Rat der
Europäischen Union

Brüssel, den 13. Februar 2026
(OR. en)

6361/26

FREMP 48
JAI 198
HYBRID 19
EDUC 47
JEUN 26
GENDER 13
TELECOM 67
CYBER 61
DISINFO 11
COPEN 43
AUDIO 20

ÜBERMITTLUNGSVERMERK

Absender:	Frau Martine DEPREZ, Direktorin, im Auftrag der Generalsekretärin der Europäischen Kommission
Eingangsdatum:	11. Februar 2026
Empfänger:	Frau Thérèse BLANCHET, Generalsekretärin des Rates der Europäischen Union
Nr. Komm.dok.:	COM(2026) 71 final
Betr.:	MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN RAT, DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND DEN AUSSCHUSS DER REGIONEN Aktionsplan gegen Cybermobbing „Sicherer online, gemeinsam stärker“

Die Delegationen erhalten als Anlage das Dokument COM(2026) 71 final.

Anl.: COM(2026) 71 final

EUROPÄISCHE
KOMMISSION

Straßburg, den 10.2.2026
COM(2026) 71 final

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN RAT, DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND DEN AUSSCHUSS DER REGIONEN

Aktionsplan gegen Cybermobbing

„Sicherer online, gemeinsam stärker“

1. Einleitung

„Das ist ein knallhartes Geschäft. Doch die Eltern leben tagtäglich mit den damit verbundenen Risiken und schädlichen Folgen: Cybermobbing. Anstiftung zur Selbstverletzung. Cyberkriminalität. Algorithmen, die abhängig machen. Es ist an uns, unsere nächste Generation zu schützen.“

Präsidentin von der Leyen, Rede auf der hochrangigen Veranstaltung zum Thema „Schutz von Kindern im digitalen Zeitalter“ 2025

Der digitale Wandel hat die Gesellschaft radikal verändert. Er bietet Kindern und jungen Menschen enorme Möglichkeiten, ihre Fähigkeiten und ihre Kreativität zu entwickeln. Heutzutage nutzen 97 % der jungen Menschen in der EU das Internet täglich, und für junge Menschen zwischen 15 und 24 Jahren sind Social-Media-Plattformen die wichtigste Informationsquelle (65 %). Durch KI-Tools, Videospiele, Messaging-Apps und Online-Gemeinschaften vernetzen sie sich und interagieren miteinander.

Diese Plattformen bergen aber auch Risiken: Kriminelle, die sich im Internet ihre Opfer suchen, Anstiftung zur Selbstverletzung, suchterzeugende Algorithmen, gefährliche Online-Challenges und Cybermobbing.

Die Grundrechte, auch die Rechte von Kindern, sind ein wesentlicher Bestandteil der Werte der EU und müssen sowohl online als auch offline gewahrt werden. Kinder und junge Menschen haben das Recht, sicher nach Informationen zu suchen, zu lernen, sich zu vernetzen und engagierte Mitglieder der Gesellschaft zu werden. Die Freiheiten und Möglichkeiten der digitalen Welt müssen daher mit unserer Entschlossenheit einhergehen, Kinder und junge Menschen. zu schützen und zu stärken. Die Verheißungen des digitalen Zeitalters dürfen nicht durch Verhaltensweisen untergraben werden, die erniedrigen, ausgrenzen oder schaden.

Cybermobbing beschädigt das Vertrauen und das Selbstwertgefühl. Es grenzt Menschen aus und macht sie klein. Es unterwandert unser gemeinsames Ziel eines dynamischen, inklusiven und digitalen Europas für unsere Kinder und jungen Menschen.

Soziale Medien sind einer der Hauptkanäle, über die Kinder und Jugendliche Cybermobbing erfahren, und es gibt immer mehr Belege dafür, dass die Exposition von Kindern und Jugendlichen gegenüber unangemessenen Online-Inhalten dauerhafte, schädliche Auswirkungen hat. Die EU verfügt bereits über einen umfassenden rechtlichen und politischen Rahmen zum Schutz und zur Stärkung von Kindern im Internet, wobei das Gesetz über digitale Dienste derzeit das wichtigste Instrument in diesem Bereich ist.

Wie in der Rede zur Lage der Union 2025 angekündigt, führt Präsidentin von der Leyen in Anbetracht der Gefahren, die das Internet birgt, Gespräche mit Experten, in denen es um mögliche Altersbeschränkungen für die Nutzung sozialer Medien in Europa geht; entsprechende Empfehlungen sollen bis zum Sommer 2026 ergehen. Eine Reihe von Mitgliedstaaten erwägt Schritte zur Einführung eines gesetzlich vorgeschriebenen Mindestalters für den Zugang zu sozialen Medien und von Anforderungen an die elterliche Einwilligung und Kontrolle. Dazu gehören die Angleichung des Mindestalters für den Zugang zu sozialen Medien an das Alter der digitalen Einwilligung, die Vorgabe eines standardmäßigen

Datenschutzes für Minderjährige und die Festlegung von Lösungen für die anonyme Altersüberprüfung.

Ein koordinierter europäischer Ansatz für Altersgrenzen würde sicherstellen, dass alle europäischen Kinder den gleichen Schutz erhalten, und eine rechtliche Fragmentierung im digitalen Binnenmarkt verhindern. Das Expertengremium wird den Weg für einen koordinierten, möglicherweise legislativen europäischen Ansatz für Altersgrenzen und eine evidenzbasierte Sensibilisierungskampagne ebnen, um Eltern in die Lage zu versetzen, den Zugang ihrer Kinder zu Online-Inhalten wirksam zu kontrollieren.

Der Jugendbeirat hat der Kommissionspräsidentin auch die Sichtweisen junger Menschen zu diesem Thema mitgeteilt. Die Kommission erprobt gemeinsam mit den Mitgliedstaaten eine Lösung für die Altersüberprüfung, die benutzerfreundlich ist, die Privatsphäre schützt und einen „Referenzstandard“ für die Online-Altersüberprüfung festlegt. Das Europäische Parlament hat ein einheitliches europäisches digitales Mindestalter von 16 Jahren für den Zugang zu sozialen Medien, Video-Sharing-Plattformen und KI-Begleiter gefordert, wobei der Zugang für 13- bis 16-Jährige mit Einwilligung der Eltern ermöglicht werden kann.

Die Kommission wird auch eine EU-weite Untersuchung einleiten, um eine faktengestützte Debatte über die Auswirkungen sozialer Medien und übermäßiger Bildschirmzeit auf das Wohlbefinden und die psychische Gesundheit junger Menschen anzustoßen.

Wenn Kinder online sind, stellt Cybermobbing nach wie vor eine erhebliche Bedrohung dar, die eine koordinierte Reaktion auf EU- und nationaler Ebene erfordert. Online-Plattformen müssen ihrer Verantwortung für die Gewährleistung von Sicherheit durch Technikgestaltung Rechnung tragen. Die Bekämpfung von Cybermobbing erfordert die Zusammenarbeit auf allen Regierungs- und Verwaltungsebenen, einschließlich der Regulierungs- und Strafverfolgungsbehörden, sowie einen gesamtgesellschaftlichen Ansatz, an dem Eltern, Fachleute, pädagogische Fachkräfte, die Zivilgesellschaft und die jungen Menschen selbst beteiligt sind.

