrittswahrscheinlichkeit und das Schadenspotenzial ebenso berücksichtigt werden wie vorhandene strukturelle Vorsorgemaßnahmen.

Für die unabhängige Gremienprüfung der USK unter staatlicher Beteiligung der Obersten Landesjugendbehörden der Länder stehen von den hier zu erörternden Risiken insbesondere zwei

Kategorien im Fokus: Risiken, die über Kommunikations- und Kontaktfunktionen entstehen, sowie Risiken, die durch exzessive Mediennutzung begünstigt werden. Die Einordnung der Risikosphären erfolgt dabei gemäß § 10b Abs. 3 JuSchG.²

Zu a), c), d): Gebündelte Risiken aufgrund von Kommunikations- und Kontaktfunktionen

Grundsätzlich gehören Kommunikations- und Kontaktfunktionen in digitalen Angeboten zu gelebten Nutzungspraktiken von Kindern und Jugendlichen und sind ein wesentlicher Bestandteil zeitgemäßer Jugendkultur sowie demokratischer Teilhabe. Aus Sicht der USK sind jedoch zur Prävention und Begrenzung digitaler sexualisierter Gewalt, Hate Speech, Desinformation sowie verschwörungsideologische und extremistische Inhalte, Belästigung/Cybermobbing und weiterer Interaktionsrisiken, sofern diese durch Kommunikations- und Kontaktfunktionen ausgelöst oder verstärkt werden, insbesondere folgende Maßnahmen³ wirksam:

- Einsatz von **Wortfiltern, Blockierfunktionen, Moderation** von Chats sowie Meldewegen für problematische oder grenzverletzende Inhalte,
- **Elterliche Begleittools** zur Einschränkung der Kommunikation auf ausgewählte Kontakte (z. B. Freundeslisten) sowie die Möglichkeit, Kommunikationsfunktionen vollständig zu deaktivieren,
- **Sensibilisierende Hinweise** wie „Chats“ oder „Erhöhte Kommunikationsrisiken“ im Rahmen der Alterskennzeichnung von digitalen Angeboten
- Berücksichtigung aller auf Plattformebene implementierten **Sicherheits- und Moderationsmechanismen**, sofern Kommunikation nicht unmittelbar im Spiel, sondern über die Plattform erfolgt,
- **Standardmäßig restriktive Einstellungen** zur Verhinderung der Weitergabe von Klarnamen, Standortdaten oder anderen kontaktrelevanten Informationen,
- Technische und gestalterische Maßnahmen, die das **Teilen persönlicher Daten** oder externer Kommunikationswege **verhindern** oder zumindest deutlich davor warnen,
- Sichtbare Integration von Informations- und Unterstützungsangeboten zur **Stärkung der Medienkompetenz** und zur Hilfe im Fall von Grenzverletzungen,
- **Keine spielmechanischen Belohnungen** oder **wiederholten Aufforderungen** zur **Preisgabe hochsensibler persönlicher Daten**, die eine Kontaktaufnahme oder missbräuchliche Nutzung erleichtern könnten.

Zu b) Risiken durch exzessive Mediennutzung

Phasen intensivierte Medien- und Spielverhaltens sind insbesondere in bestimmten Entwicklungsphasen des Kindes- und Jugendalters nicht ungewöhnlich und für sich genommen nicht automatisch problematisch oder pathologisch. Gleichwohl kann vorübergehend erhöhtes Spielverhalten bei bestimmten Ausgestaltungen digitaler Angebote durch gezielte Anreizmechaniken verstetigt oder verstärkt werden. Das aktuelle Jugendschutzgesetz adressiert bei der Bewertung

² Vgl. USK-Leitkriterien Abschnitt 5.3.

³ Vgl. USK-Leitkriterien S. 32f.

von digitalen Medien bereits Mechanismen, die eine exzessive Mediennutzung fördern können. Die USK prüft im Rahmen der Altersbewertung von digitalen Spielen Mechaniken, die Spieler*innen dazu verleiten, übermäßig lange zu spielen, unter dem Aspekt der „Exzessiven Mediennutzung“. Darunter fallen Mechanismen wie Push-Nachrichten, Season- oder Battle Passes, Lootboxen, Anreize zum Spielen zu bestimmten Zeitpunkten (Playing by Appointment, Wait to Play) oder Belohnungssysteme für häufiges und dauerhaftes Spielen, wie etwa Comeback-Geschenke, oder Sanktionen für Inaktivität (z. B. Verlust von Spielfortschritten oder Spielfiguren). Auch Belohnungen für das regelmäßige Einloggen können dabei relevant sein.⁴ Aus Sicht der USK sind zur Prävention und Begrenzung der Mechanismen, die eine exzessive Mediennutzung in digitalen Spielen fördern, insbesondere folgende Vorsorgemaßnahmen wirksam⁵:

- **Elterliche Begleittools zur Begrenzung** der Spielzeit, dem Deaktivieren von Push-Nachrichten oder der
- Deaktivierung bzw. **Einschränkung von Lootboxen** und Season- oder Battle Passes.

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

Gemäß der USK-Leitkriterien zur Alterskennzeichnung von digitalen Spielen sind konkrete Gestaltungsentscheidungen digitaler Spiele und deren Funktionalitäten dann jugendschutzrelevant, wenn sie die Selbststeuerungsfähigkeit von Kindern und Jugendlichen beeinflussen und dadurch erhebliche Risiken für die persönliche Integrität entstehen (§ 10b Abs. 3 JuSchG). Maßgeblich ist nicht die bloße Existenz einer Mechanik, sondern ob **dauerhaft im Spiel angelegte Funktionalitäten die geistig-seelische Integrität oder das psychische Wohlbefinden nachhaltig beeinträchtigen** können.

Solche Mechanismen können auf verschiedenen Ebenen der persönlichen Integrität wirken:

- **Psychische Integrität:** Beeinträchtigung der Identitätsfindung, inneren Autonomie oder individuellen Meinungsbildung durch übermäßige Anreize, Druckmechanismen oder manipulative Handlungsvorgaben.
- **Soziale Integrität:** Einfluss auf Geltungsansprüche in Gemeinschaften, Identitäts- und Beziehungsmanagement, etwa durch Ranglisten, Wettbewerbsdruck oder soziale Ausschlussmechanismen.
- **Dezisionale Integrität:** Einschränkung der Entscheidungsfreiheit oder kommerziellen Autonomie durch intransparente Kaufoptionen, Lootboxen, Pay-to-Progress-Mechanismen oder Glückspiel-Imitationen.
- **Sexuelle Integrität:** Gefährdung der sexuellen Selbstbestimmung durch ungesicherte Kommunikations- oder Sharing-Funktionen.

⁴ Vgl. USK-Leitkriterien S. 36.

⁵ Vgl. USK-Leitkriterien S. 37.

Die USK bewertet diese Risiken im Rahmen einer konkreten Gefahrenprognose, die Eintrittswahrscheinlichkeit und Schadenspotenzial individuell abwägt. Dabei wird geprüft, ob die Risiken unausweichlich mit dem Spiel verbunden sind oder durch wirksame strukturelle Vorsorgemaßnahmen begrenzt werden können.

