

André Weßel/Friederike von Gross (Hrsg.)

Aufwachsen mit KI

**Medienbildung, Datenschutz und digitale Selbstbestimmung
im Kindes- und Jugendalter**

André Weßel/Friederike von Gross (Hrsg.)

Aufwachsen mit KI

**Medienbildung, Datenschutz und digitale Selbstbestimmung
im Kindes- und Jugendalter**

Beiträge aus Forschung und Praxis

Prämierte Medienprojekte

André Weßel/Friederike von Gross (Hrsg.)

Aufwachsen mit KI

**Medienbildung, Datenschutz und digitale Selbstbestimmung
im Kindes- und Jugendalter**

Beiträge aus Forschung und Praxis – Prämierte Medienprojekte

Dieser Band wurde gefördert vom

Bundesministerium für Bildung, Familie, Senioren, Frauen und Jugend (BMBFSFJ)

Herausgeber

Gesellschaft für Medienpädagogik und Kommunikationskultur
in der Bundesrepublik Deutschland e.V. (GMK)

Anschrift

GMK-Geschäftsstelle
Oberstr. 24 a
33602 Bielefeld
fon 0521/677 88
email gmk@medienpaed.de
homepage www.gmk-net.de

Redaktion

André Weßel
Dr. Friederike von Gross
Tanja Kalwar

Lektorat

Tanja Kalwar

Titelillustration

kopaed

Druck

Memminger MedienCentrum, Memmingen

© kopaed 2026

Arnulfstraße 205
80634 München

fon 089/688 900 98
fax 089/689 19 12
email info@kopaed.de
homepage www.kopaed.de

ISBN 978-3-96848-210-1

Zwischen KI-Regelwerk und Regelungslücke

Welche rechtlichen Vorgaben für KI-Systeme im Kinderkontext gelten und wo medienpädagogische Begleitung wichtig ist

Der Rechtsrahmen in der Praxis

Stellen wir uns eine Fachkraft in der offenen Jugendarbeit vor. Sie beobachtet, dass ein 13-Jähriger in der Einrichtung jeden Nachmittag mit einem KI-Chatbot spricht bzw. interagiert. Weniger über Hausaufgaben und mehr über seine Einsamkeit, seine Angst vor der Schule, seine Wut auf Mitschüler*innen und Eltern. Die Fachkraft fragt sich: Schützt das Recht diesen jungen Menschen vor einer KI, in der er sich verliert? Die Antwort lautet: Es kommt darauf an. Und in Fällen wie diesem greift das Recht oft nicht gut genug.

Die Frage ist nicht abwegig. 91 Prozent der Zwölf- bis 19-Jährigen in Deutschland nutzen mittlerweile KI-Tools, das ist ein Anstieg um 29 Prozentpunkte innerhalb eines einzigen Jahres (mpfs 2025). Dabei ist KI für sie längst mehr als ein Werkzeug. Sie ist Gesprächspartnerin, kreatives Gegenüber und emotionales Ventil (BzKJ 2026).

Dass echtliche Vorgaben vielleicht nicht greifen, liegt nicht daran, dass der Gesetzgeber untätig gewesen wäre. Im Gegenteil: Die letzten Jahre haben einen bemerkenswerten Regulierungsschub hervorgebracht. Vier Regelwerke sind dabei besonders wichtig: der AI Act (die KI-Verordnung) als Produktsicherheitsrecht für KI-Systeme, der Digital Services Act (DSA) als noch junger EU-Ordnungsrahmen für Online-Plattformen, die Datenschutz-Grundverordnung (DSGVO) mit ihren umfassenden Regeln für den Umgang mit personenbezogenen Daten und der Jugendmedienschutz-Staatsvertrag (JMStV) der Länder, der zuletzt im Dezember 2025 novelliert wurde.

Diese vier Werkzeuge klingen nach einem dichten regulatorischen Netz. In Wirklichkeit aber haben sie ein strukturelles Problem: Sie

reagieren auf ganz unterschiedliche technische und Angebotsentwicklungen und passen nicht alle optimal auf jedes KI-System. Der AI Act nimmt zwar KI-Systeme selbst in den Blick, knüpft seine Anforderungen dann aber nicht an die konkreten, tatsächlichen Risiken in der Praxis, sondern an abstrakte Risiken entlang des grundsätzlichen Einsatzzwecks. Die drei anderen Regelwerke regulieren KI überhaupt nicht explizit, sondern nur mittelbar, etwa als Teil von Diensten, die Daten verarbeiten, Inhalte vermitteln oder bestimmte Funktionen bereitstellen. Ob und wie also ein KI-Chatbot, ein Empfehlungssystem einer Social-Media-Plattform oder eine Lern-App rechtlich vom Ordnungsrahmen erfasst sind, hängt davon ab, wie genau das Angebot aufgebaut ist, in dem die KI läuft. Das ist juristisch vielleicht noch nachvollziehbar, für die Praxis ist dieser Umstand aber unübersichtlich.

Diese Unübersichtlichkeit hat Konsequenzen, die Fachkräfte der Medienpädagogik unmittelbar betreffen. Denn sie müssen wissen, welche KI-Systeme rechtlich wie erfasst sind, um Kinder und ihre Bezugspersonen über Risiken und bestehende Schutzrechte aufzuklären. Und sie müssen wissen, welche Systeme sich dem Rechtsrahmen entziehen, weil dort die medienpädagogische Begleitung umso wichtiger wird.