Wie in den politischen Leitlinien 2024-2029 der Kommission angekündigt, wird in dieser Mitteilung ein gezielter Aktionsplan vorgestellt, um dem zunehmenden Trend zu Missbrauch im Internet entschlossen entgegenzutreten. Das Hauptaugenmerk dieses Aktionsplans liegt auf Kindern und jungen Menschen, berücksichtigt aber auch die erhöhte Vulnerabilität bestimmter Gruppen. Viele der vorgeschlagenen Maßnahmen werden aber dazu beitragen, Cybermobbing auch in der breiteren Bevölkerung zu bekämpfen.

Die Kommission wird alle ihr zur Verfügung stehenden Instrumente nutzen, um das Gesetz über digitale Dienste zu ergänzen und sicherzustellen, dass digitale Plattformen ihrer Verantwortung für die Aufdeckung und Bekämpfung von Cybermobbing in vollem Umfang gerecht werden. Sie wird alle Mitgliedstaaten bei der Übernahme der in der EU verfügbaren bewährten Verfahren unterstützen, um die Wirksamkeit ihres Kampfes gegen Cybermobbing zu maximieren. Und sie wird die Bemühungen verstärken, alle Teile der Gesellschaft mit Informationen zu erreichen und das Bewusstsein dafür zu schärfen, was Cybermobbing ist, wie es verhindert werden kann und wie Opfer unterstützt werden können.

Mit diesem Aktionsplan fordert die Kommission die Mitgliedstaaten, die regionalen und lokalen Behörden, Online-Plattformen, die Zivilgesellschaft, Bildungseinrichtungen, Familien, Kinder und junge Menschen auf, sich für ein gemeinsames Ziel einzusetzen, nämlich zu gewährleisten, dass der digitale Raum sicher, respektvoll, inklusiv und unterstützend ist. Die Kommission schlägt vor, dass unsere Union gemeinsam für das psychische Wohlbefinden und die Würde aller Kinder und jungen Menschen eintritt.

2. Cybermobbing: Der Sachverhalt

Cybermobbing betrifft Kinder überall: 18,3 % der Kinder weltweit erleben Cybermobbing durch Instant-Messaging, Beiträge in den sozialen Medien, E-Mails oder Textnachrichten. Doch Cybermobbing findet nicht nur über schriftliche Kommunikation statt, sondern auch über audiovisuelle Inhalte wie Bilder oder Videos, die online geteilt werden.

In Europa gibt jedes sechste Kind im Alter von 11 bis 15 Jahren an, im Internet schon einmal gemobbt worden zu sein, und etwa jedes achte gibt zu, andere im Internet gemobbt zu haben. Zwischen 2018 und 2022 ist die Zahl der jugendlichen Opfer von Cybermobbing bei Jungen um ein Viertel und bei Mädchen um knapp ein Viertel gestiegen. In den letzten fünf Jahren war Cybermobbing stets der Hauptgrund für Anrufe bei den Helplines der Safer-Internet-Zentren (SIC).

Die 6 343 Befragten im Alter von 12 bis 17 Jahren, die für diesen Aktionsplan konsultiert wurden, berichteten über eine weitverbreitete Exposition gegenüber Cybermobbing: Jedes vierte Kind bzw. jeder vierte Jugendliche im Alter von 12 bis 17 Jahren hat bereits selbst Cybermobbing erlebt, und mehr als jedes dritte Kind bzw. jeder dritte Jugendliche hat angegeben, Zeuge von Cybermobbing gewesen zu sein.

2.1 Was ist Cybermobbing?

Digitale Technologien haben die Möglichkeiten zur Vernetzung erweitert, aber sie haben auch die Online-Risiken erhöht, z. B. soziale Ausgrenzung, hassmotivierte Straftaten, Belästigung, Erniedrigung und Missbrauch, die über physische Grenzen hinausgehen und rund um die Uhr bestehen können.

Für die Zwecke dieses Aktionsplans beabsichtigt die Kommission, **ein gemeinsames Verständnis von Cybermobbing** zu fördern:

Cybermobbing bezeichnet **ein Verhalten, das mittels digitaler Technologien mit der primären Absicht oder der Wirkung ausgeübt wird, insbesondere Kinder oder junge Menschen wiederholt oder ständig zu erniedrigen, sozial auszugrenzen, zu missbrauchen, zu belästigen oder zu schädigen**.

Als wesentliches Merkmal von Mobbing und Cybermobbing wird die Wiederholung angesehen. Sie verursacht anhaltende Auswirkungen auf das Opfer, das möglicherweise auch befürchtet, dass ein einmaliges Ereignis wiederholt online geteilt werden könnte, was das Trauma vergrößert und zu einer erneuten Viktimisierung führt, ohne dass der Täter noch einmal direkt beteiligt ist.

Machtungleichgewicht ist ein zentrales Element des Mobbings, kann sich online aber anders äußern. Beim traditionellen Mobbing beruht das Machtungleichgewicht häufig auf körperliche Stärke, sozialem Status oder Gruppennormen. Beim Cybermobbing resultiert es auch aus einem ungleichen Maß an digitalem Einfluss, an digitalen Kompetenzen, an Zugang zu Technologie oder an Kontrolle über Inhalte.

Cybermobbing ist zunehmend schwieriger zu bekämpfen, da es auf privaten Geräten jederzeit und überall ohne physische Anwesenheit des Täters auftreten kann. Darüber hinaus findet es auch auf nicht öffentlich zugänglichen Kanälen statt.

Zu den häufigsten Formen von Cybermobbing gehören gemeine oder verletzende Kommentare, die Verbreitung von Gerüchten im Internet oder das Teilen bloßstellender oder erniedrigender Beiträge.

Die Anonymität, die große Reichweite und die Möglichkeit, jederzeit private Nachrichten an Einzelpersonen zu senden, potenzieren den Schaden, den traditionelles Mobbing anrichten kann. Darüber hinaus fördern digitale Umgebungen die Loslösung von moralischen Überzeugungen, verminderte Empathie und den Enthemmungseffekt im Internet, wodurch die Hemmschwellen für Online-Aggression sinken.

Schädliche Inhalte können auf unbestimmte Zeit online präsent bleiben. Sie können immer wieder abgerufen und geteilt werden oder viral gehen, was den Schaden noch größer macht, zu erneuter Viktimisierung führt und den Verarbeitungsprozess der Opfer erschwert. Diese Faktoren müssen berücksichtigt werden, um wirksame Unterstützung zu leisten. Der Kreis der potenziellen Beteiligten wird immer größer und ermöglicht ein Aggressionskontinuum zwischen dem physischen Raum und dem Online-Raum bzw. umgekehrt.

Die ständige rasante Weiterentwicklung digitaler Technologien bedeutet, dass sich auch die Umgebungen und Tools, die genutzt werden, um Schaden zuzufügen, ständig verändern. Um Flexibilität zu gewährleisten, sollten die neuesten Technologien genutzt werden, um Cybermobbing zu erkennen und zu bekämpfen.