Zentrale Vorsorgemaßnahmen sind:

- **Alterskennzeichen und Deskriptoren,**
- **Parental Controls,**
- **Kauf- und Spielzeitbeschränkungen,**
- **Melde- und Abhilfewege,**
- **Safety-by-Default-Einstellungen** sowie
- ggf. **Altersverifikationsmaßnahmen** in Hochrisikokontexten.

Diese Maßnahmen vermitteln Schutz, Orientierung und ermöglichen digitale Teilhabe, indem sie die Selbststeuerungsfähigkeit stärken und die Eintrittswahrscheinlichkeit belastender Situationen reduzieren. Ihre Angemessenheit, Wirksamkeit und Umgehungssicherheit fließen direkt in die Altersfreigabeentscheidung ein.

Erfahrungen aus der **USK-Spruchpraxis** zeigen, dass die systematische **Berücksichtigung solcher Mechanismen und Vorsorgemaßnahmen in der Praxis wirkt**: Laut USK-Jahresstatistik 2024 enthalten rund 30 % der geprüften Spiele mit Online-Funktionen potenzielle Nutzungsrisiken. In etwa einem Drittel dieser Fälle führten die Risiken zu einer höheren Altersfreigabe, wenn Vorsorgemaßnahmen unzureichend waren, z. B. bei Mechanismen, die exzessive Nutzung oder erhöhte Kaufanreize begünstigen. Gleichzeitig ermöglicht die Integration von Zusatzhinweisen Eltern und Erziehenden, die Risiken zu erkennen und durch elterliche Steuerung abzumildern.⁶

Diese Praxis zeigt, dass die präventive Risikobewertung digitaler Mechanismen, kombiniert mit wirksamen Vorsorgemaßnahmen und Alterskennzeichen, den Schutz der persönlichen Integrität von Kindern und Jugendlichen zuverlässig gewährleistet, ohne ihre digitale Teilhabe unverhältnismäßig einzuschränken.

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

-

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

Ein wirksamer Jugendmedienschutz sollte weiterhin darauf aufbauen, dass Kinder und Jugendliche altersgerecht an digitalen Angeboten teilhaben können. Um dies zu ermöglichen braucht es eine Verzahnung der folgenden Elemente:

- **Qualifizierte Risikobewertungen von digitalen Angeboten:** Prüfinstitutionen wie die USK oder andere Einrichtungen der freiwilligen Selbstkontrolle, die Inhalte und Mechanismen prüfen und mit einer entsprechenden Alterskennzeichnung versehen.

⁶ Vgl. USK-Jahresstatistik 2024, abrufbar unter: <https://usk.de/usk-jahresstatistik-2024/>.

- **Elterliche Begleittools:** Von anerkannten Einrichtungen der Freiwilligen Selbstkontrolle gemäß § 11 JMStV zertifizierte Jugendschutzprogramme, die in der Lage sind, diese Bewertungen auszulesen und Minderjährigen den Zugang damit altersgerecht ermöglichen.
- **Strukturelle Vorsorgemaßnahmen:** Von Anbieter*innen implementierte, geeignete und verhältnismäßige Maßnahmen zur Eindämmung von Risiken, um ein hohes Maß an Privatsphäre, Sicherheit und Schutz für Minderjährige auf ihren Diensten zu gewährleisten.

a) Qualifizierte Risikobewertungen von digitalen Angeboten

Alterskennzeichen gemäß Altersstufen im Bereich von digitalen Angeboten bilden zusammen mit ergänzenden Zusatzhinweise ein zentrales Element zur Orientierung im Bereich von Medieninhalten. Insbesondere dann, wenn sie **Inhalte**, Mechaniken und potenzielle **Nutzungsrisiken** sowie ihnen entgegenwirkend **Vorsorgemaßnahmen** berücksichtigen und sich an den gesetzlichen Altersstufen ausrichten.

Entsprechendes praktiziert die USK mit ihren Alterskennzeichnungen. Im Bereich des JuSchG erteilen staatliche Vertreter*innen der Obersten Landesjugendbehörden (OLJB) auf Empfehlung von unabhängigen Jugendschutzsachverständigen am Ende eines USK-Verfahrens die gesetzlichen Alterskennzeichen. Die Altersfreigabe stellt einen Verwaltungsakt dar. Die USK vergibt zudem als Mitgründerin des global genutzten und plattformgebundenen automatisierten Bewertungssystems IARC (International Age Rating Coalition) Alterskennzeichen. Das IARC-System wurde Anfang des letzten Jahres gemäß dem JuSchG als automatisiertes Bewertungssystem einer anerkannten Selbstkontrolleinrichtung durch die Obersten Landesjugendbehörden anerkannt.

Beide Kennzeichenverfahren und Kriterien fußen auf einer pluralen Einbindung, insbesondere von Industrie, Staat, Aufsicht und Wissenschaft und bilden dadurch eine einheitliche sowie hochaktuelle Spruchpraxis ab. Alterskennzeichen der Selbstkontrolleinrichtungen bilden somit ein besonders hohes Niveau an **Qualität** und **Wertigkeit** ab.

Alterskennzeichen ermöglichen es Eltern, Erziehenden und Pädagoginnen und Pädagogen somit, informierte Entscheidungen zu treffen, und erhöhen zugleich das Bewusstsein für Risiken bei Kindern. Als Indikatoren für die Wirksamkeit dienen insbesondere Rückmeldungen von Eltern und Nutzerinnen und Nutzern zur Verständlichkeit der Alterskennzeichen und zu deren Nutzung im Alltag.⁷

b) Elterliche Begleittools: Durch Selbstkontrollen zertifizierte Jugendschutzprogramme

Die Nutzung von elterlichen Begleittools bei der Mediennutzung ist ein zentraler Schlüssel für einen wirksamen Jugendmedienschutz. Durch Selbstkontrollen zertifizierte Jugendschutzprogramme sind Systeme, die einer anerkannten Einrichtung der freiwilligen Selbstkontrolle vorgelegt wurden und deren Eignung gemäß § 11 JMStV zertifiziert wurde. Sie bündeln Vorsorge, auslesbare Alterskennzeichen und Umgehungskontrollen in einem anerkannten und überprüfbaren System.

⁷ USK-Elternbefragung 2023/2024, abrufbar unter: <https://usk.de/pressemitteilung-4-von-5-eltern-setzen-beim-jugendschutz-in-games-auf-alterskennzeichen-der-usk/>.

Solche Programme sind besonders geeignet, eine sichere Teilhabe zu ermöglichen und die persönliche Integrität (psychisch, sozial, dezisional, sexuell) zu schützen. Sie reduzieren Risiken, ermöglichen altersgerechten Zugang zu klassifizierten Inhalten und schränken das elterliche Erziehungsprivileg nicht über Gebühr ein (Art. 6 Abs. 2 GG).