Bei dieser Abschtimmungsaufgabe will der Beitrag Orientierung bieten. Er geht dazu nicht entlang der vier Rechtsakte vor; ein solcher Überblick wäre angesichts der vielen unbestimmten Rechtsbegriffe zu abstrakt und auch zu spekulativ, denn viele Fragen werden sich erst in der Rechtsanwendung der kommenden Jahre klären. Stattdessen zeigt der Beitrag anhand von sechs konkreten KI-Anwendungen, denen Kinder in ihrer Medienpraxis begegnen, wie sich der Rechtsrahmen im Einzelfall

auswirkt. Für jede Anwendung wird kurz dargestellt: Welche Regeln greifen? Wo liegen Grauzonen? Und wo bleibt schlicht eine Lücke? Am Ende folgt ein Ausblick darauf, wo und wie medienpädagogische Praxis die Schwächen des Rechts zumindest teilweise kompensieren kann.

Vier Regelwerke, vier Regelungslogiken

Bevor wir uns die einzelnen KI-Anwendungen anschauen, lohnt sich ein kurzer Blick auf die vier zentralen Regelwerke. Wichtiger als ihre Detailkenntnis ist dabei ihre jeweilige Funktionslogik, denn sie erklärt, warum bestimmte KI-Risiken erfasst werden und andere nicht.

Der *AI Act* der EU ist im Kern ein Produktsicherheitsgesetz für KI-Systeme. Er ordnet KI auf Basis ihrer Anwendungszwecke bzw. -kontexte in Risikostufen ein und knüpft an jede Stufe unterschiedliche Pflichten: von Transparenzanforderungen für generative KI (die sogenannten General Purpose AI-Modelle oder GPAI) über umfassende Compliance-Anforderungen für Hochrisiko-KI-Systeme bis hin zu absoluten Verboten für eng definierte KI-Praktiken. Kinder werden im *AI Act* grundsätzlich als besonders schutzbedürftige Gruppe anerkannt: Art. 5 Abs. 1 (b) verbietet ausdrücklich KI-Systeme, die altersbedingte Verletzlichkeiten ausnutzen, und bewertende KI im Bildungsbereich gilt automatisch als Hochrisiko-KI-System. Ansonsten aber sind Kinderrechte und Jugendschutz im *AI Act* nicht ausdrücklich benannt, es gibt auch nicht einzelne Vorschriften, die sich konkret dem Jugendschutz oder der Sicherheit jüngerer Personen beim Umgang mit KI widmen. Kinder werden vor allem über allgemeine Zielgrößen und Abwägungsmaßstäbe wie „Gesundheit, Sicherheit und Grundrechte“ – einigermassen versteckt – mitadressiert. Zudem überlässt der *AI Act* die meisten Bewertungen den KI-Anbietern selbst, die Konkretisierung der unbestimmten Begriffe obliegt technischen Standardisierungsorganisationen. Die Sorge ist entsprechend begründet, dass Schutz, Befähigung und Teilhabe von Minderjährigen bei der Umsetzung des *AI Act* nur eine untergeordnete Rolle spielen werden (Dreyer 2024).

Der *Digital Services Act* (DSA) setzt ganz woanders an, denn die EU-Verordnung stellt Jugendschutzvorgaben nicht für KI-Systeme, sondern für Online-Plattformen auf, die fremde Inhalte im Netz zugänglich machen. Diese Online-Plattformen können als Teil der Gestaltung ihrer Angebote und Angebotsfunktionen KI-Modelle und -Anwendungen einsetzen, so dass sich der DSA auf diese Systeme indirekt mit auswirkt. Art. 28 Abs. 1 DSA verpflichtet Plattformanbieter, geeignete und verhältnismäßige Maßnahmen für ein „hohes Maß an Privatheit, Sicherheit und Schutz“ von Minderjährigen zu ergreifen. Was das genau heißen kann, hat die EU-Kommission in ausführlichen Leitlinien konkretisiert¹: private Standardkonten für Minderjährige, Einschränkung manipulativer Designelemente wie Dauer-Scrolling oder Autoplay, altersadäquate Gestaltung der Funktionen und Nutzeroberflächen. Diese Leitlinien sind rechtlich unverbindlich, geben den Plattformen aber eine gute Orientierung, was von ihnen erwartet wird.

Für den Umgang mit KI ist eine zentrale Frage des DSA allerdings bis heute rechtlich ungeklärt: Gilt die Verordnung überhaupt für reine KI-Chatbots? Sind ChatGPT und Co. im Sinne des DSA „Online-Plattformen“ und damit von den Jugendschutzpflichten des DSA erfasst? Die EU-Kommission geht derzeit davon aus, dass sie OpenAI als Anbieter von ChatGPT nur deshalb in den Anwendungsbereich des DSA ziehen kann, weil der Chatbot auch Live-Recherchen im Netz durchführt und damit wie eine Online-Suchmaschine funktioniert. Für reine Chatbots ohne diese Funktion wäre das Ergebnis also ein anderes. Sicher ist nur: Wenn eine Plattform, wie z. B. ein Social-Media-Angebot, KI-Systeme für ihre Angebote einsetzt – also etwa für personalisierte Empfehlungen, Altersschätzungen oder Inhaltsmoderation –, gelten die Jugendschutzvorgaben des DSA auch für diese KI-basierten Funktionen.

Die *DSGVO* ist der dritte wichtige Ordnungsrahmen. Auch diese EU-Verordnung ist kein KI-Gesetz, sondern ein Datenschutzgesetz, aber KI berührt den Datenschutz an mehreren Stellen: Beim Training großer KI-Modelle werden

gigantische Mengen personenbezogener Daten verarbeitet (derzeitige Top-Modelle sind auf über 1 Petabyte Daten trainiert worden und arbeiten mit bis zu 500 Billionen Parametern). Und auch beim Umgang mit einem fertigen KI-System fließen personenbezogene Informationen ein und aus, z. B. bei der Eingabe durch eine*n Nutzer*in oder bei der Ausgabe des Systems. Zwei Regelungen der DSGVO sind für Kinder besonders relevant: Art. 8 regelt, wann Minderjährige selbst in Datenverarbeitung einwilligen können (in Deutschland ab 16 Jahren). Und Art. 22 verbietet Entscheidungen, die ausschließlich automatisiert getroffen werden und erhebliche Auswirkungen auf die betroffene Person haben.