Obwohl insbesondere künstliche Intelligenz (KI) dazu beitragen kann, Cybermobbing zu erkennen, erhöhen die zunehmende Verbreitung von KI, vor allem generativer KI, und ihre Integration in Online-Apps und -Dienste zugleich die Risiken hinsichtlich Cybermobbing und schaffen sogar neue. Beispielsweise nehmen Deepfakes zu und führen zunehmend zu eindeutig sexuellem Deepfake-Missbrauch, der sich überwiegend gegen Frauen und Mädchen richtet, auch in Fällen von Cybermobbing, und von schädlichem Verhalten bis hin zu Straftaten reicht, nämlich dann, wenn Bilder erstellt werden, die den sexuellen Missbrauch von Kindern oder geschlechtsspezifische Cybergewalt darstellen. Dadurch kommt eine zusätzliche Schadensdimension ins Spiel, die nicht nur den Ruf schädigt, sondern – wie andere Verhaltensweisen im Zusammenhang mit Cybermobbing – auch zu psychischen Traumata führen kann, was die Dringlichkeit einer Überwachung und Bekämpfung dieser neu auftretenden Risiken auf EU-Ebene deutlich macht.

Cybermobbing und Hasskriminalität können sich überschneiden, wenn Cybermobbing durch Hass motiviert ist oder zu Gewalt und Hass aufstachelt und Einzelpersonen wegen bestimmter geschützter Merkmale ins Visier nimmt. Laut dem Rahmenbeschluss 2008/913/JI des Rates

müssen die Mitgliedstaaten die öffentliche Aufstachelung zu Gewalt oder Hass gegen eine nach den Kriterien der Rasse, Hautfarbe, Religion, Abstammung oder ethnische Herkunft definierte Gruppe von Personen oder gegen ein Mitglied einer solchen Gruppe unter Strafe stellen. Außerdem wird von den Mitgliedstaaten verlangt, dafür zu sorgen, dass für Straftaten, die aus rassistischen oder fremdenfeindlichen Beweggründen begangen werden, zusätzliche Sanktionen vorgesehen werden.

Cybermobbing kann sich überschneiden mit sexuellem Missbrauch von Kindern im Sinne der Richtlinie 93/2011 zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie.

Gemäß der Richtlinie 2024/1385 zur Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt müssen die Mitgliedstaaten sicherstellen, dass geschlechtsspezifische Aufstachelung zu Gewalt oder Hass im Internet unter Strafe gestellt wird. Darüber hinaus gelten weitere Straftaten im Zusammenhang mit Cybergewalt, die häufig im Kontext von Cybermobbing auftreten, als strafbar: die nicht-einvernehmliche Weitergabe von intimem oder manipuliertem Material, Cyberstalking und Cybermobbing. Die Richtlinie enthält auch Bestimmungen, mit denen die unverzügliche Entfernung von illegalem Material zu Cybergewalt ermöglicht wird.

2.2 Gruppen, die von Cybermobbing bedroht sind

Cybermobbing ist vor allem bei **Kindern und Jugendlichen im Schulalter** weitverbreitet, insbesondere mit der Zunahme ihrer Online-Aktivität.

Mädchen und junge Frauen sind sexistischem und frauenfeindlichem Mobbing ausgesetzt und unverhältnismäßig stark betroffen, z. B. durch die nicht einvernehmliche Weitergabe intimer Bilder und sexuell eindeutiger Deepfakes.

Schutzbedürftige Gruppen sind unverhältnismäßig stark von Cybermobbing betroffen, da sich Cybermobbing gegen eine Person richten kann, die als einer solchen Gruppe zugehörig wahrgenommen wird.

Kinder aus einkommensschwachen Haushalten sind Cybermobbing stärker ausgesetzt als ihre Altersgenossen.

Kinder und junge Menschen mit Behinderungen erfahren ein höheres Maß an Online-Viktimisierung, einschließlich sexueller und geschlechtsspezifischer Gewalt. Manche ziehen sich sogar aufgrund von ständigem Missbrauch aus dem digitalen Raum zurück.

Ethnische und religiöse Minderheiten, Migranten sowie Geflüchtete sind von einem erhöhten Risiko für rassistisches oder diskriminierendes Mobbing betroffen. So sind beispielsweise Roma und andere ethnische Minderheiten in besonderem Maße Online-Belästigungen und illegaler Hetze im Internet ausgesetzt, die mit systematischer Ausgrenzung einhergehen, und 90 % der jüdischen und Europäer berichteten im vergangenen Jahr, online Antisemitismus erlebt zu haben.

63 % der **LGBTIQ+-Personen** sind häufig mit gewalttätigen Online-Inhalten gegen die LGBTIQ+-Gemeinschaft konfrontiert gewesen. Darüber hinaus berichteten 11 %, dass im

vergangenen Jahr beleidigende oder bedrohliche Kommentare über sie im Internet veröffentlicht wurden, und zwei Drittel sind in ihrer Schulzeit verspottet oder belästigt worden.

Die in diesem Aktionsplan vorgeschlagenen Maßnahmen sollen dazu beitragen, Cybermobbing zu bekämpfen, und zwar für alle Opfer. Die oben dargelegten Gleichstellungsaspekte werden bei der Umsetzung berücksichtigt, um die Wirkung der Maßnahmen zu verstärken.

2.3 Die Auswirkungen von Cybermobbing

Cybermobbing kann schwerwiegende und langfristige Folgen haben, sowohl für den Einzelnen als auch für die Gesellschaft insgesamt. Auch kann Cybermobbing ein erster Schritt hin zu schwereren Straftaten oder zu Missbrauch sein, u. a. zu sexuellem Missbrauch.

Für Opfer von Cybermobbing besteht ein erhöhtes Risiko für Angstzustände, Depressionen, Einsamkeit, Selbstverletzung und suizidales Verhalten, und sie sind anfälliger für Verhaltensauffälligkeiten, z. B. schädliches Bewältigungsverhalten. Darüber hinaus können Opfer von Cybermobbing selbst zu Cybermobbing-Tätern werden, und sei es nur in dem Versuch, ihrer Opferrolle zu entkommen. Dies erfordert eine wohlüberlegte und kindgerechte Reaktion.

Cybermobbing kann auch die schulische Leistung, das Wohlbefinden der Schülerinnen und Schüler und das schulische Umfeld beeinträchtigen. Dies kann langfristige Folgen für die schulischen und beruflichen Laufbahnen sowie für das allgemeine Wohlbefinden und die Lebenszufriedenheit der Schüler haben.

Die Auswirkungen auf Kinder und junge Menschen können somit weitreichende Folgen für die Gesellschaft haben und bestehende Ungleichheiten verschärfen.

3. Der Weg in die Zukunft

Es bedarf einer robusteren, konsequenteren und besser koordinierten Reaktion der EU auf Cybermobbing, um die Prävention und die digitale Kompetenz zu stärken sowie die Meldung von Vorfällen und die Unterstützung der Opfer in der gesamten Union zu verbessern und zu vereinfachen. Unsere Vision ist ein Europa, in dem jedes Kind und jeder junge Mensch frei von Cybermobbing und in seiner Würde geschützt aufwachsen kann und befähigt wird, sich in einer digitalen Welt, die die europäischen Werte achtet, zu entfalten. Daher stützt sich dieser Aktionsplan auf drei miteinander verbundene Säulen: auf einen koordinierten EU-Ansatz, auf Prävention und Sensibilisierung sowie auf Meldung und Unterstützung.

