2023 BERICHT

Jugendschutz im Internet

Risiken und Handlungsbedarf

JUGEND SCHUTZ.NET

Kontakt
jugendschutz.net
Kaiserstraße 22, 55116 Mainz
Tel.: 06131 3285-20
buero@jugendschutz.net
www.jugendschutz.net
www.x.com/jugendschutznet

Verantwortlich
Stefan Glaser

Redaktion
Steffen Eisentraut, Andreas Hautz, Murat Özkilic

Grafische Gestaltung
elements of art

Stand
Juli 2024

Finanziert von:

kjm Kommission für Jugendmedienschutz
die medienanstalten

Gefördert vom:
Bundesministerium für Familie, Senioren, Frauen und Jugend

Im Rahmen von:
GAMM Gutes Aufwachsen mit Medien

Kofinanziert von der Europäischen Union

Digitaler Umbruch erfordert konzertierten Jugendmedienschutz

Die Welt der Games, Challenges und Shorts lockt täglich Kinder und Jugendliche ins Netz. Der Nutzungsvielfalt und Attraktivität von Angeboten stehen leider schon lange negative Erfahrungen gegenüber: Sexualisierte Gewalt und Mobbing, Beiträge, die sich gegen unsere Demokratie und eine diverse Gesellschaft wenden oder belastende Gewaltbilder sind Normalität im nutzergenerierten Kosmos. Seit geraumer Zeit wirft zudem die rasante Entwicklung und Verbreitung von KI-Systemen Fragen nach Risiken auf, die sich für Heranwachsende bei der Anwendung ergeben. Denn die Kehrseite von hilfreichen Tools sind Phänomene wie Deepfakes, die kaum mehr von echten Inhalten zu unterscheiden sind.

Beim Blick auf das vergangene Jahr wird deutlich, dass die Probleme für Kinder und Jugendliche in der digitalen Welt nicht geringer werden. Es zeigt sich auch, dass Anbieter die Jüngsten bei der Nutzung ihrer Angebote weiterhin nicht effektiv vor der Konfrontation mit gefährdenden Inhalten und Übergriffen schützen: Meldesysteme versagen und führen nicht oder nicht schnell genug zur Löschung von Verstößen. Altersdifferenzierte Ansätze laufen ins Leere, weil nicht verlässlich überprüft wird, wie alt die Nutzenden tatsächlich sind. Das ist angesichts der potenziellen Gefährdungen, die in beliebten Diensten bestehen, unbegreiflich.

Nicht nur Online-Welten verändern sich derzeit stark und bringen neue Nutzungsrisiken hervor. Durch den Digital Services Act (DSA), der einen sicheren Raum für Nutzer:innen des Internets schaffen und deren Grundrechte wahren soll, wandelt sich europaweit auch das System des Kinder- und Jugendmedienschutzes. Die großen, international operierenden Plattformen werden nun von der EU reguliert. Damit dieser positive Ansatz wirken kann und Maßnahmen der Kommission greifen, müssen national zuständige Fach- und Aufsichtsstellen eingebunden werden und gut zusammenwirken.

Mit jugendschutz.net haben die Jugendministerien der Länder vor vielen Jahren eine Stelle geschaffen, die am Puls der Zeit agiert. Sie greift Entwicklungen im Arbeitsfeld rasch auf, schätzt Jugendschutzprobleme präzise und vorausschauend ein und leitet Handlungsbedarfe für Politik, Aufsicht und Praxis ab. Sie unterstützt die Medienaufsicht von Ländern und Bund durch einzelfall- und strukturbezogene Prüfungen von Angeboten. Und sie ist mit wichtigen Akteur:innen national wie international vernetzt. Mit dieser jahrelangen Erfahrung und Expertise bildet jugendschutz.net im sich verändernden System eine wichtige Konstante und kann auch zukünftig dazu beitragen, Kindern ein gutes Aufwachsen mit dem Internet zu ermöglichen.

Stefan Glaser
Leiter von jugendschutz.net

Aktuelle Erkenntnisse und weiterführende Informationen

GEFAHREN UND RISIKEN

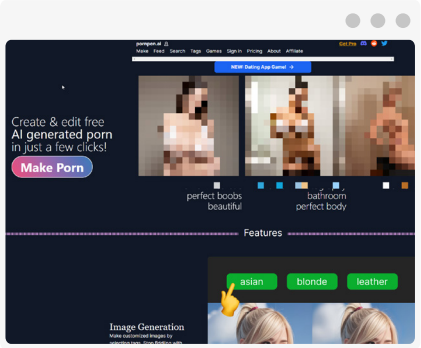
Generative KI: Deepfakes und realistische Fälschungen verschärfen Risiken

2023 ist die Entwicklung von Systemen der Künstlichen Intelligenz, insbesondere generativer KI, rasant vorangeschritten. Die neuen Technologien bestimmten mediale Debatten und hielten Einzug in den Alltag von Kindern und Jugendlichen. Viele Anwendungen sind einfach zu bedienen, frei zugänglich und erfordern keine Kenntnisse im Programmieren. Mit wenigen Textanweisungen („Prompts") erzeugen ChatGPT und ähnliche Programme Texte, Bilder, Sprache und Videos zu beliebigen Themen. Anwendungen sind in Smartphones und Social-Media-Dienste integriert.

Während die Technik junge Menschen etwa bei Schularbeiten unterstützen und kreative Fähigkeiten fördern kann, verschärft sie bestehende Risiken im Internet wie sexualisierte Gewalt, Mobbing und Extremismus.

So genannte Deepfakes lassen sich inzwischen im Handumdrehen erstellen und verbreiten. Viele der generierten Fälschungen sehen täuschend real aus und sind kaum von tatsächlichen Fotos zu unterscheiden. Gepaart mit Nacktheit (Deepnudes) oder Pornografie (Deepporn) entstehen hieraus schnell Cybermobbing oder sexualisierte Gewalt. Wie leicht junge Menschen zu Opfern werden können, zeigen Fälle aus Spanien. Dort fertigten Schüler:innen mithilfe von KI Nacktbilder von Mitschülerinnen an und brachten sie in Umlauf – mit dramatischen Folgen für die Betroffenen.

Zwar sperren Social-Media-Anbieter in ihren KI-Systemen Schlüsselbegriffe für Inhalte wie Missbrauchsdarstellungen, Gewalt und Pornografie, um die Erzeugung betreffender Inhalte zu verhindern. User:innen können diesen Schutz jedoch einfach durch alternative Beschreibungen umgehen. Es gibt auch Dienste, die auf das Erzeugen von pornografischem Material spezialisiert sind: Nach Eingabe von Merkmalen wie Alter, Größe oder Geschlecht werden Pornos wunschgemäß erstellt und können heruntergeladen werden.