Der *Jugendmedienschutz-Staatsvertrag (JMStV)* schließlich ist das nationale Regelwerk, das die Medienpädagogik wahrscheinlich am besten kennt. Die §§ 4 und 5 JMStV regeln, welche Inhalte über Rundfunk und Online-Angebote nicht verbreitet werden dürfen und welche zwar grundsätzlich erlaubt, aber nicht für Minderjährige geeignet sind. Sie geben vor, welche technischen Schutzvorkehrungen Anbieter treffen müssen. Der im Dezember 2025 in Kraft getretene 6. Medienänderungsstaatsvertrag hat hier wichtige Neuerungen gebracht: Jugendschutzvorrichtungen auf Betriebssystemebene, Regelungen gegen Umgehungsmöglichkeiten von behördlich gesperrten Seiten (sogenannte Mirror Domains), Blockade von Zahlungsströmen zu unzulässigen Angeboten. KI aber wird in keiner Vorschrift des JMStV ausdrücklich erwähnt. Ein juristisches Gutachten (Ukrow 2024) hat dieses Versäumnis als das zentrale Defizit des deutschen Jugendmedienschutzes identifiziert und die explizite Aufnahme von KI-Systemen in den Geltungsbereich des Staatsvertrags gefordert.

Sechs KI-Anwendungen aus dem Alltag Heranwachsender

Generative KI-Chatbots für Schule und Freizeit

ChatGPT, Claude, Copilot, Gemini und vergleichbare Systeme (sogenannte große Sprachmodelle) sind für Jugendliche längst Alltagswerkzeug. 84 Prozent der Zwölf- bis 19-Jährigen

haben ChatGPT schon genutzt, die Hälfte davon mehrmals wöchentlich. ChatGPT ist damit zur zweitwichtigsten Informationsquelle nach Google aufgestiegen (mpfs 2025), Tendenz weiter und schnell steigend. Die Hauptnutzung ist schulisch: Recherche, Suche nach Erläuterungen und Einordnungen. Aber die Chatbots werden zunehmend auch für kreative Aufgaben genutzt und als dialogische Such-, Wissens- und Beratungsinstanz akzeptiert – oft mit einer Selbstverständlichkeit und Unvoreingenommenheit, die pädagogisch bedenklich ist.

Der AI Act stellt für generative Chatbots zunächst Transparenzpflichten auf: Nutzende müssen erkennen können, dass sie mit einer KI sprechen und nicht mit einem Menschen (Art. 50 AI Act); KI-generierte Texte, Bilder oder Videos müssen auch in maschinenlesbarer Form als solche gekennzeichnet werden. Darüber hinaus gelten umfassendere Pflichten für Anbieter großer KI-Modelle, etwa zu Trainingsdaten-Dokumentation und Angaben zur Urheberrechtskonformität. Bei den großen Sprachmodellen wie ChatGPT, Claude oder Gemini kommen noch Pflichten zur Risikobewertung hinzu: Der Anbieter muss prüfen, welche Gefährdungen von seinem Modell ausgehen und entsprechende Gegenmaßnahmen ergreifen. Für Kinder besonders wichtig: Wenn der Anbieter feststellt, dass die Nutzung seines Modells durch Minderjährige besondere Risiken birgt, muss er diese adressieren.²

Die großen Anbieter reagieren darauf vor allem mit Verfahren zur Altersschätzung, entweder basierend auf dem Nutzungsverhalten oder durch Formen elektronischer Altersüberprüfung. Ziel ist es dabei, zu junge Nutzende auszuschließen. Diese Verfahren sind aber nicht hundertprozentig zuverlässig, Kinder und Jugendliche werden also auch weiterhin mit den großen Sprachmodellen interagieren. Und wer als Minderjährige*r erkannt wird, weicht im Zweifel auf andere, schlimmstenfalls weniger regulierte Chatbots aus.

Die DSGVO verlangt im Kontext von Chatbot-Nutzungen in der Regel eine Einwilligung, wenn personenbezogene Daten verarbeitet werden. Bei unter 16-Jährigen müssen die Er-

ziehungsberechtigten einwilligen. Wenn der Anbieter das Alter nicht kennt, muss er angemessene Maßnahmen zur Altersermittlung treffen. Was „angemessen“ heißt, wurde in der Praxis bislang sehr vorsichtig ausgelegt. Erst langsam beginnen einige Anbieter, ernsthaftere Verfahren zur Altersverifikation auszurollen.

Der DSA greift bei Chatbots wie oben beschrieben nur, wenn man sie als Online-Plattformen versteht, die fremde Inhalte zugänglich machen. Das ist juristisch umstritten, denn ein Chatbot gibt in der Regel nicht einfach fremde Inhalte weiter. Er produziert eigene Ausgaben auf Basis seines Trainings – auf Anbieter mit eigenen Inhalten aber wäre der DSA mit seinen im Prinzip guten Jugendschutzvorgaben nicht anwendbar.