Dieser Aufruf zum Handeln besitzt Rückhalt in der Öffentlichkeit: Mehr als neun von zehn Europäerinnen und Europäern halten es für dringend geboten, dass der Staat Maßnahmen ergreift, um Kinder vor Cybermobbing zu schützen. Die öffentliche Konsultation zu diesem Plan hat gezeigt, dass es eine starke Befürwortung für Programme zur Förderung der digitalen Kompetenz und der Empathie an Schulen und in der Lehrerausbildung sowie für verbesserte Meldeinstrumente und Unterstützungsdienste für Opfer gibt.

3.1 Säule I: Ein koordinierter EU-Ansatz beim Schutz

Die Kommission wird die bestehenden politischen und rechtlichen Instrumente in vollem Umfang nutzen und ermitteln, welche Maßnahmen zur Bekämpfung von Cybermobbing im Rahmen künftiger Initiativen möglich sind. Darüber hinaus **werden die Mitgliedstaaten aufgefordert, gemeinsame Ziele in wirksame nationale Maßnahmen umzusetzen und ein integriertes und gut funktionierendes Ökosystem zur Bekämpfung von Cybermobbing aufzubauen**.

Das Gesetz über digitale Dienste ist nach wie vor zentral für die Durchsetzungsbemühungen, da es Anbieter von Online-Plattformen, die für Minderjährige zugänglich sind, dazu verpflichtet, für ein hohes Maß an Privatsphäre, Sicherheit und Schutz von Minderjährigen innerhalb ihres Dienstes zu sorgen.

Darüber hinaus sind in den Leitlinien des Gesetzes über digitale Dienste zur Durchsetzung des Schutzes Minderjähriger im Internet Maßnahmen festgelegt, die Anbieter von Online-Plattformen ergreifen sollten, um dieser Verpflichtung nachzukommen, einschließlich geeigneter Maßnahmen zur Verringerung des Risikos, dass Minderjährige schädlichen Inhalten ausgesetzt sind, wie z. B. die Gestaltung von Empfehlungssystemen zum Wohl von Minderjährigen, oder dass sie schädlichem Verhalten ausgesetzt sind, u. a. kontaktbedingten Risiken durch Interaktionen mit anderen. Zum Schutz der Opfer von Cybermobbing umfassen die Leitlinien ferner Maßnahmen zur Kontrolle und Stärkung der Nutzenden, kinderfreundliche Meldemechanismen und Beschwerdeinstrumente sowie die Moderation von Inhalten in den Amtssprachen des Mitgliedstaats, in dem der Dienst bereitgestellt wird. Das Gesetz über digitale Dienste verpflichtet Anbieter von Online-Plattformen auch, leicht zugängliche und benutzerfreundliche Mechanismen einzurichten, die es allen Nutzenden, einschließlich Minderjährigen, ermöglichen, rechtswidrige Inhalte, z. B. bestimmte Formen rechtswidriger Hassrede oder Material über sexuellen Kindesmissbrauch, zu melden. Je nach den nationalen Rechtsvorschriften können auch Formen von Cybermobbing rechtswidrig sein. Die Anbieter müssen unverzüglich Entscheidungen treffen, wenn sie solche Meldungen erhalten.

Dieser Aktionsplan wird in die bevorstehende Überprüfung und Aktualisierung der Leitlinien zum Schutz Minderjähriger im Internet im Rahmen des Gesetzes über digitale Dienste einfließen. Insbesondere könnten die Leitlinien Anbietern von Online-Plattformen dabei helfen, effizientere Meldeinstrumente zu entwickeln, z. B. in Bezug auf deren Sichtbarkeit, technische Zugänglichkeit und sprachliche Gestaltung, und wirksame Technologien zu nutzen, um die Exposition gegenüber Cybermobbing zu verhindern. Die Leitlinien könnten den Anbietern auch dabei helfen, geeignete Maßnahmen zu konzipieren, um auf Meldungen Minderjähriger zu reagieren, z. B. durch Unterstützung der Nutzenden bei der Speicherung von Informationen, die als Beweismittel dienen können.

Das Gesetz über digitale Dienste sieht auch die Möglichkeit von „vertrauenswürdigen Hinweisgebern“ vor, d. h. sachverständigen Stellen, deren Meldungen priorisiert werden müssen. Diese Bestimmungen können genutzt werden, um gegen Cybermobbing vorzugehen, wobei vertrauenswürdige Hinweisgeber dazu beitragen, die Verbreitung illegaler Cybermobbing-Inhalte zu bekämpfen. Die Kommission wird Leitlinien zu vertrauenswürdigen Hinweisgebern herausgeben, die helfen sollen, die Rolle der Hinweisgeber bei der Bekämpfung

illegaler Inhalte, einschließlich illegalen Cybermobbings, zu klären. Die Leitlinien werden auch dazu beitragen, die Pflichten der Anbieter von Online-Plattformen in Bezug auf Meldungen vertrauenswürdiger Hinweisgeber zu präzisieren.

Cybermobbing kann auch über audiovisuelle Online-Inhalte erfolgen. Die Richtlinie über audiovisuelle Mediendienste (AVMD-Richtlinie) enthält allgemeine Anforderungen an den Schutz Minderjähriger vor schädlichen Inhalten – insbesondere im Internet –, die ihre körperliche, geistige oder sittliche Entwicklung beeinträchtigen könnten. Dazu gehören auch Inhalte, die Cybermobbing sind. Gemäß der AVMD-Richtlinie müssen Video-Sharing-Plattform-Dienste geeignete Maßnahmen ergreifen, um zu verhindern, dass Minderjährige auf schädliche Inhalte zugreifen, indem Standards für Medieninhalte in die Allgemeinen Geschäftsbedingungen oder in Systeme zur Kontrolle durch Eltern und zur Bewertung von Inhalten aufgenommen werden. Darüber hinaus sind die Mitgliedstaaten verpflichtet, bei der Umsetzung der AVMD-Richtlinie die Menschenwürde zu schützen. Bei der laufenden Evaluierung und Überarbeitung der Richtlinie wird bewertet, wie wirksam Video-Sharing-Plattformen diese Vorschriften angewandt haben und ob im Einklang mit dem Gesetz über digitale Dienste mehr getan werden muss, um Minderjährige vor schädlichen Online-Inhalten, auch in Bezug auf Cybermobbing, zu schützen.

Die Verordnung über künstliche Intelligenz verbietet KI-Systeme, die Personen manipulieren oder täuschen, indem sie deren Vulnerabilität aufgrund ihres Alters ausnutzen, um ihr Verhalten zu beeinflussen, und dadurch erheblichen Schaden verursachen. Diese Verbote können Cybermobbing verhindern. Die Kommission hat Leitlinien zu verbotenen KI-Praktiken angenommen, um eine einheitliche und wirksame Umsetzung in der gesamten Union zu erleichtern. In der KI-Verordnung sind auch Transparenzanforderungen festgelegt, einschließlich der Verpflichtung, Nutzern mitzuteilen, dass sie es mit einem KI-System zu tun haben, und von KI generierte oder manipulierte Inhalte wie Deepfakes eindeutig zu kennzeichnen, um eine Täuschung zu verhindern.