Auf Seiten für KI-Bilderstellung können User:innen eigene pornografische Inhalte erzeugen. (Bild im Original unverpixelt)

In der Online-Kommunikation wird es zunehmend schwerer zu erkennen, ob sich hinter dem Gegenüber eine tatsächliche Person oder ein KI-System verbirgt. Dies erschwert es insbesondere Kindern und Jugendlichen abzuschätzen, wie vertrauenswürdig übermittelte Informationen sind oder welche persönlichen Daten sie problemlos preisgeben können. Fremde können sich mit Hilfe von Chatbots und Stimmgeneratoren noch einfacher als Gleichaltrige ausgeben. Sie können dadurch leichter Vertrauen aufbauen, sensible persönliche Informationen abgreifen und zu Zwecken des Groomings missbrauchen.

Daneben liefern KI-Systeme auch falsche oder unpassende Ergebnisse und bringen Kinder dadurch in Gefahr: Tests von jugendschutz.net mit dem Chatbot MyAI von Snapchat führten bei einer vermeintlich 14-jährigen Userin zum Alkohol-Trinkspiel „Flunkyball“ und zum Horrorfilm „Saw“ (FSK 18).

KI-generierte Beiträge und Identitäten werden auch genutzt, um extremistische Propaganda und Desinformation zu verbreiten. Besonders wirkmächtig ist dabei, wenn die Akteure Unterhaltung mit manipulierenden Inhalten verbinden. Im Zuge einer jugendaffinen Challenge für KI-generierte Bilder relativierten Rechtsextreme den Holocaust oder verharmlosten Terrorismus. Tausendfach geteilt wurde z. B. das Plakat eines vermeintlich neuen Disney-Films mit dem Titel „Caust“, das trügerisch echt im Pixar-Stil durch KI generiert wurde. Das Bild zeigt Adolf Hitler, als Figur animiert, lächelnd vor einem Konzentrationslager.

Hitler und KZs im populären “Pixar”-Filmstil: Per bildgenerativer KI wird der Holocaust verniedlicht. (Quelle: TikTok)

Hassinhalte: Extremist:innen nutzen Kriegsleid und Klimawandel für Propaganda

Extremist:innen nutzen aktuelle Krisen, um Kinder und Jugendliche im Netz zu indoktrinieren und zu radikalisieren. Der Klimawandel oder die Kriege in der Ukraine und im Nahen Osten sind für junge Menschen wichtige Themen, über die sie sich online informieren. Hierbei stoßen sie schnell auf Desinformationen, Hassinhalte und Gewaltdarstellungen.

Junge Menschen, die sich auf Plattformen wie TikTok, Instagram oder YouTube für Klimaschutz stark machen, werden schnell zur Zielscheibe von herabwürdigenden Posts. Kommentare stellen sie als unzurechnungsfähig und „geisteskrank" dar und legen ihnen nahe, sich in psychiatrische Behandlung zu begeben.

Gegenüber weiblichen Aktivist:innen werden frauenfeindliche Diffamierungen, sexualisierte Kommentare und sogar Vergewaltigungsfantasien geäußert.

Auf Kinder und Jugendliche kann die Konfrontation mit derlei abwertenden und hasserfüllten Aussagen negative Auswirkungen haben. In Social Media erleben sie eine hochemotionale und polarisierende Debattenkultur, die grundlegende soziale Wertevorstellungen beeinflusst. Eine vergiftete Atmosphäre beim Austausch über politische Probleme steht Entwicklungszielen wie der Achtung anderer Personen und Meinungen entgegen.

Klimaaktivistinnen werden aufgefordert, erotische oder pornografische Inhalte zu publizieren, etwa auf der einschlägigen Plattform OnlyFans. (Quelle: Twitter/X; Original unverpixelt)

Auch der Terrorangriff der Hamas auf Israel am 7. Oktober 2023 wird missbraucht, um Stimmung zu machen und extremistische Ideologien zu verbreiten. In den Tagen und Wochen nach dem Überfall kam es auf jugendaffinen Diensten wie Instagram und TikTok zur Verbreitung von drastischen Gewaltdarstellungen, Desinformation sowie antisemitischer und muslimfeindlicher Propaganda. Verstörende Bilder und Videos von Verschleppung und Misshandlung, teils auch von Kindern, wurden massenhaft verbreitet. Sowohl pro-palästinensische als auch pro-israelische Gruppen teilten drastische Opferaufnahmen.

Unter Verweis auf die israelische Siedlungspolitik verharmlosten viele Akteure die Attacke der Hamas und versuchten sie zu rechtfertigen. In den Beiträgen fand jugendschutz.net vor allem nach dem militärischen Gegenangriff antisemitische Verschwörungserzählungen, Gewaltdrohungen und volksverhetzende Inhalte. User:innen relativierten den Holocaust, etwa durch Gleichsetzung des israelischen Vorgehens mit den Verbrechen der Nationalsozialisten in Deutschland. Dabei kamen auch KI-generierte Inhalte zum Einsatz. Diese zeigten Juden etwa als Vampire, die es auf das Blut unschuldiger Babys abgesehen hätten. Gleichzeitig fanden sich Abwertungen und Hetze gegen Muslim:innen oder Menschen, die für arabisch gehalten wurden.

Israel wird mit dem deutschen NS-Regime gleichgesetzt. (Quelle: Instagram)

Unter dem Vorwand der Israel-Solidarität schürten Extremist:innen Ressentiments gegen muslimische Bevölkerungsgruppen und stellten sie pauschal als Gefahr dar.

INACH

jugendschutz.net kooperiert seit über 20 Jahren im International Network Against Cyber Hate (INACH) mit derzeit 35 Mitgliedern aus 28 Ländern. Ziele des Netzwerks sind die schnelle Löschung rechtswidriger Hassbeiträge, der Austausch von Wissen und die Stärkung von Zivilcourage im Netz.

Seit 2016 überprüfen INACH und europäische Meldestellen im Auftrag der EU-Kommission, wie Social-Media-Dienste, die dem EU-Verhaltenskodex zur Bekämpfung illegaler Hassrede im Internet beigetreten sind, auf Meldungen von Hassinhalten reagieren.
(inach.net)

Sexualisierte Gewalt: Videochats mit Kindern für intime Aufnahmen missbraucht

2023 dokumentierte jugendschutz.net 4.983 Fälle mit Darstellungen sexualisierter Gewalt.