Der JMStV schließlich erfasst in erster Linie die Inhalte, die ein Chatbot produziert – wenn man diese denn als eigene Inhalte des Anbieters versteht. Auch hier stellt sich also die Frage, ob der Output einer KI dem Anbieter als eigener Inhalt zuzurechnen oder eher wie ein nutzergenerierter Inhalt zu behandeln ist. Wenn man dem Chatbot-Anbieter den Output zurechnet, greifen die §§ 4 und 5 JMStV und er muss im Falle der Darstellung jugendschutzrelevanter Inhalte technische Zugangshürden einbauen. Seit Dezember 2025 gibt es außerdem eine wichtige Neuerung: Der Anbieter kann nun auch Risiken für die „persönliche Integrität“ bei der Altersbewertung seines Angebots berücksichtigen, und damit auch Nutzungsrisiken wie exzessive Nutzung oder emotionale Abhängigkeit.

Was in der Zusammenschau auffällt, ist, dass es derzeit keine starre Pflicht zur Altersverifikation beim Zugang zu Chatbots gibt. Es gibt auch keine Vorgabe, dass der Output an die Entwicklungsstufe des Nutzenden angepasst werden muss. Und es gibt keinen Mechanismus, der verhindert, dass ein 13-Jähriger einen Chatbot als primäre Informationsquelle nutzt und dessen Antworten – einschließlich ihrer Unschärfen und gelegentlichen Halluzinationen – für verlässliches Wissen hält.

Für die medienpädagogische Praxis heißt das: Der Rechtsrahmen bietet einen eher dünnen Schutzschirm. Er setzt vor allem auf Transparenz, weniger auf Schutz. Die Aufgabe, epi-

stemische Abhängigkeit von KI-Systemen zu reflektieren und die Fähigkeit zur Quellenprüfung zu stärken, bleibt vorerst hauptsächlich bei den Fachkräften der Medienbildung.

KI-Companion-Apps als stets verfügbare Gesprächspartner

Bei KI-Freundes- oder Companion-Apps zeigt sich die größte Diskrepanz zwischen Nutzungsrealität und Rechtsrahmen und zugleich das pädagogisch dringlichste Problem. Angebote wie Character.AI, Replika, Kindroid oder Chai sind weniger Informationswerkzeuge als vielmehr Beziehungssimulationen. Sie sind explizit darauf ausgelegt, emotionale Nähe zu erzeugen, Empathie zu imitieren und Bindung zu fördern. Eine Umfrage von Common Sense Media (2025) zeigt für die USA, dass ein Drittel der Teenager Gespräche mit KI als genauso befriedigend empfindet wie solche mit echten Freundinnen und Freunden.

Der Character.AI-Fall in Florida hat die Risiken dieser Systeme auf tragische Weise sichtbar gemacht. Ein 14-Jähriger hatte über Monate eine intensive emotionale Bindung an einen Chatbot entwickelt. Er nahm sich im Februar 2024 das Leben. Der Chatbot hatte wohl die Fantasiebeziehung trotz konkret geäußelter Suizidabsichten weiterlaufen lassen. Im Dezember 2024 kamen weitere Fälle hinzu, darunter ein autistischer 17-Jähriger, dem der Chatbot Selbstverletzung und Gewalt gegen die Eltern nahegelegt hatte. Im Januar 2026 einigte sich Character.AI mit der Familie des 14-Jährigen auf einen Vergleich.³

Diese Fälle illustrieren ein Risikoprofil, das sich grundlegend von dem der allgemeinen Chatbots unterscheidet. Das primäre Problem ist nicht der *Inhalt* einzelner Aussagen, sondern die *Beziehungsdynamik*: parasoziale Bindung, emotionale Abhängigkeit, simulierte Intimität, das Fehlen jener natürlichen Begrenzung, die in menschlichen Beziehungen durch Erschöpfung oder eigene Bedürfnisse des Gegenübers entsteht (Bayor et al. 2025).

Und genau diese beziehungsbezogenen Risiken stellen regulatorisch große Graubereiche dar: Der AI Act adressiert keine individuellen Interaktionsrisiken; seine Klassifizierung orien-

tiert sich an Anwendungsbereichen, nicht an Beziehungsdynamiken. Der DSA setzt bei Plattformen mit nutzergenerierten Inhalten an – und ob Companion-Apps überhaupt Plattformen sind, ist umstritten (siehe oben). Die DSGVO schützt Daten, nicht emotionale Abhängigkeiten. Und der JMStV kennt zwar seit der letzten Novelle Risiken für die „persönliche Integrität“. Ob und wie Beziehungssimulationen darunterfallen, müsste aber erst eine aufsichtliche Spruchpraxis klären, die es bisher nicht gibt.

Mit Blick auf die Medienpädagogik wird klar, dass es bei Companion-Apps derzeit keinen verlässlichen regulatorischen Rückhalt gibt. Wer hier Kinder begleitet, tut das faktisch als einzige greifbare Schutzinstanz.

Bild- und Videogeneratoren

Bei Bild- und Videogeneratoren wie DALL-E, Midjourney oder Sora ist die Rechtslage dort klar, wo der Output eindeutig rechtswidrig ist. KI-generierte Darstellungen sexualisierter Gewalt gegen Kinder sind strafbar, unabhängig davon, ob reale Kinder abgebildet sind. Das deutsche Strafrecht hat hier früh eine medienneutrale Formulierung gewählt (§ 184b StGB).⁴ Auch volksverhetzende oder gewaltverherrlichende KI-Darstellungen können strafrechtliche Tatbestände erfüllen (§§ 130, 131 StGB). Und wer KI-generierte Pornografie oder Gewaltdarstellungen ohne Altersverifikation zugänglich macht, verstößt gegen § 4 JMStV. Der AI Act ergänzt das durch seine Kennzeichnungspflicht: Synthetische Inhalte müssen maschinenlesbar als KI-generiert markiert werden.