Darüber hinaus müssen diese Maßnahmen durch die Erhebung von Daten über Cybermobbing ergänzt werden, die derzeit uneinheitlich erfolgt, was ein umfassendes Bild von den Tendenzen in den Mitgliedstaaten behindert. Als Reaktion auf die Aufforderung aus der öffentlichen Konsultation wird die Kommission eine kohärente und vergleichbare Datenerhebung zu Cybermobbing in der gesamten EU erleichtern, indem sie beispielsweise Leitlinien wie einen gemeinsamen Datenerhebungsrahmen und gemeinsame Indikatoren bereitstellt, und die Einleitung EU-weiter Erhebungen über die Plattform „Besseres Internet für Kinder“ (BIK) in Zusammenarbeit mit anderen Mechanismen zur Beteiligung von Kindern und jungen Menschen ermöglicht. Es werden angemessene Ressourcen bereitgestellt, damit das Netz der Safer-Internet-Zentren (SIC) diese zusätzlichen Aufgaben übernehmen und die langfristige Kontinuität dieser Arbeit sicherstellen kann.

Die Kommission wird

1. bei der **Überarbeitung der Leitlinien zum Schutz Minderjähriger im Rahmen des Gesetzes über digitale Dienste** den Fokus auf die Bekämpfung von Cybermobbing ausweiten, insbesondere bezüglich Maßnahmen zum besseren Schutz vor schädlichen

Inhalten und zur Verbesserung der Meldesysteme von Online-Plattformen – geplant für **2026**;

2. **Leitlinien zu vertrauenswürdigen Hinweisgebern im Rahmen des Gesetzes über digitale Dienste erlassen**, die dazu beitragen werden, die Rolle dieser Hinweisgeber bei der Bekämpfung rechtswidriger Inhalte, z. B. von rechtswidrigem Cybermobbing, zu klären – **bis zum 2. Quartal 2026**;

3. Möglichkeiten zur Bekämpfung von Cybermobbing auf Video-Sharing-Plattformen bewerten, und zwar im Rahmen der laufenden **Bewertung der Richtlinie über audiovisuelle Mediendienste (AVMD-Richtlinie) und ihrer Überarbeitung – bis zum 3. Quartal 2026**;

4. die **wirksame Umsetzung der Bestimmungen der KI-Verordnung zu verbotenen KI-Praktiken**, auch wenn sie für Cybermobbing eingesetzt werden, durch Koordinierung innerhalb des KI-Gremiums und die Leitlinien der Kommission zu verbotenen KI-Praktiken **unterstützen – ab dem 3. Quartal 2026**;

5. **die wirksame Erfüllung der Transparenzpflichten gemäß der KI-Verordnung erleichtern, u. a. durch einen Verhaltenskodex für die Kennzeichnung von durch KI erzeugten Inhalten**, der die Einhaltung der in der KI-Verordnung vorgeschriebenen Transparenzpflichten hinsichtlich der Kennzeichnung von KI-generierten Inhalten, einschließlich solcher, die für Cybermobbing verwendet werden, unterstützen soll – **ab dem 3. Quartal 2026**;

Die Mitgliedstaaten werden aufgefordert,

1. **umfassende nationale Pläne zur Bekämpfung von Mobbing, einschließlich Cybermobbing**, zu erstellen und dabei die Unterstützung des EU-Netzes für die Rechte des Kindes zu nutzen, im Einklang mit der Mitteilung und Empfehlung der Kommission zu integrierten Kinderschutzsystemen;

2. das in diesem Aktionsplan dargelegte gemeinsame Verständnis von Cybermobbing zu nutzen, um **kohärente, vergleichbare Daten über Cybermobbing zu erheben**, was durch die Unterstützung der Kommission über das Netz der Safer-Internet-Zentren und die Plattform „Besseres Internet für Kinder“ erleichtert wird, und geschlossen auf gemeinsame Normen zur Bekämpfung von Cybermobbing in der gesamten EU hinzuarbeiten.

3.2 Säule II: Prävention und Sensibilisierung

Der beste Weg zur Bekämpfung von Cybermobbing besteht darin, zu handeln, bevor es zu schädlichen Vorfällen kommt. Um Cybermobbing zu verhindern, muss bereits in der Kindheit ein gesundes digitales Verhalten erlernt werden. Das heißt, Kinder, junge Menschen und Erwachsene müssen mit den Fähigkeiten und dem Selbstvertrauen ausgestattet werden, über Online-Risiken zu sprechen und diese zu erkennen. Es ist auch wichtig, sich mit der zugrunde liegenden Gesinnung zu befassen, die zu schädlichem Verhalten im Internet führen kann.

Damit Präventionsbemühungen wirksam sind, müssen Unbeteiligte, Gleichaltrige, Täter, Eltern, Betreuungspersonen, pädagogische Fachkräfte und die Schulgemeinschaft im weiteren Sinne mit Unterstützung aller relevanten Akteure, insbesondere der Organisationen der Zivilgesellschaft, beteiligt werden. Dies wurde von 62 % der Teilnehmer an der öffentlichen Konsultation befürwortet, die der Meinung waren, dass Schulungen von Lehrkräften, Strafverfolgungsbehörden und Sozialarbeitern gefördert werden müssten.

Präventions- und Sensibilisierungsinitiativen sollten auch in informellen und nichtformalen Lernumgebungen wie Jugendzentren, Sportvereinen und Gemeinschaftseinrichtungen stattfinden, in denen Kinder und junge Menschen viel Zeit verbringen. Solche Initiativen sollten auch die Prävention und Bekämpfung jeglicher Form von Diskriminierung in Synergie mit den Gleichstellungsstrategien der EU umfassen.

Digitale Bildung und digitale Kompetenz werden immer wichtiger, um sich sicher und verantwortungsvoll in der Online-Welt zu bewegen. Die Aufklärung von Kindern und jungen Menschen über die Bedeutung eines respektvollen und verantwortungsvollen Verhaltens im digitalen Raum kann verhindern, dass absichtlich oder unabsichtlich Schäden verursacht werden. Dies ist auch als Präventivmaßnahme in der Richtlinie zur Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt vorgesehen.

Kinder und junge Menschen, auch solche mit besonderen Bedürfnissen, mit Behinderungen oder in prekären Situationen, sollten aktiv in die Gestaltung und Durchführung von Sensibilisierungsmaßnahmen einbezogen werden, die befähigend, inklusiv und barrierefrei sind, und das Schweigen über Cybermobbing brechen.

Die Kommission wird auf EU-Ebene eine Reihe von Präventions- und Sensibilisierungsinstrumenten bereitstellen, die in Partnerschaft mit Kindern und jungen Menschen, Eltern, pädagogischen Fachkräften, Fachleuten im Bereich der psychischen Gesundheit und den Mitgliedstaaten sowie Organisationen der Zivilgesellschaft entwickelt wurden.