Ein Großteil der registrierten Verstöße sind Aufnahmen aus Videochats. Sie zeigen überwiegend minderjährige Mädchen – häufig vor dem Eintritt in die Pubertät – allein oder gemeinsam mit Gleichaltrigen vor der Kamera. Leichtbekleidet oder nackt, nehmen sie sexualisierte Posen ein oder führen sexuelle Handlungen an sich selbst durch.

Die Aufnahmen entstehen oftmals in der Folge von Cybergrooming. Auch Bilder und Videos, die wahrscheinlich einvernehmlich im Rahmen von Sexting entstanden, werden missbräuchlich zugänglich gemacht. Vereinzelt gingen Hinweise auf strafbare KI-generierte Darstellungen ein, die sexualisierte Gewalt gegen Kinder und Jugendliche zeigen.

Ein anhaltendes Problem ist die Vernetzung von Pädokriminellen über das Netz. Sie tauschen dort beispielsweise Darstellungen sexualisierter Gewalt. Auch Alltagsbilder von Kindern stellen die Täter:innen durch Kommentare in einen sexualisierten Kontext. Die verwendeten Keywords, Tags und Albentitel bringen Kinder mit sexuellen Handlungen in Verbindung und machen die Intention deutlich.

2023

4.983

Fälle von Darstellungen sexualisierter Gewalt

In einigen Fällen kommt es zu direkten Aufforderungen, Darstellungen sexualisierter Gewalt zu tauschen. Für die Vernetzung mit Gleichgesinnten weichen die Täter:innen auf Dienste wie Telegram oder andere Messenger aus.

Ein Beispiel aus einer Sammlung von Bildern mit dem Titel "Kleine Mädchen lecken Eiscreme", die sexuell kommentiert werden. (Bild im Original unverpixelt)

Mit „Sugardating“ rückte ein Phänomen in den Blick, welches ein erhebliches Gefährdungspotenzial für Kinder und Jugendliche aufweist: Sie kommen hierbei direkt mit Erwachsenen in Kontakt, die sexuelle Absichten verfolgen. Auf Portalen wie mysugardaddy.eu können sich ältere (zumeist männliche) User:innen mit jüngeren Personen zu pseudoromantischen Treffen gegen Geld, Geschenke oder andere Zuwendungen verabreden. Beim Test mit einem erkennbar als minderjährig angelegten Profil auf mysugardaddy.eu erhielt jugendschutz.net binnen 30 Minuten private Nachrichten von Erwachsenen. Sie fragten direkt „nach lockeren Dates und Sex gegen Bezahlung“.

Obwohl die AGB der Plattform die Nutzung von unter 18-Jährigen ausschließen, existiert keine Altersprüfung bei der Registrierung. jugendschutz.net stieß auf Profilnamen wie „KLEINESMÄDCHEN_MA“ oder „13JAHREJUNGE“, die darauf hindeuteten, dass auch Minderjährige den Dienst nutzen.

Die Verwendung entsprechender Hashtags auf TikTok oder Instagram zeigt, dass das Thema bei Kindern und Jugendlichen präsent ist. Bei der Sichtung von Livestreams auf TikTok und Likee beobachtete jugendschutz.net wiederholt Kommentare wie „Treffen für Geld“ oder „Was dazu verdienen“. Kombiniert waren die Kommentare teils mit der Bitte um private Kontaktaufnahme über die interne Nachrichtenfunktion oder Messenger wie WhatsApp oder Snapchat.

INHOPE

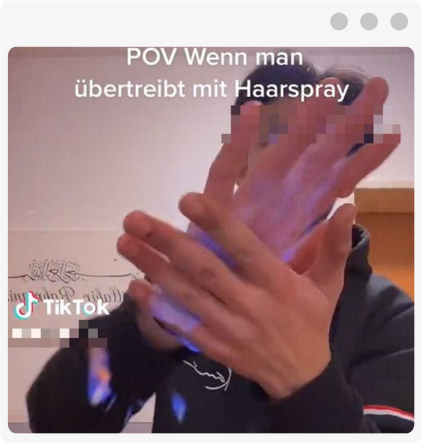
jugendschutz.net arbeitet als Gründungsmitglied mit den Partnern der International Association of Internet Hotlines (INHOPE) zusammen. Ziel ist die Bekämpfung von Darstellungen sexualisierter Gewalt gegen Kinder im Netz.

Die beteiligten Organisationen geben Verstöße über eine gemeinsame Datenbank weiter. Sie erarbeiten Best Practices und tauschen Fachwissen sowie technisches Know-How aus. Das Netzwerk hat aktuell weltweit 54 Mitglieder aus 50 Ländern. (inhope.org)

Challenges, Pranks und Fitness: Trends mit gefährlichen Folgen

In Social-Media-Diensten wie TikTok gibt es viele Trends, die Kinder und Jugendliche zum Mitmachen einladen und schnell viral gehen. Die Bandbreite ist vielfältig und reicht von spaßigen Wettbewerben bis hin zu Lifestyletipps im Bereich Ernährung, Gesundheit und Körperbewusstsein. Insbesondere Beiträge mit Challenges und Pranks (Streiche) erzielen in Social Media viele Klicks.

Weit verbreitet war im vergangenen Jahr die Hot-Chip-Challenge. Bei ihr muss ein extrem scharfer Tortilla-Chip gegessen werden. Danach soll möglichst lange nichts getrunken werden, um die Schärfe nicht zu neutralisieren. Dies kann schwerwiegende Folgen wie Atemnot, Magenkrämpfe und Kreislaufprobleme haben.

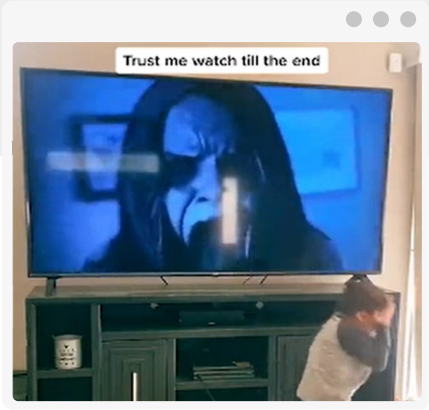


Hochgefährlich: Bei einer Firefinger-Challenge entzündet ein User versehentlich die ganze Hand und Teile seiner Jacke. (Quelle: TikTok; Original unverpixelt)

jugendschutz.net beobachtete viele Beiträge, in denen vor allem junge Menschen aufgerufen wurden, Mut zu beweisen und mitzumachen. Die Chips konnten lange an vielen Kiosken ohne Zugangshürde erworben werden, inzwischen haben einige Bundesländer den Verkauf verboten.