Indikatoren für Wirksamkeit sind insbesondere die Bedeutung der internationalen Plattformen und Angebote, die selbst entsprechende Programme nutzen oder dafür sorgen, dass Angebote durch solche Programme gefiltert oder wirksam im Zugang beschränkt werden können (z. B. Nintendo Switch, Xbox).

c) Strukturelle Vorsorgemaßnahmen

Vorsorgemaßnahmen sind Schutzvorkehrungen, die dazu bestimmt sind, Risiken für die persönliche Integrität von Kindern und Jugendlichen, die im Rahmen der Nutzung entstehen können, zu minimieren. Um diesen Schutz zu erreichen, muss den im jeweiligen Angebot bestehenden Risiken im Einzelfall hinreichend begegnet werden bzw. die Schutzvorkehrungen angemessen und wirksam sein.⁸ Vorsorgemaßnahmen einschließlich sicherer Voreinstellungen zum Jugendschutz ermöglichen Kindern und Jugendlichen eine selbstbestimmte, unbeschwerter Teilhabe und befähigen sie durch eine stufenweise Erweiterung der Angebote nach und nach zu einem verantwortungsvollen Umgang.⁹

Indikatoren für Wirksamkeit sind insbesondere die Auswirkung auf die Altersstufe bzw. Altersfreigabe bei Spielen mit enthaltenen angemessenen und wirksamen Vorsorgefunktionen, durch welche das Risiko zur Beeinträchtigung der persönlichen Integrität wirksam gemindert werden kann.

Die Wirksamkeit von Maßnahmen sollte sich an einer **nachweisbaren Reduktion relevanter Risiken** messen lassen, etwa an der Verringerung problematischer Interaktionen oder von Zugriffen auf nicht altersgerechte Inhalte. Zentrale Indikatoren sind dabei die praktische Wirksamkeit von Filtern, funktionierende Melde- und Abhilfeprozesse sowie die Stabilität der Maßnahmen gegen Umgehung. Ergänzend ist die **Einbindung von Kindern, Jugendlichen und Eltern** in Feedback- und Evaluationsprozesse, etwa durch Nutzerbefragungen oder partizipative Reviews, von besonderer Bedeutung. Querschnittlich sollte die Evaluation risikobasiert, regelmäßig und transparent erfolgen. Entscheidend ist dabei nicht die einzelne Maßnahme, sondern ihr **Zusammenspiel** und ihr nachweisbarer Beitrag zu Schutz, Befähigung und altersangemessener Teilhabe.

⁸ Vgl. USK-Leitkriterien S. 11.

⁹ Vgl. USK-Leitkriterien S. 5.

II. Plattformverantwortung, Regulierung und Durchsetzung

1. Wie sollte die Verantwortung der Plattformbetreiber gegenüber Kindern und Jugendlichen rechtlich und praktisch konkretisiert werden (z.B. Sorgfaltspflichten, Risikoanalysen, Melde- und Abhilfewege, Transparenzpflichten)?
2. Wie lässt sich die Verantwortung der Plattformbetreiber überprüfbar ausgestalten (z.B. Audits, Reporting, unabhängige Aufsicht, Beteiligung von Kindern und Zivilgesellschaft)?
3. Wie kann die Umsetzung bestehender Vorschriften – insbesondere der Vorgaben zum Schutz Minderjähriger nach Artikel 28 DSA samt Leitlinien der Kommission – sowie des JMStV und JuSchG verbessert werden?
4. Gibt es aus Ihrer Sicht Regelungslücken im Bereich des technischen Kinder- und Jugendmedienschutzes, und welche Instrumente wären geeignet, diese wirksam zu schließen?

Zu 1.-4.)

Art. 28 DSA verpflichtet Plattformbetreiber zu „geeigneten und verhältnismäßigen Maßnahmen“ zum Schutz Minderjähriger. Die Leitlinien der Kommission konkretisieren diese Vorgaben, ersetzen jedoch keine fachliche Bewertung im Einzelfall, etwa in Abhängigkeit von Risiko, Dienstyp oder Nutzungsszenario.

Nationale Einrichtungen der regulierten Selbstregulierung, wie die USK, sind weiterhin essentiell, um die Leitlinien praxisnah auf den deutschen Jugendmedienschutzkontext zu übertragen und konkrete Alters- und Zugangsregelungen zu prüfen. **Selbstkontrollleinrichtungen** wie die USK schaffen eine dauerhafte Verbindung zwischen staatlicher Aufsicht, fachlicher Expertise, Wirtschaft und Gesellschaft, berücksichtigen kulturelle und regulatorische Rahmenbedingungen, fördern Rechtsklarheit, sichern Qualitätsstandards im Vollzug und gewährleisten eine praxisnahe Umsetzung gesetzlicher Schutzpflichten in einem dynamischen Umfeld.

Bei der USK erfolgt dies z. B. durch:

- Die Kontinuierliche Einbindung staatlicher Strukturen sowie verschiedener gesellschaftlicher Akteure, u.a. die Kooperation mit den Obersten Landesjugendbehörden im Rahmen der Altersfreigabeverfahren (§ 14 Abs. 6 JuSchG) sowie Beteiligung öffentlicher Stellen im USK-Beirat, der u.a. die USK-Leitkriterien beschließt und evaluiert. Dies entspricht einem kooperativen, **multi-stakeholder-basierten Jugendmedienschutz**, wie er u.a. von den Vereinten Nationen gefordert wird.¹⁰
- Die Gewährleistung **verhältnismäßiger** und **gesellschaftlich legitimierter** Entscheidungen.
- Strukturen sind besonders effizient, da sie staatliche Stellen **organisatorisch entlasten, Kosten reduzieren und Qualitätssicherung im Vollzug** ermöglichen.

Grundsätzliche Konkretisierungs- und Verbesserungsbedarf besteht u. a. bei:

- Der Integration nationaler Einrichtungen der **freiwilligen Selbstkontrolle in den EU-Rechtsrahmen**, anstatt sie durch verbraucherschutzrechtliche Regelungen zu überlagern.

¹⁰ Vgl. UN-Kinderrechtsausschuss, Allg. Bemerkung Nr. 25 (2021), Abschnitt V, „C. Coordination“, Nr. 27.