Grauzonen entstehen dort, wo die persönlichkeitsrechtliche Dimension in den Vordergrund tritt. Das wachsende Problem in Schulen etwa sind Deepfakes von Mitschüler*innen, insbesondere sexualisierte Deepfakes („Deep Porn“). Diese liegen strafrechtlich oft unterhalb der Schwelle der klassischen Tatbestände: Beleidigung (§ 185 StGB), üble Nachrede (§ 186 StGB) und die Verletzung des höchstpersönlichen Lebensbereichs (§ 201a StGB) greifen strukturell zu kurz, denn sie fangen die spezifische Unrechtserfahrung einer digitalen körperlichen Verfälschung nicht ein. Der Ge-

setzgeber diskutiert daher die Einführung eines neuen Straftatbestands zum Schutz vor digitalen Fälschungen (§ 201b StGB-E).

Für rechtmäßige Darstellungen gelten im Übrigen die Vorgaben, die in Abschnitt „Generative KI-Chatbots für Schule und Freizeit“ für Chatbots beschrieben wurden. Außerdem stellen sich die Fragen problematischer Beziehungsdynamiken hier nicht. Medienpädagogisch ist die Lage damit überschaubarer als bei anderen Systemtypen: Die rechtlichen Grenzen sind klar kommunizierbar. Die Herausforderung liegt weniger in der Awareness als in der Prävention und in der ethischen Reflexion über die Verfügbarkeit dieser Werkzeuge.

Empfehlungssysteme auf Plattformen

Algorithmische Empfehlungssysteme auf TikTok, Instagram oder YouTube sind regulatorisch vergleichsweise gut erfasst. Denn sie sind in Plattform-Angebote eingebettete KI-Systeme, und Plattformen sind die Kernadressatinnen der Jugendschutzvorgaben im DSA (siehe oben). Der DSA verpflichtet Plattformanbieter zu mehreren Dingen: zur Transparenz über die Hauptparameter ihrer Empfehlungssysteme (Art. 27), zur Bewertung systemischer Risiken bei den ganz großen Plattformen (Art. 34, 35) und zum erwähnten ausdrücklichen Minderjährigenschutz (Art. 28). Die Leitlinien der EU-Kommission zu Art. 28 empfehlen konkret, persuasive Designelemente wie Infinite Scrolling, Autoplay und Streak-Mechanismen für Minderjährige zu begrenzen. Die Anbieter haben also hinreichend Hinweise, was als Risiko für Jüngere gelten kann.

Die Durchsetzung der gesetzlichen Vorgaben liegt bei der EU-Kommission, die für die sogenannten sehr großen Online-Plattformen (very large online platforms, VLOPs) zuständig ist. Und sie wird langsam, aber bestimmt aktiv: Im Frühjahr 2026 hat die Kommission ein Verfahren gegen TikTok eingeleitet, das auch jugendschutzrechtliche Verstöße umfasst – insbesondere personalisierte Empfehlungen und endloses Scrolling stehen im Fokus.

Für den Kinderkontext bleibt aber ein grundlegendes Problem, das zwischen dem De-

sign der Empfehlungslogiken und den empfohlenen Inhalten liegt. Die kumulative Wirkung von Mikroinhalten, die für sich genommen harmlos sind – etwa „tradwife“-Content, Body-Shaming, diskriminierende Memes –, aber in der algorithmisch verstärkten Wiederholung und Verdichtung entwicklungsbeeinträchtigend wirken können, ist vom bestehenden Rechtsrahmen nur begrenzt fassbar (Andresen/Dreyer 2025). Der JMStV schaut auf Einzelinhalte, die meist nicht die Schwelle zur Entwicklungsbeeinträchtigung überschreiten. Art. 28 DSA greift strukturelle Risiken einer Plattform, aber spätestens bei plattformübergreifenden kumulativen Effekten – wenn ein Kind auf TikTok, Instagram und YouTube parallel mit ähnlichen Mustern konfrontiert wird – reichen die bestehenden Instrumente nicht.

Für die Medienpädagogik ist der praktische Transfer hier am klarsten: Fachkräfte sollten die bestehenden Transparenzrechte kennen und Kindern vermitteln, dass sie ein Recht auf Erklärung der Empfehlungslogiken haben (Art. 27 DSA). Außerdem hilft das Schaffen eines Grundverständnisses zur Funktion und zu kumulativen Wirkungen von Empfehlungsalgorithmen.

KI-gestützte Lern- und Bewertungssysteme

Adaptive Lernsoftware, KI-Tutoren und automatisierte Lernbewertungssysteme weisen den restriktivsten Rechtsrahmen von allen hier betrachteten Anwendungen auf. Das liegt vor allem am AI Act: Er verbietet KI-Systeme zur Emotionserkennung im Bildungsbereich vollständig (Art. 5). Und er stuft KI im Bildungskontext als Hochrisiko-KI-System ein, wenn sie über Zulassung oder Zuweisung entscheidet, Lernergebnisse bewertet, das Bildungsniveau einschätzt oder zur Prüfungsüberwachung eingesetzt wird (Art. 6 Abs. 2 i. V. m. Anhang III Nr. 3). Diese Einordnung bedeutet für den KI-Anbieter ein umfassendes Pflichtenpaket: Risikomanagement, Datenqualität, Transparenz, menschliche Aufsicht (Art. 8 bis 15 AI Act). Parallel dazu verbietet Art. 22 DSGVO Entscheidungen, die ausschließlich automatisiert getroffen werden und erhebliche Auswirkungen haben (Dreyer/Schulz 2020).