Zu einem ähnlich gefährlichen Trend avancierte die Firefinger-Challenge. Dabei benetzen Jugendliche einen Finger mit brennbarer Flüssigkeit und zünden ihn an. Die Flamme soll anschließend während eines Songs bei einer bestimmten Liedzeile mit der anderen Hand gelöscht werden. Videos zeigen, wie das Feuer außer Kontrolle gerät und auf die gesamte Hand überspringt oder weitere Teile des Körpers erfasst. Bei offensichtlich gefährlichen Challenges verbreiten User:innen oft Tutorials, die den trügerischen Anschein erwecken, gefahrlos mitmachen zu können. Die vermeintlich spaßige Idee und massenhafte Dokumentation der Mutproben verleiten zusätzlich zur Nachahmung.

TikTok und weitere Dienste sperren Hashtags zu gefährlichen Challenges meist schnell. Über andere Schlagworte sind die Videos allerdings weiter aufrufbar.



Auf ein ruhiges Video folgt das Horrorbild: Der geprankte Junge schlägt panisch die Hände vor das Gesicht. (Quelle: TikTok)

Schnell viral gingen darüber hinaus Beiträge, die Trenddrogen wie Lachgas als vermeintlich unschädlich darstellten und den Konsum bewarben. Utensilien, z. B. mit Zusatzgeschmack befüllte Sahnespenderkapseln, waren über Onlineshops und zugehörige Social-Media-Accounts erhältlich. Was als harmlose und legale Partydroge dargestellt wird, ist hochgefährlich: Das häufige Inhalieren kann zu schweren neurologischen Schäden führen. Eine kritische Auseinandersetzung mit Risiken und Folgen des Missbrauchs findet in den Angeboten kaum statt.

Viele Nachahmer finden Pranks, bei denen Kinder zur Belustigung der Community absichtlich in emotionale Ausnahmezustände gebracht werden. In der Regel nehmen hierbei Jugendliche (z. B. ältere Geschwister), Eltern oder andere Bezugspersonen die Rolle des so genannten Pranksters ein. Sie bringen ihre Opfer in unheimliche, vermeintlich gefährliche oder unangenehme Situationen, um bei ihnen Angst, Ekel oder gar Verzweiflung hervorzurufen.

Bei manchen „Streichen" nutzen Prankster App-Effekte und legen mithilfe von Filtern beispielsweise Geistererscheinungen, Monster oder Spinnen über die Videos ihrer Opfer, um sie zu erschrecken. Das Smartphone wird so positioniert, dass die geprankten Kinder die Veränderungen auf dem Bildschirm wahrnehmen können. Auf diese Art wird Kindern vorgegaukelt, dass ihnen Spinnen über das Gesicht krabbeln oder Geister im Raum sind.

Beim TV-Scare-Prank werden Kinder von einer Horrorfigur erschreckt, die während eines harmlosen Videos plötzlich auf dem Fernseher auftaucht. Die Kinder sind geschockt und rennen panisch davon.

Hohe Sogwirkung entfaltete die Eggcrack-Challenge auf TikTok: Eltern schlagen aus Spaß ein rohes Ei am Kopf ihrer Kinder auf, filmen die Reaktion und stellen das Video ins Netz. Die Aktion soll Zuschauer:innen belustigen und Klicks generieren. Kinder reagieren häufig erschrocken, weinen oder schlagen um sich.

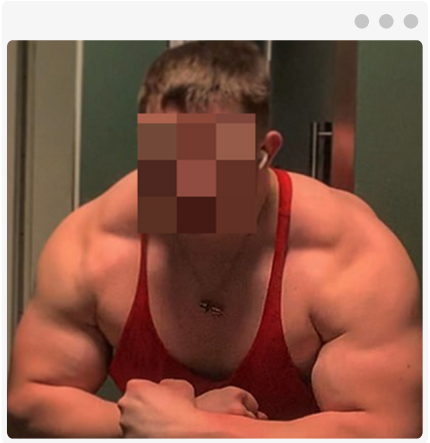
Gepranktes Kind reagiert auf Eggcrack-Challenge: Seine Reaktion wird durch Lachsmileys ins Lächerliche gezogen. (Quelle: TikTok; Original unverpixelt)

Alle "Streiche" der Prankster zielen darauf ab, emotionale Reaktionen bei den Kindern hervorzurufen. Diese sind der unangenehmen oder beängstigenden Situation schutzlos ausgeliefert. Besonders bedenklich: Noch sehr kleine Kinder fühlen sich in der Gegenwart von Eltern oder Geschwistern eigentlich sicher, sie vertrauen auf deren Schutz. Dieses Vertrauen wird durch die Pranks erschüttert. Sie werden in ihren Emotionen öffentlich bloßgestellt. Zudem können die Beiträge missbräuchlich weiterverbreitet und in anderen Kontexten zweckentfremdet werden, z. B. für Cybermobbing.

Trends in Social Media müssen nicht zwangsläufig auf kurzfristigen Nervenkitzel oder Grenzüberschreitung abzielen, um riskant zu sein. „Fitfluencing", das sich immer größerer Beliebtheit erfreut, setzt niedrigschwelliger an. Kinder und Jugendliche lockt die Vorstellung, mit der Optimierung des eigenen Körpers Geld und Anerkennung zu verdienen. Insbesondere (Kraft-)Sport wird dabei häufig zum allumfassenden Lifestyle erhoben. Die Darstellungen der durchtrainierten Gleichaltrigen können zu hohem Druck führen, ein vergleichbares Aussehen zu erreichen.

Trainingsmethoden und Ernährungsweisen der Fitfluencer:innen und die öffentliche Selbstinszenierung durch Kleidung, Sprache und Gestik werden kopiert. Oftmals empfehlen die Protagonist:innen zum Erreichen der Ziele ungesunde Nahrungsergänzungsmittel und Trainingseinheiten weit über Belastbarkeitsgrenzen hinaus. Ein Hobby, das Spaß bringt, geht so schnell zu Lasten der Gesundheit und fördert überzogene und unrealistische Körperideale.