- Der Gesetzessystematischen **Stärkung von qualitativ hochwertigen Alterskennzeichen**, die im Rahmen pluralistischer Kennzeichnungsverfahren entstehen (z.B. USK-Alterskennzeichen) gegenüber einfacher Anbieterkennzeichnungen.
 - Der Schaffung zusätzlicher gesetzlicher **Anreize zur Kooperation mit Selbstkontrolleinrichtungen** (vgl. insbesondere den Anbieter privilegierenden Ansatz des sog. Vorbefassungsschutz für Mitglieder einer Selbstkontrolleinrichtung i.S.d. § 20 Abs. 5 JMStV im Rahmen einer Selbstverpflichtung).
 - Der ausdrücklichen Berücksichtigung und Verortung von **Alterskennzeichen sowie Deskriptoren** (z. B. USK-Alterskennzeichen), wie sie für Spieleplattformen im Rahmen der Kennzeichnungspflicht in § 14a JuSchG festgelegt sind, **als Vorsorgemaßnahme** auf Onlineplattformen. Außerdem effektive Instrumente der Durchsetzung in Verknüpfung mit Privilegierungen im Rahmen der regulierten Selbstregulierung (s.o.).
 - **Gesetzlich normierte Einbindung von Selbstkontrolleinrichtung im Rahmen „dialogischer Verfahren“** des Digital Services Koordinators in Bezug auf Mitglieder von Selbstkontrolleinrichtungen.
 - Ausdrücklichere Berücksichtigung von **Elternbegleittools als zentrale Schutzmaßnahmen**. Diese stellen die Basis jeglicher Jugendschutzeinstellungen und Filterfunktionen dar. Auch Altersfeststellungen sind von solchen Einstellungsfunktionalitäten abhängig.
 - Stärkung und Schaffung von **Anreizen für präventive Ansätze**, z.B. im Rahmen von Zertifizierungen und Anerkennungen technischer Maßnahmen, insbesondere bei Selbstkontrolleinrichtungen (SKE).
 - Der **Abgrenzung** des Begriffs „Nebenfunktion eines Dienstes“ (z. B. bei Gaming-Plattformen).
 - Der Notwendigkeit einer klaren **EU-weiten Definition von „Altersverifikation“**, um nationale Rechtsunsicherheiten zu vermeiden.
5. **Welche Rolle spielen starke Verschlüsselungslösungen (z.B. Ende-zu-Ende-Verschlüsselung) für den Schutz von Kindern – und welche Spannungsfelder ergeben sich mit Überwachungs- und Interventionsmöglichkeiten?**
-
6. **Welche Rolle sollen Betriebssysteme und App-Stores für den technischen Jugendmedienschutz übernehmen (z.B. geräteweite Jugendschutzeinstellungen, einheitliche Altersstufen-/Label-Standards, Default- und Kaufbeschränkungen) und welche regulatorischen Instrumente wären dafür geeignet?**

Für Betriebssysteme und App-Stores gelten kürzlich in Kraft getretene Regelungen des JMStV (vgl. §§ 12 ff JMStV).

Die USK lehnt eine „One-Button-Lösung“ auf Betriebssystemebene ab: Eine solche „One-Button“-Lösung, die am Betriebssystem andockt, mag zwar auf den ersten Blick attraktiv klingen, führt jedoch bei näherem Hinsehen und vor dem Hintergrund der denkbaren Anwendungsfälle zu einer Verschlechterung des technischen Jugendmedienschutzes. Dies betrifft insbesondere Konstellationen, in denen mehrere Familienmitglieder dasselbe Gerät nutzen. Hier sind unterschiedliche Einstellungsmöglichkeiten absolut notwendig, da es andernfalls entweder zu einem

„Overblocking“ von Medieninhalten kommt oder das Risiko einer nicht oder nicht angemessenen Einstellung bzw. Aktivierung durch die Eltern besteht. Ein „Overblocking“ widerspricht zudem dem Partizipationsgedanken des Art. 17 der UN-Kinderrechtskonvention, der bereits im Rahmen der Gesetzesnovelle zum JuSchG als gleichwertiger Bestandteil neben Schutz und Orientierung verankert wurde.

Verhältnis zu europäischer Regulierung: Parallel gelten auch Anforderungen des DSA bzw. der E-Commerce-Richtlinie für App-Stores. Das Verhältnis dieser Regelwerke ist derzeit unklar. Derzeit fallen jedenfalls die großen vertriebseigenen App-Stores marktführender mobiler Endgeräte unter die Regulierung des DSA. Darüber hinaus existieren Vertriebsplattformen von Spielen, die unter die Definition einer Spieleplattform im Sinne des § 14a JuSchG fallen. Daneben wird der freie Verkehr von Diensten der Informationsgesellschaft gemäß Art. 3 Abs. 2 ECRL ggf. durch die Regelungen des JMStV beschränkt. Gerade die Anforderungen an Betriebssysteme sowie an die Anbieter von Apps gemäß der §§ 12 und 12a JMStV formulieren Einschränkungen durch abstrakt-generelle Maßnahmen, da Apps nur dann nutzbar gemacht werden dürfen, wenn sie deutsche Altersstufen vorhalten, die von der Jugendschutzvorrichtung der einschlägigen Betriebssysteme ausgelesen werden können. Genannte unionsrechtliche Bedenken wurden seitens der EU-Kommission im Rahmen der Notifizierung geäußert.

App-Stores stellen aus Sicht der USK einen geeigneteren Anknüpfungspunkt dar: Betriebssysteme werden nicht für einen geeigneten Ansatzpunkt gehalten. Die Storefront ist der bessere Anknüpfungspunkt (so wird es derzeit bei dem internationalen automatisierten Bewertungssystem IARC praktiziert; hier werden an die Spruchpraxis einer Selbstkontrolle angeschlossene wertige Alterskennzeichen vergeben und auf den Storefronts ausgespielt; sie sind verknüpft mit technischen Jugendschutzeinstellungen, idealerweise durch Selbstkontrollen anerkannte Jugendschutzprogramme, wie bei Nintendo oder der Xbox). Das IARC-System knüpft hingegen an dem jeweiligen App-Store an, was den Vorteil hat, dass grundsätzlich keine Schnittstelle zum Betriebssystem erforderlich ist.

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

-

III. Altersgrenzen, Altersverifikation und spezifische Schutzräume

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

Verbindliche pauschale Altersgrenzen oder generelle Zugangsverbote für bestimmte digitale Angebote sind aus Sicht der Unterhaltungssoftware Selbstkontrolle (USK) weder rechtlich erforderlich noch sachgerecht. So verfolgt insbesondere der Digital Services Act (DSA) im Bereich der Online-Plattformen einen **vollharmonisierenden** Ansatz und entfaltet entsprechend Anwendungsvorrang gegenüber nationalem Recht. Nationale „Alleingänge“, z.B. pauschale Altersverbote für Social-Media- oder vergleichbare interaktive Dienste, sind im Anwendungsbereich des DSA nicht vorgesehen und würden dem Ziel einer unionsweit kohärenten Plattformregulierung widersprechen. Darüber hinaus ist das sog. **Herkunftslandprinzip** (Art. 3 E-Commerce-RL 2000/31/EG) zu beachten, wonach sich die regulatorischen Pflichten der Anbieter nach den

rechtlichen Vorgaben ihres Sitzstaates richten, sodass nationale Regelungen praktisch nur begrenzt durchsetzbar wären. Eine Vielzahl der relevanten Anbieter hat einen Sitz im EU-Ausland. Zwar sind Ausnahmen möglich, doch unterliegen diese entsprechenden formellen und materiellen Voraussetzungen und sind nur in Bezug auf behördliche Einzelmaßnahmen möglich.