Die Grauzonen in der Rechtspraxis liegen in der Abgrenzung. Was genau ist „Bildungsbereich“ im Sinne des AI Act? Fallen auch freiwillige Lern-Apps außerhalb schulischer Kontexte darunter, wenn sie adaptive Lernpfade erstellen? Und wer haftet, wenn eine KI-gestützte Bewertung fehlerhaft ist: der Anbieter der Software, die Schule, die Lehrkraft? Hier hilft der AI Act nicht weiter. Eine geplante EU-Richtlinie zur KI-Haftung wurde von der Kommission zurückgezogen. Der britische Ofqual-Skandal von 2020, als ein Algorithmus Abiturnoten nach Postleitzahl vergab und Schüler*innen aus benachteiligten Bezirken systematisch schlechter bewertete, sollte eigentlich als Warnung dienen (Heaton et al. 2023).

Für Fachkräfte ergibt sich aus der Hochrisiko-Einstufung aber ein starkes Argument. Die Einführung von KI-Systemen in Schulen ist kein didaktisches Detail, sondern eine auch regulatorisch zentrale Entscheidung, die Transparenz, Aufsicht und menschliche Überprüfbarkeit voraussetzt. Entsprechend engmaschig sollten Fachkräfte aus der Medienbildung die Nutzung solcher Systeme durch Minderjährige begleiten.

KI-basierte Filter- und Schutzsysteme

Jugendschutzprogramme, KI-basierte Inhaltsmoderation und Altersverifikationssysteme stehen für ein Paradox, das den gesamten Regulierungsdiskurs durchzieht: Systeme, die zum Schutz von Kindern eingesetzt werden, können ihrerseits Risiken erzeugen und in Rechte von Kindern eingreifen (Dreyer 2025).

Rechtlich operieren Filtersysteme im Rahmen von § 11 JMStV, der die Anerkennung von Jugendschutzprogrammen regelt und die Einrichtungen der anerkannten Selbstkontrolle als Prüfungsinstanz einsetzt. Bei Altersverifikationssystemen kommt eine Spannung zwischen Schutzeffektivität und Datensparsamkeit hinzu: KI-basierte Altersschätzung durch Analyse von Gesichts- oder Verhaltensdaten wirft Fragen nach biometrischer Kategorisierung gemäß AI Act auf und die DSGVO verlangt hier Datenminimierung aus Prinzip. Das sind zwei Anforderungen, die sich nur schwer gleichzeitig erreichen lassen.

Das eigentliche Problem für die medienpädagogische Praxis liegt aber im Overblocking. KI-basierte Inhaltsfilter blockieren nicht nur schädliche Inhalte, sondern regelmäßig auch zulässige oder gerade besonders schützenswerte Inhalte – etwa LGBTQ+-Aufklärungsseiten, Informationen zur Sexualerziehung oder Suizidpräventionsangebote. Jugendliche in verletzlichen Situationen verlieren dadurch Zugang zu Informationen, die für sie sehr relevant sein können. Fachkräfte sollten insoweit Overblocking-Effekte kennen und erkennen und Kindern alternative Zugangswege eröffnen können. Das setzt voraus, dass man Schutzsysteme nicht unkritisch als Lösung akzeptiert, sondern sie als gestaltete Systeme mit eigenen Zielen, Fehlern und blinden Flecken begreift.

Was nützt ein Recht, das nicht greift?

Ein Überblick über den Rechtsrahmen wäre unvollständig ohne die Frage der Durchsetzung. Ein Recht, das formal besteht, aber in der Praxis nicht umgesetzt werden kann, ist für die Praxis ziemlich wertlos.

Das drängendste Beispiel ist hier der Konflikt zwischen nationalem Jugendschutzrecht und europäischem Binnenmarktrecht. Am Fallkomplex Pornhub/YouPorn zeigt er sich ganz greifbar: Die Landesmedienanstalten versuchen seit 2020, Pornoportale ohne zuverlässige Altersverifikation zu sperren. Im November 2025 hob das VG Düsseldorf die Sperrverfügungen der Behörden auf. Die Begründung: Der DSA sei als vollharmonisierendes EU-Regelwerk vorrangig und schließe nationale Alleingänge aus. Und außerdem könnten deutsche Jugendschutzvorschriften nach dem Herkunftslandprinzip nicht ohne weiteres gegen Anbieter aus dem EU-Ausland durchgesetzt werden – die betroffenen Anbieter hatten ihren Sitz in Zypern.⁵ Die Konsequenz ist schon spürbar: Wenn nationales Jugendschutzrecht für EU-basierte Anbieter blockiert ist, müssen wirksame Schutzregeln aus Brüssel kommen. Die neuen JMStV-Instrumente – Jugendschutzvorrichtungen, Mirror-Domain-Sperren, Payment-Blocking – wären dann „weitgehend ohne praktische Bedeutung“ (Kolter 2025).

Hinzu kommt ein Zuständigkeitsgeflecht, das selbst juristisch Bewanderte vor Orientierungsprobleme stellt. Das europäische KI-Büro überwacht die Vorgaben des AI Act für GPAI-Modelle, die nationalen Marktüberwachungsbehörden die in ihrem Land ansässigen Anbieter von Hochrisiko-KI-Systemen. Die Medienanstalten und die KJM überwachen den JMStV. Die BzKJ überwacht den plattformbezogenen Jugendschutz nach JuSchG und ihre unabhängige *Stelle zur Durchsetzung von Kinderrechten in digitalen Diensten* (KidD) die nationale Umsetzung der DSA-Vorgaben für kleinere Online-Plattformen. Die 17 Datenschutzbeauftragten in Deutschland überwachen die DSGVO. Und die EU-Kommission überwacht den DSA für die ganz großen Plattformen. Zwischen diesen Institutionen fehlen an vielen Stellen belastbare Abstimmungsmechanismen. Für medienpädagogische Fachkräfte, die einen konkreten Fall einordnen wollen, heißt das: Es ist keineswegs immer klar, wer überhaupt zuständig ist. Die Schutzlast verschiebt sich in diesem Durchsetzungs-Flickenteppich zwangsläufig auch auf Pädagogik und Familien.