Zunehmend posten Fitfluencer:innen Bilder in optisch perfekter Form, z. B. durch den Einsatz von "Beauty"-Filtern, KI oder Bildbearbeitung. Diese verzerren die Vorstellung vom idealen Körper zusätzlich und erhöhen den Erwartungsdruck.



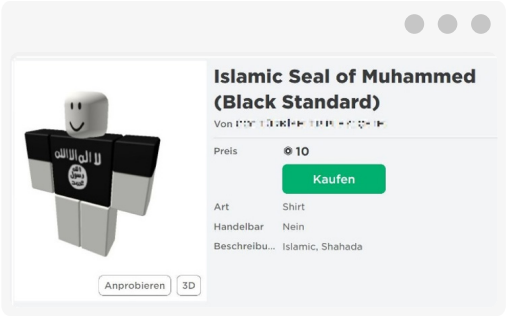
Ein 15-jähriger Fitfluencer zeigt seinen Follower:innen seine Muskeln. (Quelle: Instagram; Original unverpixelt)

Spieleplattform Roblox: Extremismus, Belästigung und Kostenfallen

Roblox ist mit täglich über 70 Millionen aktiven Nutzer:innen eine der beliebtesten Spieleplattformen weltweit. Der Dienst ist unter Kindern und Jugendlichen besonders populär: Anfang 2023 war knapp die Hälfte aller Spieler:innen unter 13 Jahre alt.

Attraktiv macht die Plattform vor allem die große Bandbreite an Spiel-, Gestaltungs- und Kommunikationsmöglichkeiten. Nach Belieben können dort eigene virtuelle Spielewelten (genannt „Erlebnisse") erschaffen und visuell gestaltet werden. Roblox fördert jedoch nicht nur Kreativität und Spielfreude, sondern birgt auch gefährdende Inhalte.

jugendschutz.net fand in Gruppen, Erlebnissen oder auf Avatar-Kleidung rechtsextreme und islamistische Inhalte, darunter verfassungswidrige Kennzeichen wie das Schwarze Banner der Terrororganisation Islamischer Staat (IS), Hakenkreuze und SS-Runen. In einer Spielewelt konnten Nutzer:innen auf einer Nachbildung der norwegischen Insel Utøya schwer bewaffnet andere Menschen erschießen. Dort hatte der Rechtsextreme Anders Breivik 2011 einen Anschlag verübt und dabei 77 junge Menschen ermordet. Weiterhin gab es detailgetreue nationalsozialistische Konzentrationslager; nebst der Möglichkeit, dem Avatar das Aussehen von NS-Offizieren zu geben.



Shirt mit IS-Flagge: Nutzer:innen können Kleidung kaufen, ihren Avataren anziehen und so auch (in Deutschland) verbotene Symbole verbreiten. (Quelle: Roblox; Original unverpixelt)

Im Erlebnis „Öffentliches Badezimmer" imitieren Nutzer:innen in Badewannen sexuelle Handlungen. (Quelle: Roblox; Original unverpixelt)

Unzureichend ist auch der Schutz vor Belästigung und Cybergrooming. Nutzer:innen machen mit einschlägigen Keywords auf sich aufmerksam und sexualisieren Konversationen durch eindeutige Smileys. Zudem werden bei Interaktionen Bewegungen und Handlungen (z. B. Liegestütze) von Avataren zur Imitation sexueller Handlungen zweckentfremdet. Roblox verbietet all dies in seinen Community-Regeln zwar und setzt einen strengen Wortfilter ein. Dennoch lassen sich immer wieder Übergriffe dokumentieren.

Effektive Meldesysteme können in solchen Fällen zumindest schnell Abhilfe schaffen und vor weiteren Konfrontationen schützen. Bei Tests schnitt Roblox allerdings wenig zufriedenstellend ab: Von 26 gemeldeten Inhalten, die gegen den JMStV verstießen, entfernte der Dienst nach User:in-Meldung lediglich fünf.

Roblox ist grundsätzlich kostenfrei. Es lassen sich jedoch In-Game-Käufe tätigen. Hierzu müssen Nutzer:innen die plattformeigene Währung (Robux) erwerben. Damit können sie ihren Avatar mit speziellen Skins und Items ausstatten, um ihn zu individualisieren und zu verbessern. Der Anreiz kann schnell zum Sog und damit zur erheblichen Kostenfalle werden. Obwohl Käufe erst ab 18 Jahren oder mit Zustimmung der Erziehungsberechtigten erlaubt sind, holt der Dienst diese nicht aktiv ein.

Roblox hat mit der elterlichen Begleitmöglichkeit des Accounts für den Zugriff auf Inhalte und die Nutzung von In-App-Käufen zwar Vorsorgemaßnahmen getroffen, um Kinder und Jugendliche zu schützen. Diese Vorkehrungen reichen jedoch nicht aus, da sie kaum Schutz vor Gefährdungen durch nutzergenerierte Inhalte bieten. Mit vielen kind- und jugendrelevanten Diensten teilt Roblox ein Kernproblem: Bei der Registrierung findet keine verlässliche Altersprüfung statt. Solange Nutzer:innen sich leicht unter Angabe eines falschen Alters anmelden können, greifen selbst die besten altersdifferenzierten Vorsorgemaßnahmen nicht.

safer internet de

Mit den „Safer Internet Centres" fördert die EU sichere Kommunikation im Internet, in Deutschland gebündelt unter saferinternet.de: das Awareness-Center klicksafe.de, die Hotlines von jugendschutz.net, eco und FSM sowie das Kinder- und Jugendtelefon Nummer gegen Kummer. (saferinternet.de)

SCHUTZ UND TEILHABE

Über 7.600 Verstoßfälle registriert

jugendschutz.net prüft Angebote im Netz, die bei Recherchen entdeckt oder über die Online-Beschwerdestelle, Behörden und Partnerorganisationen gemeldet werden. 2023 wurden 7.645 Verstoßfälle bearbeitet (2022: 7.363).

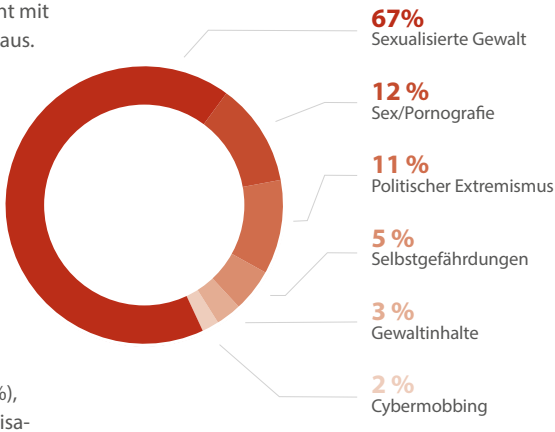
Die thematische Verteilung ist vergleichbar mit den Vorjahren. Sexualisierte Gewalt macht mit zwei Dritteln weiterhin den Löwenanteil aus.