Doch auch **inhaltlich** bestehen erhebliche **Abgrenzungsprobleme**, so ist kaum konsistent definierbar, welche digitalen Angebote von pauschalen Altersgrenzen erfasst werden sollen und welche nicht. Diese Problematik besteht unabhängig davon, ob es sich um europäische oder nationale Regulierungsansätze handelt. Das zeigt sich etwa im Games-Bereich, in dem digitale Spiele längst hybride Angebote darstellen, die spielerische Inhalte mit Kommunikations-, Kreativ- und Community-Funktionen von unterschiedlichster Ausgestaltung verbinden. Eine pauschale Regulierung einzelner Angebote oder Plattformen würde vergleichbare Risiken und Nutzungskontexte ungleich behandeln und birgt erhebliche Risiken in Bezug auf Innovationsfreiheit und Angebotsvielfalt.

Verbindliche Altersgrenzen für bestimmte digitale Angebote bzw. pauschale Altersgrenzen scheitern jedoch zuvorderst und regelmäßig am **Grundsatz der Verhältnismäßigkeit**. So stellt ein solches Vorgehen einen Eingriff in die Grundrechte der Minderjährigen (Informations- und Meinungsfreiheit), aber auch der Anbieter dar (Berufs- und Eigentumsfreiheit) und muss entsprechend geeignet, erforderlich und zumutbar ausgestaltet sein. Bereits im Hinblick auf die Eignetheit zeigt die Forschung, dass Zusammenhänge zwischen digitaler Nutzung und dem Wohlbefinden Minderjähriger komplex sind und keine eindeutig belastbar kausalen Aussagen rechtfertigen, die generelle Nutzungsverbote begründen könnten. Darüber hinaus stellt sich das Problem der technischen Umgehbarkeit (z.B. durch VPN-Clients), so dass solche Ansätze in ihrer Schutzwirkung bereits begrenzt sind. Als mildere und zugleich wirksamere Mittel steht vielmehr ein **risikobasierter Ansatz** mittels differenzierter Vorsorgemaßnahmen und Schutzkonzepte zur Verfügung, der eine altersangemessene Nutzung ermöglicht, anstatt sie vollständig zu unterbinden. Genau diesen risikobasierten Ansatz verfolgt auch Art. 28 DSA, der nicht auf Verbote, sondern auf geeignete und verhältnismäßige Maßnahmen zur altersgerechten Ausgestaltung von Diensten abstellt. Dies wird durch die kürzlich beschlossenen Leitlinien der EU Kommission zu Art. 28 DSA nochmals ausdrücklich bestätigt¹¹, indem die Verhältnismäßigkeit und Eignung der Maßnahmen mittels Einzelfallprüfung betont werden.

Pauschale Altersgrenzen greifen demgegenüber tief in die Rechte Minderjähriger ein. Leitprinzip der UN-KRK ist somit das **Kindeswohl**. Kinder- und Jugendrechte beschränken sich demnach nicht auf Schutzdimensionen, sondern umfassen die **gleichrangigen Befähigungs-, Beteiligungs- und Teilhaberechte**, so wie es auch die 25. Allgemeinen Bemerkung zur UN-Kinderrechtskonvention (insbesondere Art. 12 UN-KRK) in digitalen Umgebungen festhält. Der Zugang zu entwicklungsrelevanten Interessen, Informationen, Unterhaltung oder zu kreativer Entfaltung und sozialen Interaktion mit Gleichaltrigen ist andernfalls über die in unserer heutigen Gesellschaft zentralen „digitale Kanäle“ ausgeschlossen. Ein genereller Ausschluss würde diese entwicklungsrelevanten Potenziale negieren und zugleich die praktische Entwicklung von Medienkompetenz mangels Zugangs erschweren.

¹¹ Vgl. Leitlinien für Maßnahmen zur Gewährleistung eines hohen Maßes an Privatsphäre, Sicherheit und Schutz von Minderjährigen im Internet gemäß Artikel 28 Absatz 4 der Verordnung (EU) 2022/2065 (C/2025/5519), S. 5.

Auch das **Erziehungsrecht der Eltern (Art. 6 Abs. 2 GG)** würde unterlaufen, da staatliche Verbote individuelle, begleitete Erziehungsentscheidungen ersetzen würden, anstatt sie zu unterstützen. Ziel ist es somit nicht in Ausübung des Wächteramts des Staates, das elterliche Erziehungsrecht zu beschränken, sondern das elterliche Erziehungsrecht störungsfrei zu gewährleisten und einen verhältnismäßigen Flankenschutz für Erziehungs- und Sozialisationsprozesse zu schaffen. Dies kann insbesondere durch verbindliche Altersfreigabeverfahren erfolgen, wie sie in Deutschland von der USK im Rahmen gemeinsamer Verfahren nach § 14 Abs. 6 JuSchG vergeben werden, oder durch anerkannte automatisierte Bewertungssysteme wie dem IARC-System. Alterskennzeichen schaffen Transparenz, ohne in das Erziehungsrecht einzugreifen.

Gerade im Games-Bereich hat sich gezeigt, dass altersdifferenzierte Schutzmechanismen wirksam umgesetzt werden können, ohne die **Teilhabe** von Kindern und Jugendlichen grundsätzlich auszuschließen. So berücksichtigen **Alterskennzeichen der USK** den gesetzlichen Vorgaben des JuSchG entsprechend neben **Inhalts- auch Nutzungsrisiken** (z.B. Kommunikations- und Kontaktfunktionen, Glücksspielähnliche Mechanismen, Förderung der exzessiven Mediennutzung) sowie **technische Vorsorgemaßnahmen** (z.B. Jugendschutzeinstellungen auf Spiel- oder Plattformebene) im Rahmen der Abwägung und vergeben neben der Altersfreigabe transparente **Zusatzhinweise** zur zusätzlichen Orientierung. Dies ermöglicht es Eltern, informierte Entscheidungen zu treffen und altersgerechte Nutzungsräume zu schaffen. Solche Instrumente sind seit Jahren etabliert, empirisch erprobt, rechtlich anerkannt und entsprechen dem Leitbild des DSA, Schutz, Befähigung und Teilhabe miteinander in Einklang zu bringen. Diese sind insbesondere dann wirksam, wenn Eltern den technischen Jugendschutz aktivieren und eine entsprechende Filterung stattfindet. Ein Beispiel hierfür sind die von der USK anerkannten Jugendschutzprogramme, die beispielsweise auf der Nintendo Switch¹² oder der Microsoft Xbox¹³ von Eltern oder Erziehungsbeauftragten genutzt werden können, um so Minderjährige effektiv vor beeinträchtigenden Inhalten zu schützen. Aber auch auf Onlineplattform-Ebene können anerkannten Jugendschutzprogramme in Kombination mit Alterseinstufungen wirken, wenn, wie beispielsweise auf dem von Epic angebotenen Kreativmodus „Islands“, für die von Nutzern geteilten Inseln IARC-Kennzeichen vergeben werden und diese an die internen Jugendschutzeinstellungen gekoppelt sind¹⁴.