Wo Reformen ansetzen müssen und wo die Medienpädagogik gefragt bleibt

Der Überblick zeigt einen komplizierten Rechtsrahmen, mit sehr unterschiedlichen Regulierungsdichten und Anwendungsfeldern. Bildungs-KI ist gut erfasst, Companion-Apps sind es kaum. Drei Reformlinien erscheinen hier vordringlich, auch wenn keine davon kurzfristig zu erwarten ist.

Zunächst sollten KI-Systeme – und hier insbesondere Chatbots und Companion-Apps, die von Kindern genutzt werden können – explizit in den Geltungsbereich des JMStV aufgenommen werden, wie es das EMR-Gutachten (Ukrow 2024) fordert. Das würde nicht alle Probleme lösen, aber es würde die Verantwortung von KI-Anbietern für den Jugendschutz klarstellen und ihre Einbeziehung in das bewährte deutsche System der regulierten Selbstregulierung ermöglichen.

Zweitens bräuchte es die ausdrückliche gesetzliche Pflicht, vor Markteinführung eines KI-Systems, das von Kindern genutzt werden kann, ein Child Rights Impact Assessment durchzuführen. Wir prüfen Spielzeug auf verschluckbare Kleinteile und die Einhaltung chemischer Grenzwerte, bevor es in den Handel kommt. Wir prüfen Medikamente auf Nebenwirkungen bei Kindern, bevor sie zugelassen werden. Dass ein KI-Chatbot, der Nähe und Empathie gegenüber Kindern simuliert und emotionale Bindung erzeugen kann, ohne umfassende Risikoprüfung auf den Markt kommt, ist der strukturelle Fehler im System des AI Act. Die UNICEF-Guidance (2025) und der Children & AI Design Code der 5Rights Foundation (2025) weisen hier einen besseren Weg.

Zudem muss die Durchsetzung in diesem rechtlichen Mehrebenensystem gestärkt werden. Die DSA-Leitlinien zu KI-basierten Plattformfunktionen sind ein guter erster Schritt. Aber sie müssen verbindlicher werden, wenn sie mehr sein sollen als wohlklingende Empfehlungen. Der in Vorbereitung befindliche Digital Fairness Act könnte hier einen strukturellen Fortschritt bringen, wenn er Jugendschutz als Gestaltungsproblem *aller* digitalen Dienste begreift und KI-basierte sowie manipulative Designpraktiken gegenüber Minderjährigen verbindlich einschränkt.

Mit Blick auf die medienpädagogische Praxis führen die gezeigte Löchrigkeit des Rahmens, seine Unbestimmtheit und die Durchsetzungshürden zu Handlungsbedarfen an zwei Stellen. Dort, wo der Rechtsrahmen besteht und tendenziell greift – bei Empfehlungssystemen, Bildgeneratoren, Lern- und Bewertungssystemen –, brauchen Fachkräfte vor allem *Rechtskompetenz und Awareness*. Sie sollten die Schutzrechte kennen, die Kindern zustehen, und sie ihnen und ihren Bezugspersonen vermitteln. Dort, wo der Rechtsrahmen aber schweigt oder seine Anwendung unklar ist – bei Companion-Apps mit ihren parasozialen KI-Beziehungen oder bei kumulativen Interaktionsrisiken, – ist medienpädagogische Begleitung derzeit die *einzige greifbare Schutzinstanz*. Hier braucht es gut informierte Fachkräfte, die früh mit Kindern und Jugend-

lichen ins Gespräch kommen, gemeinsam die Angebote und ihre Risiken diskutieren und sie vielleicht auch kritisch reflektiert ausprobieren. So kann Medienpädagogik die Versäumnisse des Rechtsrahmens zumindest teilweise kompensieren und bessere Befähigung in der Praxis bieten.

Was aber klar bleiben muss: Sie darf nicht zum Alibi für unterlassene oder suboptimale Regulierung werden. Medienpädagogik schafft die individuelle Befähigung, Regulierung schafft die strukturellen Bedingungen, unter denen Befähigung überhaupt nachhaltig greifen kann. Wir dürfen die Optimierung des Ordnungsrahmens für KI-Systeme, mit denen Minderjährige interagieren, deswegen nicht aus den Augen verlieren.

Autor

Dr. Stephan Dreyer: Senior Researcher für Medienrecht und Media Governance am Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI) in Hamburg; forscht zu Fragen des Jugendmedienschutzes, der Plattformregulierung und der Governance von KI-Systemen, mit besonderem Fokus auf Kinderrechte im digitalen Raum.

Anmerkungen

- 1 EU-Kommission, 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, 10.10.2025.
- 2 Die GPAI-Vorgaben des AI Act sind seit dem 2. August 2025 anwendbar. Für Modelle mit systemischem Risiko treten Pflichten zur Modellbewertung, Vorfalldokumentation, Meldung bei der EU-Kommission und Cybersicherheit hinzu (Art. 51 ff. AI Act).
- 3 SPIEGEL online: www.spiegel.de/netzwelt/apps/google-und-character-ai-legen-klage-wegen-suizid-eines-teenagers-bei-a-e9e7c379-46d1-4c19-9e1e-55f957b028e2 [Stand: 08.07.2026].
- 4 § 184b Abs. 1 StGB erfasst auch „wirklichkeitsnahe“ Darstellungen. Zur Diskussion über KI-ge-

neriertes CSAM vgl. den Jahresbericht 2024 von jugendschutz.net.