Als Bestandteil des Aktionsplans für digitale Bildung (2021-2027) wird die Europäische Kommission ihre Leitlinien für Lehrkräfte und Pädagogen zur Bekämpfung von Desinformation und zur Förderung der digitalen Kompetenz durch allgemeine und berufliche Bildung aktualisieren. Darüber hinaus werden die Aktualisierungen, wie in der Mitteilung über den Europäischen Schutzschild für die Demokratie angekündigt, den Entwicklungen in der KI und den sozialen Medien Rechnung tragen, Lehrmaterial und Aktivitäten zum Cybermobbing umfassen und Inklusion und Vielfalt berücksichtigen. Die Europäische Kommission wird außerdem einen Kompetenzrahmen für die Unionsbürgerschaft sowie Leitlinien zur Förderung der politischen Bildung in Schulen ausarbeiten.

Darüber hinaus werden digitale Kompetenz, die Prävention von Cybermobbing und das digitale Wohlbefinden im Mittelpunkt des Fahrplans für die Zukunft der digitalen Bildung und Kompetenzen bis 2030 stehen. Mit dem Fahrplan 2030 soll sichergestellt werden, dass junge Menschen bei der Entwicklung gesunder Online-Gewohnheiten unterstützt und über den verantwortungsvollen Umgang digitaler Geräte sowohl innerhalb als auch außerhalb des Klassenzimmers aufgeklärt werden.

Diese Arbeit zur digitalen Kompetenz baut auf Initiativen auf, die die Kommission im Rahmen des Programms Erasmus+ und des Europäischen Solidaritätskorps, der Europäischen Plattform für die schulische Bildung (ESEP) und eTwinning durchführt. Im Rahmen der ESEP wird die Kommission für eine bessere und dauerhafte Sichtbarkeit aller Materialien zum Thema Mobbing, einschließlich Cybermobbing, sorgen, die für Schulen nützlich sind. Ab der Aufforderung von 2026 zur Einreichung von Vorschlägen für Erasmus+ wird das Wohlbefinden in der Schule gestärkt, um Projekte zur Bekämpfung von Mobbing und Cybermobbing besser zu unterstützen, zu überwachen und zu fördern.

Das EU-Netz für die Prävention des sexuellen Missbrauchs von Kindern wird dazu beitragen, die Aufklärung und Sensibilisierung von Kindern in Bezug auf sexuellen Missbrauch zu fördern, einschließlich der Prüfung von Initiativen, mit denen verhindert werden soll, dass Cybermobbing zu kriminellem Verhalten eskaliert (z. B. Verbreitung von Darstellungen des sexuellen Missbrauchs von Kindern). Darüber hinaus wird die Prävention von Cybermobbing auch im bevorstehenden EU-Aktionsplan zum Schutz von Kindern vor Kriminalität berücksichtigt. Der Aktionsplan soll kohärente und umfassende Maßnahmen gegen die verschiedenen Risiken enthalten, denen Kinder im Zusammenhang mit Straftaten sowohl online als auch offline ausgesetzt sind.

Die Plattform „Besseres Internet für Kinder“ (BIK) und deren Netz von SIC bieten Unterstützungsinstrumente für Kinder, Eltern, pädagogisches Fachpersonal und Fachkräfte auf EU-Ebene (BIK) und nationaler Ebene (SIC). Diese Ressourcen werden weiter ausgebaut, um die Kapazitäten zu stärken, mehr Interessenträger zu erreichen und auf neue Herausforderungen im Zusammenhang mit Cybermobbing zu reagieren.

Da Schulen eine Schlüsselrolle bei der Prävention von Cybermobbing spielen, werden mit Unterstützung der SIC und der BIK-Plattform Sensibilisierungsmaßnahmen durchgeführt, beginnend mit der jährlichen „Back-to-school“-Kampagne zu Beginn jedes neuen Schuljahres, um Lehrkräfte und Kinder mit Schulungsmaterialien, Tools und Informationen über die mögliche Prävention und die Meldung von Cybermobbing auszustatten.

Über europäische Plattformen werden Ressourcen und Schulungen zum Thema Cybermobbing für die nichtformale und informelle Bildung verstärkt. Dazu gehören das Europäische Jugendportal, die zentrale Anlaufstelle zur Sensibilisierung und Förderung von Chancen für junge Menschen und die Europäische Plattform für die schulische Bildung, der Treffpunkt für die Schulbildungsgemeinschaft und die Lernecke, wo Lehrkräften und Fachkräften im Bildungswesen Ressourcen und Toolkits zu EU-Initiativen zur Verfügung gestellt werden.

Veranstaltungen wie die Europäische Jugendwoche und die Europäische Woche des Sports erleichtern das Engagement für eine Vielzahl von Themen, einschließlich der Bekämpfung von Cybermobbing. Die Gruppe im Rahmen der „Offenen Methode der Koordinierung“ zur Bekämpfung von Hetze im Sport, die im Rahmen des EU-Arbeitsplans für den Sport eingerichtet wurde, arbeitet an Empfehlungen für die Mitgliedstaaten und Interessenträger für das Sportumfeld im Allgemeinen, auch im Internet. Der Bericht wird voraussichtlich Ende 2026 vorliegen und Empfehlungen zur Bekämpfung von Cybermobbing enthalten.

Die Kommission wird

6. **Cybermobbing** bei der **Aktualisierung der Leitlinien für Lehrkräfte und pädagogische Fachkräfte zur Bekämpfung von Desinformation und zur Förderung der digitalen Kompetenz** durch allgemeine und berufliche Bildung **berücksichtigen – bis zum 2. Quartal 2026**;

7. **die staatsbürgerliche Bildung in Schulen stärken**, und zwar durch einen Kompetenzrahmen und Leitlinien für die Unionsbürgerschaft – **2027**;

8. die digitale Kompetenz, **die Prävention von Cybermobbing** und das digitale Wohlbefinden durch **den Fahrplan für die Zukunft der digitalen Bildung und Kompetenzen bis 2030 stärken – bis zum 3. Quartal 2026**;

9. im bevorstehenden **EU-Aktionsplan zum Schutz von Kindern vor Kriminalität** einen Beitrag zur **Prävention von Cybermobbing** leisten – **bis zum 3. Quartal 2026**;

10. **Ressourcen und Schulungen zum Thema Cybermobbing** für Schulen sowie für die nichtformale und informelle Bildung, die für Menschen mit Behinderungen zugänglich sind, **ausbauen**, und zwar über die BIK-Plattform, die SIC, das Europäische Jugendportal und die Europäische Plattform für die schulische Bildung – **ab dem 2. Quartal 2026**;

11. die Gruppe im Rahmen der „Offenen Methode der Koordinierung“ zur Bekämpfung von Hetze im Sport bei ihrer Arbeit an **Empfehlungen zur Bekämpfung von Cybermobbing im Sportumfeld** unterstützen – der Bericht ist bis zum **4. Quartal 2026** vorzulegen.