Vor diesem Hintergrund sind pauschale Altersgrenzen weder unions- noch verfassungsrechtlich überzeugend. Ein wirksamer und zukunftsfähiger Minderjährigenschutz liegt vielmehr in differenzierten, risikobasierten Ansätzen, wie sie der DSA vorgibt und wie sie im Games-Bereich seit Jahren durch selbstregulatorische Strukturen erfolgreich praktiziert werden. Die Stärkung solcher bewährten **Selbstkontrollmechanismen** ist daher der sachgerechte Weg, um Schutz, Befähigung und Teilhabe von Kindern und Jugendlichen im digitalen Raum nachhaltig zu gewährleisten.

¹² Vgl. <https://usk.de/pressemitteilung-anerkennung-nintendo-switch-jugendschutzeinstellungen-verlaengert/>

¹³ Vgl. <https://usk.de/usk-pressemitteilung-zertifizierung-jugendschutzsystem-microsoft-xbox/>.

¹⁴ Vgl. <https://usk.de/fortnite-fuehrt-iarc-altersbewertungen-ein/>, <https://dev.epicgames.com/documentation/de-de/fortnite/iarc-overview-and-faqs-in-fortnite-creative>.

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

Die Frage nach einer verpflichtenden Altersverifikation für digitale Produkte, die Minderjährigen zugänglich sind, bedarf einer sorgfältigen **Abwägung zwischen Schutz, Befähigung und Teilhabe**.

Ein pauschaler Ausschluss Minderjähriger durch Altersverifikationsmaßnahmen ist weder eine angemessene noch eine verhältnismäßige Maßnahme zum Schutz Minderjähriger vor potenziell schädlichen kommerziellen Praktiken. Kinder und Jugendliche haben ein Recht auf gleichberechtigten, sicheren und altersgerechten Zugang zur digitalen Umwelt. Dieses Recht ergibt sich insbesondere aus Art. 17 und Art. 31 der UN-Kinderrechtskonvention, die das Recht auf Zugang zu Informationen, Medien und kultureller Teilhabe festschreiben. Die UN-Kinderrechtsausschuss-Allgemeine Bemerkung Nr. 25 (2021) zur Verwirklichung der Kinderrechte im digitalen Umfeld konkretisiert diesen Anspruch dahingehend, dass Kinder „nicht nur vor Risiken zu schützen, sondern auch aktiv in die Lage zu versetzen sind, die Chancen der digitalen Welt wahrzunehmen“. Organisationen wie UNICEF und die Stiftung digitale Chancen betonen in diesem Zusammenhang, dass ein rein restriktiver oder ausschließender Ansatz den Kinderrechten widersprechen und Teilhabechancen, digitale Bildung und soziale Integration erheblich beeinträchtigen würde.¹⁵

Aufgrund des Verhältnismäßigkeitsprinzips betonen daher sowohl **die Leitlinien der EU Kommission zu Art. 28 DSA**¹⁶, als auch die **USK-Leitkriterien** selbst¹⁷, dass stets eine Einzelfallprüfung erforderlich ist, um im Rahmen einer Risikoabwägung festzustellen, ob angemessene und wirksame anbieterseitig vorgehaltene Vorsorgemaßnahmen implementiert sind. Entsprechend sieht der Prüfrahmen der USK ebenfalls ausdrücklich vor, dass technische und strukturelle Vorsorgemaßnahmen in die Altersbewertung einzubeziehen sind (§ 10b JuSchG). Sind diese vor dem Hintergrund der enthaltenen Risiken für die persönliche Integrität nicht angemessen und wirksam, kann es zu einer höheren Altersfreigabe kommen. Die Leitlinien EU Kommission zu Art. 28 DSA betonen die **Flexibilität der Maßnahmenwahl** und verlangen eine Orientierung an der jeweiligen **Risikobewertung**: „Bevor Anbieter von Online-Plattformen, die für Minderjährige zugänglich sind, entscheiden, ob sie auf dem Alter basierende Zugangsbeschränkungen einführen, die durch Methoden der Altersfeststellung unterstützt werden, sollten sie stets eine Bewertung durchführen, um zu bestimmen, ob eine solche Maßnahme dazu geeignet ist, für ein hohes Maß an Privatsphäre, Sicherheit und Schutz von Minderjährigen innerhalb ihres Dienstes zu sorgen, und ob sie verhältnismäßig ist oder ein solch hohes Maß vielmehr bereits durch Rückgriff auf andere, weniger weitreichende Maßnahmen erreicht werden kann.“¹⁸

Bei der Ausgestaltung altersangemessener Altersverifikation ist jedoch „wichtig, zwischen der **Altersbeschränkung**, die den Zugang ... auf Nutzer unter oder über einem bestimmten Alter be-

¹⁵ Vgl. https://www.unicef.org/innovation/stories/protecting-childrens-rights-in-digital-environments?utm_source=chatgpt.com; https://www.digitale-chancen.de/aktuelles/detail/kinderrechte-im-digitalen-raum-leitlinien-des-europara-tes?utm_source=chatgpt.com.

¹⁶ Vgl. Leitlinien für Maßnahmen zur Gewährleistung eines hohen Maßes an Privatsphäre, Sicherheit und Schutz von Minderjährigen im Internet gemäß Artikel 28 Absatz 4 der Verordnung (EU) 2022/2065 (C/2025/5519), S. 9, Nr. 31.

¹⁷ Vgl. Abschnitt 3 der USK Leitkriterien, abrufbar unter: https://usk.de/wp-content/uploads/2024/12/USK-Leitkriterien_2024.pdf.

¹⁸ Vgl. Leitlinien für Maßnahmen zur Gewährleistung eines hohen Maßes an Privatsphäre, Sicherheit und Schutz von Minderjährigen im Internet gemäß Artikel 28 Absatz 4 der Verordnung (EU) 2022/2065 (C/2025/5519), S. 9, Nr. 31.

schränkt, einerseits und den Methoden der **Altersfeststellung** [(z.B. Eigenerklärung, Altersschätzung und Altersüberprüfung)], die zur Bestimmung des Alters eines Nutzers angewandt werden, andererseits zu unterscheiden,¹⁹ wobei der Hauptunterschied im Grad der Genauigkeit liegt. Alterskennzeichen und Rating-Systemen (z.B. das IARC-System) kommt in diesem Kontext eine zentrale Rolle zu, da sie eine **altersdifferenzierte Nutzung bzw. Kategorisierung** von Angeboten und Funktionalitäten überhaupt erst ermöglichen. Die jeweiligen Angebote können anschließend mit proportionalen Schutzmaßnahmen verknüpft werden entsprechen damit einem risikobasierten Regelungsansatz.

Altersverifikationssysteme können in bestimmten Fällen ein wirksames Mittel darstellen, insbesondere bei Angeboten mit eindeutigem Hochrisikopotenzial. Jedoch sind nicht alle Risiken für Minderjährige gleichermaßen altersabhängig. Verhaltens- und Interaktionsrisiken hängen stärker von sozialen Dynamiken und Designentscheidungen als vom biologischen Alter ab. Die **bloße Kenntnis des Alters** verhindert aber weder exzessive Mediennutzung noch riskante Selbstdarstellung oder unangemessene soziale Interaktionen.