Beim Gros der Verstoßfälle handelte es sich um Angebote, deren Verbreitung nach dem Jugendmedienschutz-Staatsvertrag (JMStV) absolut unzulässig ist. Diese Inhalte dürfen von Anbietern nicht verbreitet werden, auch nicht an Erwachsene. 2023 traf dies auf 82 % zu (2022: 84 %). Dabei handelte es sich vor allem um Straftatbestände wie die Verbreitung von Kinderpornografie (73 %), Kennzeichen verfassungswidriger Organisationen (9 %) und Jugendpornografie (5 %).

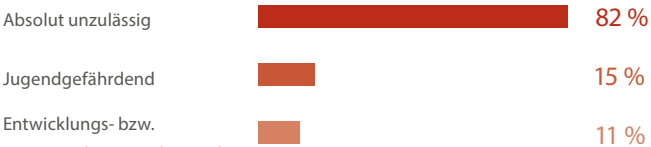
REGISTRIERTE VERSTOSSFÄLLE 2023

7.645

Erneut Steigerung gegenüber den Vorjahren.



Sexualisierte Gewalt macht Gros der Fälle aus.



Im Fokus der Arbeit: Absolut unzulässige Fälle.

90 % der Verstöße zum Jahresende entfernt

jugendschutz.net weist Anbieter und Selbstkontrolleinrichtungen auf Verstöße gegen den Jugendmedienschutz hin. Ziel ist eine schnelle Abhilfe und damit unmittelbare Beseitigung der Beeinträchtigung oder Gefährdung für Kinder und Jugendliche. Diese Aktivität erfolgte im vergangenen Jahr bei 3.210 Verstoßfällen.

Ist ein verantwortlicher Anbieter greifbar, gibt jugendschutz.net den Fall an die Kommission für Jugendmedienschutz (KJM) bzw. die zuständige Landesmedienanstalt zur Einleitung eines Verfahrens ab. 2023 geschah dies bei 105 Verstoßfällen. Zusätzlich wurden 252 Fälle an die KJM zur Indizierung durch die Bundeszentrale für Kinder- und Jugendmedienschutz (BzKJ) geleitet.

Enthalten Angebote kinder- bzw. jugendpornografische Darstellungen oder besteht Gefahr für Leib und Leben, werden die Strafverfolgungsbehörden direkt von jugendschutz.net informiert. Dies war bei 3.582 Verstoßfällen erforderlich. Damit machte diese Aktivität 2023 den größten Anteil aus. Fälle mit Missbrauchsdarstellungen ohne deutschen Ermittlungsansatz werden an INHOPE-Partnermeldestellen abgegeben.

Am Jahresende waren bei 6.902 Fällen (90 %) die Verstöße beseitigt.

Hinweise an Anbieter und Selbstkontrollen

3.210

Hauptsächlich sexualisierte Gewalt und politischer Extremismus.

Aufsichtsfälle an KJM

105

Mehrheitlich Pornografie und indizierte Inhalte.

Indizierungsfälle an KJM

252

Vorwiegend tierpornografische Inhalte.

Weitergabe an Strafverfolgung

3.582

Sexualisierte Gewalt.

Weitergabe an INHOPE-Partner

280

Sexualisierte Gewalt.

Überprüfung von Vorsorgemaßnahmen von Anbietern

Um Kindern und Jugendlichen eine sichere und altersgerechte Teilhabe im Internet zu ermöglichen, sind Betreiber von Plattformen inzwischen gesetzlich verpflichtet, geeignete Vorsorgemaßnahmen zu treffen. In Deutschland formuliert das 2021 novellierte Jugendschutzgesetz (JuSchG) Vorschriften für einen besseren Schutz von Minderjährigen. Mit dem Digital Services Act (DSA) existiert darüber hinaus ein EU-weites Regelwerk, welches Anbieter von Internetdiensten in die Pflicht nimmt, systemische Risiken auf ihren Plattformen zu minimieren.

jugendschutz.net hält Vorsorgemaßnahmen bei Diensten, die für Kinder und Jugendliche besonders relevant sind, kontinuierlich im Blick. 2023 fielen darunter TikTok, Instagram, YouTube, Snapchat und Facebook. Weitere Dienste wurden anlassbezogen und punktuell überprüft.

jugendschutz.net prüft Vorsorgemaßnahmen in verschiedenen Bereichen:

- verlässliche Mechanismen bei der Registrierung und Nutzung
- altersdifferenzierte Funktionalitäten und Profileinstellungen

- schnell erreichbar und leicht bedienbar
- zeitnahe Abhilfe bei gemeldeten Verstößen

- sichere Voreinstellungen und nachträgliche Einstellungsmöglichkeiten
- einfach zu konfigurieren

- kindgerecht aufbereitet
- klar verständlich und vollständig

- gut auffindbar und verständlich
- praxisnahe Tipps, z. B. zum sicheren Verhalten
- Unterstützung im Notfall, z. B. durch Verweis auf externe Beratungsangebote

Fehlende Altersprüfung bleibt das größte Problem

Eine zuverlässige Altersprüfung von User:innen in Online-Diensten ist Mangelware und bleibt die zentrale Schwachstelle in den Schutzkonzepten der Anbieter. Zwar legen fast alle von jugendschutz.net beobachteten Plattformen ein Mindestalter fest und bieten altersdifferenzierte Zugänge an. Aber: Die Anbieter kontrollieren das Alter nicht oder nur unzureichend. Bei der Registrierung fragen die Plattformen in der Regel lediglich das Geburtsdatum ab und vertrauen den Angaben. Versucht man sich mit einem Alter unter dem gesetzten Mindestalter zu registrieren, wird der Vorgang oft nur unterbrochen. Meist kann das Geburtsdatum direkt korrigiert und die Registrierung fortgeführt werden.

Dabei ist eine verlässliche Altersprüfung essenziell für die meisten weiteren Vorsorgemaßnahmen. Schutzmechanismen, die beispielsweise die Kontaktaufnahme oder den Zugriff auf die eigenen Inhalte durch Fremde verhindern sollen, greifen bei falscher Altersangabe nicht. Dasselbe gilt für Filter, die Anbieter bei Accounts von Minderjährigen einsetzen. Sie sollen die Konfrontation mit beeinträchtigenden oder gefährdenden Inhalten verhindern. Auch diese Schutzfunktion wird ausgehebelt, wenn sich Kinder und Jugendliche mit einer Altersangabe ab 18 Jahren anmelden können. Sie sind dann schutzlos allen Risiken im Dienst ausgeliefert.