Die Mitgliedstaaten werden aufgefordert,

3. die Prävention und frühzeitige Erkennung von Cybermobbing durch **klare Leitlinien und Schulungen für Interessenträger** wie pädagogisches Fachpersonal, Betreuungspersonen und Fachkräfte, die in unterschiedlichen Bereichen mit Kindern arbeiten (z. B. Gesundheit, Sport, Justiz, Strafverfolgung), zu stärken;

4. die **Beteiligung von Kindern** an der Politikgestaltung und der Umsetzung von Maßnahmen zum Wohlergehen von Kindern **zu stärken**.

3.3 Säule III: Meldung und umfassende Unterstützung

Opfer von Cybermobbing müssen über klare, vertrauenswürdige und barrierefreie Kanäle verfügen, um Missbrauch zu melden und Hilfe zu erhalten, auch für Cybermobbing über private Nachrichtenübermittlungen. Um wirksam zu sein, müssen die Unterstützungsbemühungen über die Hilfe für Cybermobbing-Opfer hinausgehen und auch Unbeteiligte, Täterinnen und Täter, Eltern, Betreuungspersonen, pädagogische Fachkräfte und die breitere Schulgemeinschaft erreichen.

Die Kommission wird kohärente, EU-weite Meldemöglichkeiten und Unterstützung für Opfer fördern. Die Meldung eines Vorfalls sollte rasch zu multidisziplinärer Unterstützung – sowohl online als auch offline – führen. Sie sollte alle einschlägigen Behörden auf allen Ebenen, private Akteure, Organisationen der Zivilgesellschaft sowie Eltern und Betreuungspersonen und die Kinder und jungen Menschen selbst einbeziehen.

Aufbauend auf den Erkenntnissen, die anhand mehrerer gezielter Konsultationen gewonnen wurden, **wird die Kommission die Einführung einer Online-Sicherheits-App in allen Mitgliedstaaten** auf der Grundlage erfolgreicher bestehender nationaler Praxismodelle wie der französischen App „3018“ **fördern**. Die App soll ein sicheres, benutzerfreundliches und vertrauliches Instrument sein, das es Kindern und jungen Menschen ermöglicht,

i. **Cybermobbing einfach** bei einer **Helpline zu melden**,

ii. **Beweismittel sicher zu speichern und zu übermitteln**, im Einklang mit den nationalen Rechtsrahmen, und

iii. **durch koordinierte Weiterverweisungen**, z. B. an Strafverfolgungs-, Bildungs- und Kinderschutzdienste, **maßgeschneiderte Unterstützung** zu erhalten.

Soweit erforderlich und relevant, wird die Kommission die Mitgliedstaaten dabei unterstützen,

i. **die App an die nationalen Umstände und die nationalen Bedürfnisse anzupassen** (z. B. Übersetzung, Branding, Vernetzung mit einschlägigen nationalen Unterstützungsdiensten und Meldeplattformen), Bereitstellung von Funktionen wie sicheres Melden, Beweissicherung im Einklang mit dem nationalen Recht und garantierte Vertraulichkeit;

ii. die **Interoperabilität** mit bestehenden Infrastrukturen und Unterstützungssystemen **sicherzustellen** und

iii. die **Verbreitung** der App in den Mitgliedstaaten, bei Nutzenden und auf Online-Plattformen zu **fördern**.

Online-Plattformen werden weiterhin für die Einrichtung wirksamer Meldemechanismen verantwortlich sein. Dies kann eine der Maßnahmen darstellen, die ergriffen wurden, um die Einhaltung der Verpflichtungen aus dem Gesetz über digitale Dienste zum Schutz Minderjähriger sicherzustellen. Ergänzend dazu wird die App Online-Plattformen zur Verfügung gestellt, damit sie in deren Melde- und Benutzerunterstützungsinstrumente integriert werden kann, u. a. durch Anwendungsprogrammierschnittstellen (API), sodass ressourceneffiziente und wirksame Meldungen und Reaktionen ermöglicht werden.

Der Erfolg der App hängt von der Verfügbarkeit von Unterstützung und Folgemaßnahmen durch die nationalen Behörden ab. Die Mitgliedstaaten werden eine wichtige Rolle dabei spielen, sicherzustellen, dass Meldungen über die App zu koordinierter Offline-Unterstützung (z. B. juristischer, sozialer, psychologischer und pädagogischer Unterstützung) führen, und die Vorteile der App zu kommunizieren. Ziel der App ist es, in den Mitgliedstaaten Synergien mit etablierten Meldemechanismen für die Meldung von Material über sexuellen

Kindesmissbrauch und von Gewalt gegen Frauen im Internet sowie mit EU-, nationalen und internationalen Helplines, insbesondere Helplines für Kinder (116 111) und Helplines für vermisste Kinder (116 000), zu schaffen.

Die Kommission wird 2026 die nächste EU-Strategie für die Rechte von Opfern annehmen und die EU-Rechtsvorschriften durch nichtlegislative Maßnahmen ergänzen. Mit der Strategie werden Strukturen für gezielte Unterstützung (z. B. medizinische Untersuchungen, emotionale und psychologische Betreuung) und Schutzdienste für Opfer im Kindesalter, einschließlich Opfer von Online-Kriminalität, gefördert. Diese dienen auch den Opfern von Cybermobbing in den Mitgliedstaaten, in denen solche Handlungen nach nationalem Recht unter Strafe gestellt sind.

Gemäß der Datenschutz-Grundverordnung ist das Recht auf Löschung personenbezogener Daten besonders relevant, wenn eine betroffene Person ihre Einwilligung als Kind gegeben hat und sich der damit verbundenen Risiken möglicherweise nicht vollständig bewusst war, auch im Zusammenhang mit Cybermobbing. Die Kommission wird die Datenschutzbehörden weiterhin bei der Entwicklung kindgerechter Instrumente unterstützen, um Daten in sozialen Medien zu schützen, Daten- oder Kontodiebstahl zu verhindern und die Ausübung ihrer Rechte zu ermöglichen.

Die Kommission wird

12. **die Einführung einer barrierefreien Online-Sicherheits-App in allen Mitgliedstaaten** für die einfache Meldung von Cybermobbing unterstützen, angepasst an die nationalen Gegebenheiten und in Synergie mit bestehenden Meldemechanismen, einschließlich Helplines und Hotlines, und die multidisziplinäre Unterstützung sowohl online als auch offline fördern – **ab dem 3. Quartal 2026**;

13. sich in der nächsten **EU-Strategie für die Rechte von Opfern** mit Opfern im Kindesalter und Online-Viktimisierung, die auch Cybermobbing umfassen kann, befassen – **2026**;

Die Mitgliedstaaten werden aufgefordert,

5. ihren nationalen Kontext zu analysieren, um eine **nationale Online-Sicherheits-App** mit maßgeschneiderter Unterstützung zur Verfügung zu stellen und – auf der Grundlage erfolgreicher bestehender nationaler Praxismodelle – **ein solches Modell an den nationalen Kontext anzupassen**, einschließlich z. B. Übersetzung, Branding, Vernetzung mit einschlägigen nationalen Unterstützungsdiensten und Meldeplattformen, wobei zentrale Funktionen wie sicheres Melden, Beweissicherung im Einklang mit dem nationalen Recht und garantierte Vertraulichkeit zu gewährleisten sind;