Daher sollte der nationale sowie europäische Rahmen ausdrücklich **alternative technische Schutzmaßnahmen berücksichtigen**, die in vergleichbarer Weise ein hohes Schutzniveau gewährleisten. Hierzu zählen insbesondere Jugendschutzprogramme, wie sie in Deutschland im Rahmen der regulierten Selbstregulierung nach gesetzlichen Kriterien zertifiziert und anerkannt sind. Diese Programme ermöglichen eine elternbasierte Alterssteuerung (Elternprivileg Art 6 GG), indem Inhalte, Funktionen und Features anhand der von Eltern festgelegten Altersstufe freigeschaltet und/oder gefiltert werden und zugleich wirksame Barrieren gegen Umgehungsversuche aufgestellt werden. Kinder können sich somit beispielsweise kein alternatives „Fake“-Profil anlegen, während Eltern die Einstellungen an die Reife und Fähigkeiten ihres Kindes individuell anpassen können. Das wiederum ermöglicht die Entwicklung von Medienkompetenz in einem altersangemessenen und angemessen geschützten digitalen Umfeld.

Die USK spricht sich daher grundsätzlich für eine **koordinierte europäische Lösung aus, die bestehende nationale Selbstkontrollstrukturen und Learnings aus dem nationalen Rahmen respektiert und in einen gemeinsamen Rahmen integriert**. Hierbei ist insbesondere die seit Jahren bestehende und praktizierte Entscheidungspraxis auf Basis des JMStV sowie die formulierten Ansätze der EU Kommission im Rahmen ihrer Leitlinien zu Art. 28 DSA zu berücksichtigen.²⁰ Nur so kann ein effektiver, verhältnismäßiger und grundrechtskonformer Schutz Minderjähriger gewährleistet werden, der zugleich ihr Recht auf Zugang, Teilhabe und Befähigung im digitalen Raum wahrt.

¹⁹ Vgl. Leitlinien für Maßnahmen zur Gewährleistung eines hohen Maßes an Privatsphäre, Sicherheit und Schutz von Minderjährigen im Internet gemäß Artikel 28 Absatz 4 der Verordnung (EU) 2022/2065 (C/2025/5519), S. 8, Nr. 28.

²⁰ Vgl. Leitlinien für Maßnahmen zur Gewährleistung eines hohen Maßes an Privatsphäre, Sicherheit und Schutz von Minderjährigen im Internet gemäß Artikel 28 Absatz 4 der Verordnung (EU) 2022/2065 (C/2025/5519), S. 11, 6.1.3.2, Nr. 39 ff.

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

Geeignete Formen der Altersabsicherung sind solche, die insbesondere **verhältnismäßig** bzw. **risikobasiert, datenminimiert und technisch robust** ausgestaltet sind.²¹ Je nach Risikoprofil des Dienstes sollte auch der **Verzicht auf Altersfeststellungen oder abgestufte Altersfeststellungen** in Betracht kommen. Ersteres kommt insbesondere dann in Betracht, wenn im Rahmen der risikobasierten Rechteabwägung bereits andere Maßnahmen einen ausreichenden Schutz gewährleisten (z.B. Jugendschutzeinstellungen, „by default“-Einstellungen etc.). Dies wird dem Prinzip der Elternverantwortung besonders gerecht (Art. 6 GG, s.o.) und ermöglicht das Schaffen eines altersangemessenen Rahmens, der eine betreute Medienkompetenzvermittlung ermöglicht (s.o.). Andernfalls sollte die Möglichkeit abgestufter, niedrigschwelliger Alterseinschätzungen bei geringen Risiken, tokenisierte oder wallet-basierte Altersnachweise bei höheren Risiken sowie klassische Altersverifikation nur dort, wo sie zwingend erforderlich sind erfolgen.

Over-Collection lässt sich vermeiden, indem Altersabsicherung strikt auf die binäre Altersaussage („über/unter der relevanten Altersgrenze“) beschränkt, als separater Vorgang ausgestaltet und über anonymisierte Alterstoken unabhängiger Dritter umgesetzt wird. Privacy-by-Design-Technologien (z. B. Zero-Knowledge-Proofs) können zusätzliche Datenerhebungen verhindern. Diskriminierungsrisiken sollten durch technologieoffene, barrierearme und nicht biometrisch verpflichtende Verfahren minimiert werden. Im Rahmen der Umgehbarkeit können ebenfalls risikobasierte abgestufte Bewertungsmaßstäbe angewandt werden (z.B. der „einfachen“ Umgehbarkeit²²).

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

Speziell gestaltete digitale Räume für Kinder und Jugendliche können **sinnvoll und förderlich** sein, **wenn** sie nicht als pauschale Abschottung, sondern als altersangemessen ausgestaltete Schutz- und Teilhaberäume verstanden werden. Die Leitlinien der EU Kommission zu Art. 28 DSA stellen ausdrücklich klar, dass „Instrumente zur Altersfeststellung ... Anbietern auch dabei helfen [können], den Zugang von Erwachsenen zu bestimmten Plattformen, die für Minderjährige konzipiert sind, zu anderen als legitimen elterlichen, erzieherischen oder Aufsichtszwecken zu verhindern und so das Risiko zu verringern, dass sich Erwachsene als Minderjährige ausgeben und/oder versuchen, Minderjährigen Schaden zuzufügen.“²³ Zur Frage der Realisierung s.o.

Gleichzeitig sind auch die **Grenzen solcher Schutzräume** klar zu benennen. Altersbasierte Zugangshürden können Minderjährige nicht vor allen Risiken schützen: Auch unter Gleichaltrigen bestehen Interaktions- und Kommunikationsrisiken wie Cybermobbing, Hassrede oder sexuelle Grenzverletzungen. Zudem können zulässige Inhalte kumulative Wirkungen entfalten, etwa

²¹ Vgl. Leitlinien für Maßnahmen zur Gewährleistung eines hohen Maßes an Privatsphäre, Sicherheit und Schutz von Minderjährigen im Internet gemäß Artikel 28 Absatz 4 der Verordnung (EU) 2022/2065 (C/2025/5519), S. 11, 6.1.3.2, Nr. 39 ff.

²² Vgl. Kriterien für die Eignungsanforderungen nach § 11 Abs. 3 JMStV für Jugendschutzprogramme, abrufbar unter: https://www.kjm-online.de/fileadmin/user_upload/KJM/Themen/Technischer_Jugendmedienschutz/Kriterien_fu_r_die_Eignungsanforderungen_fu_r_Jugendschutzprogramme_12.10.2016.pdf.

²³ Vgl. Leitlinien für Maßnahmen zur Gewährleistung eines hohen Maßes an Privatsphäre, Sicherheit und Schutz von Minderjährigen im Internet gemäß Artikel 28 Absatz 4 der Verordnung (EU) 2022/2065 (C/2025/5519), S. 11, Nr. 27 ff.

durch Schönheitsideale oder Rollenklischees.²⁴ Ebenso lassen sich angebotsübergreifende Nutzungsrisiken durch Altersüberprüfung allein nicht wirksam adressieren. Speziell gestaltete Räume müssen daher stets durch begleitende Schutzmechanismen wie Moderation, Melde- und Abhilfeverfahren, sichere Voreinstellungen und Zeitbegrenzungen etc. ergänzt werden.