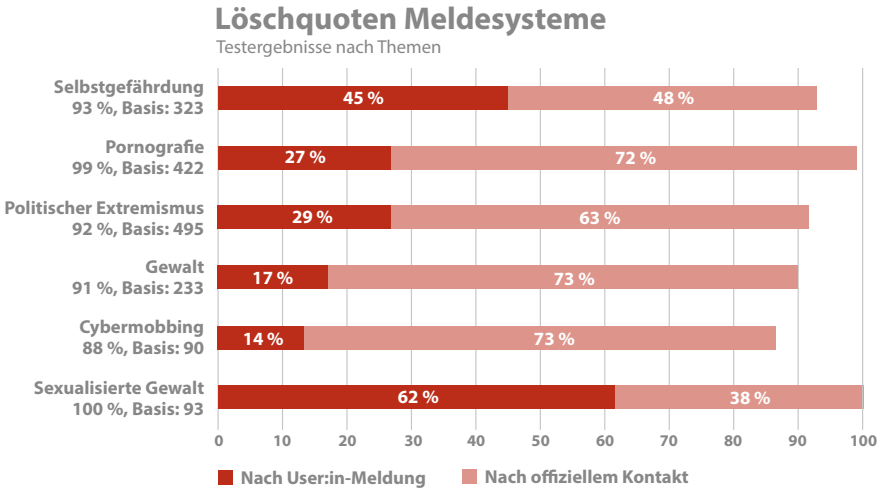
Zu einer Verbesserung des Schutzniveaus könnte mittelfristig der Einsatz von Künstlicher Intelligenz bei der Altersprüfung beitragen. Einige Dienste setzen punktuell bereits KI-gestützte „Age Estimation“ ein, allerdings nur zur Bestimmung der Volljährigkeit. Bei diesem Verfahren wird das Alter der Nutzer:innen durch eine Echtzeit-Aufnahme des Gesichts über die Webcam geschätzt. Derzeit haben „Age-Estimation-Systeme“ noch Schwierigkeiten, geringe Altersunterschiede exakt festzustellen. Sollte die Entwicklung im Bereich KI weiterhin voranschreiten, könnte sich hier ein ausreichend treffsicherer und datensparsamer Ansatz herausbilden. Dokumente und weitreichende Angaben wären dann nicht mehr vonnöten.

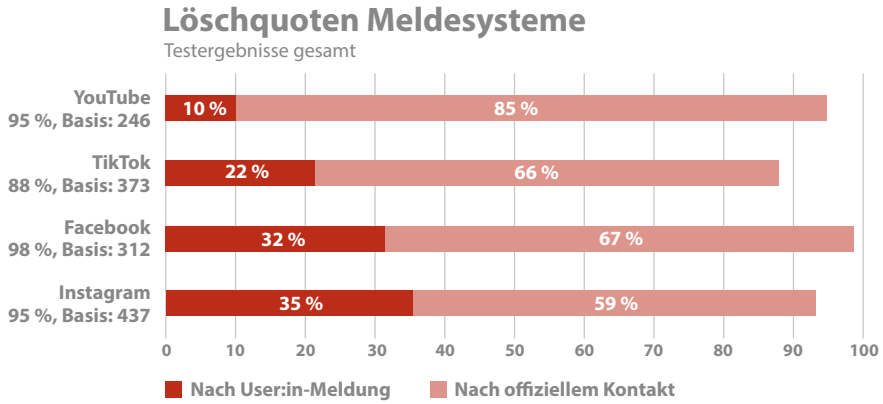
Reaktion auf die Meldung von Verstößen mangelhaft

Ein leicht handhabbares und effektives Meldesystem, das bei Verstößen für schnelle Abhilfe sorgt, ist für den Schutz von Kindern und Jugendlichen besonders wichtig. Oft ist die Meldung das einzige Mittel, um auf gefährdende Inhalte oder Kontakte hinzuweisen. Umso wichtiger, dass Anbieter Beschwerden zeitnah prüfen und bei Verstößen konsequent Maßnahmen ergreifen. In der Regel ist dies die Löschung oder Sperrung der Inhalte.

Die Ergebnisse der Tests 2023 zeigen erneut, dass jugendaffine Dienste ihre Pflicht zur raschen Abhilfe bei gemeldeten Verstößen nicht ernst nehmen. Bei mehreren Phänomenen lag die durchschnittliche Löschquote nach User:in-Meldung nur bei unter einem Drittel – darunter Gewalt, Pornografie und Politischer Extremismus. Bei selbstgefährdenden Inhalten waren die Reaktionen mit 45 % nur geringfügig besser; bei sexualisierter Gewalt führten immerhin 62 % der Meldungen zu einer Löschung.

Zur Überprüfung der Meldesysteme wendet jugendschutz.net ein zweistufiges Verfahren an: Im ersten Schritt werden Verstöße als reguläre User:in-Meldung übermittelt. Dies bedeutet, dass jugendschutz.net als Absender nicht erkennbar wird. Ist nach sieben Tagen keine Löschung oder Sperrung des gemeldeten Inhalts erfolgt, fordert jugendschutz.net offiziell als Institution zur Entfernung auf. Ob der Dienst eine Maßnahme ergriffen hat, wird nach weiteren sieben Tagen überprüft.





YouTube weist insgesamt enttäuschende Löschquoten nach Meldungen durch User:innen auf. Im Bereich Pornografie kam es zu einem drastischen Abfall im Vergleich zum Vorjahr (4 %; 2022: 62 %). Schwer verständlich sind auch die schlechten Reaktionen bei Verstößen aus dem Kontext des Politischen Extremismus (14 %): Beim überwiegenden Teil der dazu gemeldeten Inhalte handelte es sich um strafbare Kennzeichen, die in der Regel leicht als Verstoß zu erkennen sind.

Erzielte **TikTok** 2022 bei selbstgefährdenden Inhalten das beste Ergebnis mit 42 % entfernten Fällen nach User:in-Meldung, lag die Quote 2023 nur bei 22 %. Dies ist besonders problematisch, da sich gefährliche Challenges über TikTok rasend schnell verbreiten und eine hohe Reichweite bei Kindern und Jugendlichen erzielen.