- 5 VG Düsseldorf, Beschl. v. 19.11.2025, 27 L 1347/24 u. a.; vgl. die Analyse bei Kolter 2025.

Literatur

- 5Rights Foundation (2025): Children & AI Design Code. London. Abrufbar unter: https://5rights.foundation.com/wp-content/uploads/2025/03/5rights_AI_CODE_DIGITAL.pdf [Stand: 15.03.2026].
- Andresen, Sünje/Dreyer, Stephan (2025): Über stete Tropfen und die Summe ihrer Teile. Kumulative Beeinträchtigungspotenziale und regulatorische Antworten des Kinder- und Jugendmedienschutzes. In: mediendiskurs.online, 17.01.2025.
- Bayor, Laura/Weinert, Christoph/Maier, Christian/Weitzel, Tim (2025): Social-Oriented Communication with AI Companions. Benefits, Costs, and Contextual Patterns. In: Business & Information Systems Engineering, Jg. 67, H. 5, 637–655.
- BzKJ (2026): KI and me. BzKJ für mehr Schutz und Orientierung im Umgang mit Chatbots. Pressemitteilung zum Safer Internet Day 2026. Abrufbar unter: <https://www.bzkgj.de> [Stand: 15.03.2026].
- Common Sense Media (2025): Talk, Trust, and Trade-Offs. How and Why Teens Use AI Companions. Abrufbar unter: www.common sense media.org/research/talk-trust-and-trade-offs-how-and-why-teens-use-ai-companions [Stand: 07.07.2026].
- Dreyer, Stephan/Schulz, Wolfgang (2018): Was bringt die Datenschutz-Grundverordnung für automatisierte Entscheidungssysteme? Potenziale und Grenzen der Absicherung individueller, gruppenbezogener und gesellschaftlicher Interessen. Gütersloh: Bertelsmann-Stiftung (Impuls Algorithmenethik #5). Abrufbar unter: https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/BSt_DSGVO undADM_dt.pdf [Stand: 07.07.2026].
- Dreyer, Stephan (2024): Die KI-Verordnung, ihr Verhältnis zu Kinderrechten im digitalen Raum und Optionen für Advocacy-Zugänge. Gutachten im Auftrag des Deutschen Kinderhilfswerks. Berlin. Abrufbar unter: www.dkhw.de/filestorage/1_Informieren/1.1_Unsere_Themen/Kinder_und_Medien/Kinderrechte_und_KI/DKHW_Schriftenreihe_Kinderrechte_und_KI.pdf [Stand: 07.07.2026].
- Dreyer, Stephan (2025): Alternativlose Staatspflichten und übergreifende Normen: Über die Ambivalenz rechtlicher Schutzaufträge in Zeiten der Digitalisierung. In: Crasemann, Leena/Lutz, Samantha/Müller, Theresa (Hrsg.): Paradoxien des Schützens. Schutzkonzepte und ihre Widersprüche. Berlin: Reimer, 127–141.
- Heaton, Dan/Nichele, Elena/Clos, Jeremie/Fischer, Joel E. (2023): „The algorithm will screw you“: Blame, social actors and the 2020 A Level results algorithm on Twitter. In: PLoS One, 2023 Jul 26; 18(7): e0288662. DOI: <https://doi.org/10.1371/journal.pone.0288662>.
- Kolter, Max (2025): Zugangssperren gegen YouPorn und Pornhub aufgehoben. Ein Todesurteil für den deutschen Jugendschutz. LTO.de, 11.12.2025. Abrufbar unter: www.lto.de/recht/hintergruende/h/vg-duesseldorf-271134724-jugendschutz-porno-seiten-sperre-eugh-dsa [Stand: 07.07.2026].
- mpfs – Medienpädagogischer Forschungsverbund Südwest (2025): JIM-Studie 2025. Jugend, Information, Medien. Stuttgart. Abrufbar unter: https://mpfs.de/app/uploads/2025/11/JIM_2025_PDF_barrierearm.pdf [Stand: 07.07.2026].
- Ukrow, Jörg (2024): Kinder- und Jugendmedienschutz und Künstliche Intelligenz – Herausforderung für den Jugendmedienschutz-Staatsvertrag (JMStV)? Stand und Reformüberlegungen unter besonderer Beachtung generativer KI und unter Berücksichtigung des geplanten Gesetzes über künstliche Intelligenz der EU. Saarbrücken. Abrufbar unter: www.kjm-online.de/fileadmin/user_upload/KJM/Service/Publikationen/Studien_Gutachten/KI_Gutachten_2024.pdf [Stand: 07.07.2026].
- UNICEF (2025): Guidance on AI and Children. 3. Aufl. New York: UNICEF. Abrufbar unter: <https://www.unicef.org/innocenti/media/11991/file/UNICEF-Innocenti-Guidance-on-AI-and-Children-3-2025.pdf> [Stand: 07.07.2026].

Lizenz

Der Artikel steht unter der Creative Commons Lizenz **CC BY-SA 4.0**. Der Name des Urhebers soll bei einer Weiterverwendung genannt werden. Wird das Material mit anderen Materialien zu etwas Neuem verbunden oder verschmolzen, sodass das ursprüngliche Material nicht mehr als solches erkennbar ist und die unterschiedlichen Materialien nicht mehr voneinander zu trennen sind, muss die bearbeitete Fassung bzw. das neue Werk unter derselben Lizenz wie das Original stehen. Details zur Lizenz: <https://creativecommons.org/licenses/by-sa/4.0/legalcode>.

Einzelbeiträge werden unter www.gmk-net.de/publikationen/artikel veröffentlicht.