Rechtlich und pädagogisch besonders sensibel ist das **Erziehungsrecht der Eltern**. Verpflichtende Altersüberprüfungen als harte Zugangshürden können elterliche Steuerungs- und Begleitmöglichkeiten einschränken und als vermeintlicher Sicherheitsgarant missverstanden werden. Damit droht eine Schwächung elterlicher Medienerziehung sowie bewährter Instrumente wie durch Selbstkontrolleinrichtungen zertifizierte Jugendschutzprogramme (§ 11 JMStV). Speziell gestaltete Räume sollten daher elternermächtigend ausgestaltet sein und individuelle Erziehungsentscheidungen unterstützen, nicht ersetzen.

Insgesamt sind altersbezogene Schutzräume dann sachgerecht, wenn sie **risikobasiert, technisch datensparsam, organisatorisch begleitet und rechtlich verhältnismäßig** umgesetzt werden. Sie können einen wichtigen Beitrag zu Schutz und Teilhabe leisten, dürfen aber nicht als alleinige Lösung verstanden werden, sondern müssen Teil eines **integrierten Schutzkonzepts** sein, das technische, pädagogische und elterliche Verantwortung miteinander verbindet.

IV. Chancen, Teilhabe und spezielle Problemfelder

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

Ein technisch integrierter Kinder- und Jugendmedienschutz, der bereits „by design“ in digitale Dienste eingebettet ist, eröffnet erhebliche Chancen für Information, Bildung, Beteiligung, Entfaltung und Freizeit von Minderjährigen. Der Ansatz entspricht Art. 28 DSA, der nicht auf pauschale Zugangsbeschränkungen, sondern auf eine altersangemessene, risikobasierte Gestaltung digitaler Dienste abstellt, wie sie auch die Leitlinien der Europäische Kommission oder die USK Leitkriterien ausdrücklich hervorheben.

Technischer Jugendschutz „by design“ ermöglicht einen **niedrigschwelligen Zugang** zu Information und Bildung, ohne Minderjährige generell auszuschließen. Durch „wertige“ Alterskennzeichen, Parental-Control-Systeme und einen elternseitig wahrnehmbaren altersdifferenzierten Zugang, können Minderjährige digitale Medien nutzen, die ihrem **Entwicklungsstand entsprechen**. Auch der Games-Bereich bietet vielfältige **Lern-, Problemlösungs- und Kreativpotenziale**, die durch eine intelligente technische Ausgestaltung erhalten bleiben, statt durch pauschale Verbote unterbunden zu werden.

Ein solcher Ansatz stärkt zudem die Beteiligungs- und Teilhaberechte von Minderjährigen. Digitale Dienste mit Community-, Kreativ- oder Kommunikationsfunktionen, sind heute zentrale soziale Räume. Technischer Jugendschutz ermöglicht es, diese Räume sicher zu gestalten, etwa durch altersgerechte Kommunikationsfunktionen, moderierte Interaktionsräume oder abge-

²⁴ Vgl. Andresen, S./Dreyer, Über stete Tropfen und die Summe ihrer Teile. Kumulative Beeinträchtigungspotenziale und regulatorische Antworten des Kinder- und Jugendmedienschutzes, in mediendiskurs, 17.01.2025. Abrufbar unter: <https://mediendiskurs.online/beitrag/ueber-stete-tropfen-und-die-summe-ihrer-teile-beitrag-772/>.

stufte Freigaben. Dadurch können Minderjährige **altersangemessen partizipieren, ihre Meinung äußern und soziale Kompetenzen entwickeln**, ohne ungeschützt Risiken ausgesetzt zu sein.

Darüber hinaus werden besondere Chancen für eine positive Freizeitgestaltung eröffnet. Beispielsweise sind Spiele für Kinder und Jugendliche nicht nur Unterhaltung, sondern auch ein wichtiger Bestandteil **sozialer Interaktion, gemeinsamer Freizeit und kultureller Teilhabe**. Alterskennzeichen, die neben Inhalts- auch Nutzungsrisiken sowie technische Vorsorgemaßnahmen im Rahmen der Abwägung berücksichtigen und transparente Zusatzhinweise neben der Altersfreigabe zur zusätzlichen Orientierung ermöglichen es, ermöglichen es **Spielräume** zu erhalten und zugleich exzessive oder entwicklungsbeeinträchtigende Nutzung zu begrenzen.

Ein „by-design“-Ansatz befähigt zudem, anstatt auszuschließen. Er fördert die **schrittweise Entwicklung von Medienkompetenz**, indem Minderjährige digitale Angebote in einem geschützten Rahmen kennenlernen und nutzen können. Lernen im und über den digitalen Raum setzt einen Zugang zu solchen Angeboten voraus. Technischer Jugendschutz schafft diesen Zugang kontrolliert und begleitet, anstatt ihn vollständig zu versperren. Gleichzeitig stärkt er das Erziehungsrecht (Art. 6 GG) der Eltern, da technische Schutzinstrumente, insbesondere sog. Parental-Control-Systeme bzw. Jugendschutzeinstellungen, individuelle Erziehungsentscheidungen unterstützen, anstatt sie durch staatliche Pauschalregelungen zu ersetzen.

Zusammenfassend eröffnet technischer Kinder- und Jugendmedienschutz „by design“ die Chance, digitale Dienste so auszugestalten, dass Schutz, Befähigung und Teilhabe nicht als Gegensätze, sondern als miteinander verbundene Ziele verstanden werden. Er ermöglicht sichere, altersangemessene Nutzung digitaler Angebote und stellt damit eine tragfähige Alternative zu pauschalen Zugangsbeschränkungen dar.

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

Ein übermäßiger Medienkonsum von Kindern und Jugendlichen lässt sich nicht durch pauschale Verbote, sondern vor allem durch **präventive Maßnahmen** wirksam begrenzen. Zentral ist dabei die **Stärkung elterlicher Steuerungsmöglichkeiten**: Hierzu gehören einerseits Parental-Control-Systeme, Nutzungsstatistiken und flexible Zeitkontingente, die eine individuelle Begleitung der Mediennutzung ermöglichen und den Entwicklungsstand des Kindes berücksichtigen. Andererseits bedarf es „wertiger“ Alterskennzeichen sowie Zusatzhinweise, die Eltern eine präventive Orientierung ermöglichen, basierend auf einheitlichen Kriterien und einheitlicher sowie aktueller Spruchpraxis, so wie sie im Rahmen der USK-Alterskennzeichnungsverfahren auf Basis eine „Private-Public-Partnership“ mit den Obersten Landesjugendbehörden vergeben werden.

Altersüberprüfungen allein sind hierfür nicht geeignet, da sie die Nutzungsdauer nicht wirksam steuern können. Außerdem ist eine Vermittlung von Medienkompetenz essentiell.

Weitere Informationen s.o. zu Frage 1 b).

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

-