Facebook reagierte besonders schlecht auf Fälle mit Bezug zu Gewalt und politischem Extremismus: So entfernte der Dienst nur 8 % der gemeldeten Gewaltdarstellungen, nur 13 % der Inhalte, die Menschenwürdeverletzungen zeigten, und nur 22 % der rechtsextremen strafbaren Kennzeichen. Unverständlich bleibt auch, dass nur 32 % der pornografischen Inhalte beseitigt wurden.

Während **Instagram** im Themenkomplex der Selbstgefährdungen besser löschte als im Vorjahr (68 %; 2022: 49 %), verringerte sich die Quote erheblich bei Cybermobbing (24 %; 2022: 62 %) und politischem Extremismus (17 %; 2022: 36 %). Besonders schlecht schnitt der Dienst bei Gewaltdarstellungen (0 %) und Menschenwürdeverletzungen (8 %) ab.

Sicherheitseinstellungen: Basisschutz mit Lücken

Sichere Voreinstellungen in Online-Diensten sind eine zentrale Voraussetzung, um Kindern und Jugendlichen eine altersgerechte Teilhabe zu ermöglichen. Ein Basisschutz wird mittlerweile von allen Diensten, die laufend überprüft werden, angeboten. Dieser greift allerdings nur bei wahrheitsgemäßer Altersangabe. Außerdem sollten Jugendliche die Möglichkeit haben, weitere Sicherheitseinstellungen einfach und schnell selbst vorzunehmen. 2023 nahmen einige Anbieter Verbesserungen vor, manches verschlechterte sich:

TikTok

Minderjährige haben mehr Kontrolle über ihre Beiträge und Daten. Sie können nun in den Einstellungen einsehen, ob Videos anderer Nutzer:innen mit eigenen Inhalten kombiniert und geteilt wurden (sogenannte Duette und Stitches). Diese lassen sich inklusive der Originale löschen.

Die Direktnachrichtenfunktion ist für ein größeres Publikum geöffnet. Für den Empfang von Privatnachrichten haben Jugendliche ab 16 Jahren neben "Freund:innen" und "Niemand" inzwischen eine dritte Wahlmöglichkeit: "Vorgeschlagene Kontakte und Freund:innen von Facebook".

Instagram

Nutzer:innen können besser kontrollieren, wer Beiträge sehen kann und wer nicht. Das Posten von Inhalten ist nun auf „Enge Freunde" (bis zu 100 Personen) eingrenzbar. Vorher ließen sich Beiträge nur mit allen Follower:innen oder komplett öffentlich teilen.

Für öffentliche Profile haben sich die Gefahren des Kontrollverlusts über die eigenen Daten sowie die missbräuchliche Weiterverwendung durch unbefugte Dritte erhöht. Reels können dort mittlerweile per Klick heruntergeladen werden – auch, wenn es sich um Accounts von Minderjährigen handelt.

Snapchat

Wenn Minderjährige von einer Person kontaktiert werden, mit der sie keine oder nur wenige gemeinsame Kontakte haben, erhalten sie nun automatisch eine Warnmeldung, dass sie diese vermutlich nicht kennen und Vorsicht geboten ist. Sie können den Account dann direkt aus dem Chatfenster heraus blockieren, melden oder der Konversation zustimmen.

Nutzungsrichtlinien und Hilfsangebote weiterentwickelt

Bei den Nutzungsrichtlinien und Hilfsangeboten besserten einige Dienste nach. Entscheidend ist jedoch, dass Verstöße gegen die eigenen Richtlinien konsequent sanktioniert werden.
Hier haben die Anbieter noch viel Luft nach oben, wie die Auswertung der Meldetests zeigt.

YouTube

Untersagt sind nun Livestreams, in denen Schusswaffen gezeigt werden. Zudem dürfen in Videos keine externen Links mehr auf Drittangebote, deren Inhalte gegen die YouTube-Richtlinien verstoßen, platziert werden. Dies gilt auch für nicht klickbare Verweise, also z. B. sprachliche Nennungen und eingeblendete Bilder im Video.

Laut der erneuerten Richtlinie zu Selbstgefährdung sind bestimmte Inhalte mit Bezug zu Essstörungen nur noch ab 18 Jahren erlaubt. Diese Maßnahme läuft jedoch bei falscher Altersangabe ins Leere. Korrespondierend zur Richtlinie wird direkt unter betreffenden Videos auf Hilfs- und Beratungsangebote hingewiesen.

TikTok

Minderjährige User:innen sehen nun bereits beim Registrierungsvorgang Kurzvideos mit Informationen, beispielsweise zu Schutzfunktionen und Hilfsangeboten. Diese altersgerechte Einführung trägt zur sicheren Nutzung des Dienstes bei.

Im neuen Informations-Hub zu Fake-News bekommen Nutzer:innen Tipps, wie sich Falschnachrichten und sonstige Desinformationen erkennen und prüfen lassen. Der Hub ist allerdings nicht ins Hilfeportal integriert, sondern nur über eine gezielte Schlagwortsuche auffindbar.

Über jugendschutz.net

jugendschutz.net fungiert als das gemeinsame Kompetenzzentrum von Bund und Ländern für den Schutz von Kindern und Jugendlichen im Internet. Die Stelle recherchiert Gefahren und Risiken in jugendaffinen Diensten. Sie wirkt darauf hin, dass Verstöße gegen Jugendschutzbestimmungen beseitigt und Angebote so gestaltet werden, dass Kinder und Jugendliche sie unbeschwert nutzen können.

Die Jugendministerien der Länder haben jugendschutz.net 1997 gegründet. Die Aufgaben wurden 2003 im Jugendmedienschutz-Staatsvertrag (JMStV) festgelegt. Die Stelle ist seither an die Kommission für Jugendmedienschutz (KJM) angebunden. 2021 hat der Bund jugendschutz.net als gemeinsamem Kompetenzzentrum im Jugendschutzgesetz (JuSchG) ebenfalls eine gesetzliche Aufgabe zugewiesen.

jugendschutz.net wird finanziert von den Obersten Landesjugendbehörden, den Landesmedienanstalten und gefördert vom Bundesministerium für Familie, Senioren, Frauen und Jugend sowie der Europäischen Union.

jugendschutz.net nimmt über seine Online-Beschwerdestelle Hinweise auf Verstöße gegen den Jugendmedienschutz entgegen.

jugendschutz.net/verstoss-melden

JUGEND SCHUTZ.NET