6. sicherzustellen, dass das Melden über die nationale Online-Sicherheits-App in **ein ganzheitliches und gut funktionierendes Ökosystem für Fallmanagement und Unterstützung** integriert wird, einschließlich koordinierter Offline-Unterstützung

(z. B. juristische, polizeiliche, soziale, psychologische und pädagogische Unterstützungsdienste);

7. **die nationale Online-Sicherheits-App den Online-Plattformen zur Integration in ihre Melde- und Benutzerunterstützungsinstrumente zur Verfügung zu stellen**, u. a. über Anwendungsprogrammierschnittstellen (API), sodass ressourceneffiziente und wirksame Meldungen und Reaktionen ermöglicht werden;

8. **für die breite Akzeptanz und Nutzung der nationalen Sicherheits-App durch alle einschlägigen Interessenträger zu werben;**

9. **Tools zu fördern, die von den Datenschutzbehörden** in ihren Landessprachen für Kinder **entwickelt wurden**, damit diese sich vor Online-Risiken wie Cybermobbing, Daten- oder Kontodiebstahl, versuchtem Betrug und sexueller Erpressung schützen können.

4. Internationale Öffentlichkeitsarbeit und Multi-Stakeholder-Zusammenarbeit

Die EU ist nicht nur bestrebt, das Wohlergehen und die Rechte von Kindern innerhalb ihrer Grenzen zu schützen, sondern will auch einen erheblichen Beitrag zur Förderung eines sichereren und inklusiveren digitalen Umfelds weltweit leisten. Der Tag des sicheren Internets ist inzwischen eine weltweite Kampagne, in der die Interessenträger aufgefordert werden, gemeinsam Maßnahmen zu ergreifen, um das Internet zu einem sichereren und besseren Ort für alle, insbesondere für Kinder und junge Menschen, zu machen und das Bewusstsein für die wichtigsten Online-Herausforderungen und neue Problematiken und Trends zu schärfen.

Der Schutz und die Befähigung von Minderjährigen zu selbstbestimmten Handeln im Internet sind eine globale Priorität. Dies spiegelt sich in der internationalen Digitalstrategie für die EU wider. Das von der EU kofinanzierte Netz von Hotlines in den Mitgliedstaaten zur Bekämpfung der Verbreitung von Material über sexuellen Kindesmissbrauch im Internet ist Teil des INHOPE-Netzwerks mit derzeit 57 weltweit tätigen Hotlines.

Die Kommission wird weiterhin mit gleich gesinnten Regulierungsbehörden im Bereich der Online-Sicherheit zusammenarbeiten, auch bei der Prävention und Bekämpfung von Cybermobbing, und zwar im Rahmen von Verwaltungsvereinbarungen (z. B. derzeit mit dem britischen Ofcom und der australischen eSafety-Kommissarin) und digitalen Partnerschaften (z. B. mit Kanada, Singapur und Indien).

Die EU wird im Einklang mit dem Globalen Digitalpakt eine Zusammenarbeit gegen Cybermobbing in internationalen Foren fördern. Organisationen der Vereinten Nationen haben Leitlinien und Instrumente entwickelt, die als bewährte Verfahren und Referenzwerte verwendet werden können, u. a. von UNICEF (Website und Open-Source-APIs), der Internationalen Fernmeldeunion (Leitlinien zur Online-Sicherheit von Kindern) sowie von der Sonderbeauftragten des Generalsekretärs der Vereinten Nationen zum Thema Gewalt gegen Kinder. Die EU unterstützt die Bemühungen der UNESCO, sich an die Regulierungsbehörden

zu wenden, um die UNESCO-Leitlinien für die Verwaltung von Online-Plattformen umzusetzen.

Die EU finanziert über das Instrument „NDICI/Europa in der Welt“ spezielle Sensibilisierungs- und Schutzprogramme für Kinder in Nicht-EU-Ländern, insbesondere in Kandidaten- und Nachbarländern – online und offline. Die EU unterstützt auch die Angleichung an die EU-Vorschriften im Rahmen des Beitrittsprozesses für Kandidatenländer und potenzielle Kandidatenländer und fördert durch den Austausch von Wissen und bewährten Verfahren im Rahmen des Programms Safer-Internet-Zentren+ (SIC+) die Online-Sicherheit von Kindern und jungen Menschen in Nachbarländern.

5. Nächste Schritte

Die Kommission wird die Umsetzung des Aktionsplans und seiner drei Säulen überwachen und dabei eng mit den Mitgliedstaaten, den SIC und anderen Interessenträgern zusammenarbeiten. Fortschritte, Herausforderungen und bewährte Verfahren werden mithilfe bestehender Instrumente wie dem jährlichen Bericht über die Politik für ein besseres Internet für Kinder (BIK Map Tool), den Berichten der SIC und dem regelmäßigen Austausch in Expertenforen verfolgt, um eine transparente und partizipative Überwachung zu gewährleisten.

Die Kommission wird mit den Mitgliedstaaten zusammenarbeiten, um in nationale Strategien oder Maßnahmen gegen Cybermobbing Überwachungsrahmen zu integrieren und dabei die Umsetzung, Barrierefreiheit, Inklusivität und Anpassungsfähigkeit an sich verändernde digitale Kontexte zu bewerten, wobei Kinder und junge Menschen einbezogen werden sollen. Die Erkenntnisse sollen auf EU-Ebene ausgetauscht werden, um das gegenseitige Lernen und die Angleichung der Politik zu fördern, und in Aktualisierungen von Initiativen im Rahmen von BIK+ und des Gesetzes über digitale Dienste mit einfließen.

Die Kommission wird 2029 eine Bestandsaufnahme dieses Aktionsplans vornehmen, unter anderem durch Konsultationen mit Kindern und jungen Menschen.

6. Schlussfolgerungen

> *„Wir wollen einen sicheren Online-Raum für Kinder, für junge Menschen und für die nächste Generation, aber wir haben ihn noch nicht. Wir haben einige Probleme. Und das sind Probleme, die nicht nur diese Generation betreffen. Daher brauchen wir Hilfe von der EU, um unsere Online-Räume sicher zu machen. Irgendwo müssen wir anfangen. Und zwar jetzt. Für unsere Zukunft.“*
>
> Zitat von Kindern, die Mitglieder der EU-Plattform für die Beteiligung von Kindern sind

Kinder und junge Menschen bitten uns um Hilfe, damit wir Online-Räume sicher machen – für sie, für ihre Freunde und für künftige Generationen. Wir müssen uns in unserer gesamten Union dieser Herausforderung stellen, denn der Schutz und die Handlungskompetenz unserer Kinder und jungen Menschen sollten nicht von einer Postleitzahl abhängen.

Aufbauend auf einem bereits soliden EU-Instrumentarium rechtlicher und politischer Maßnahmen gegen Online-Schäden und auf Beiträgen eines breiten Spektrums von Interessenträgern wird dieser Aktionsplan dazu beitragen, ein sicheres, inklusives und befähigendes digitales Umfeld für Kinder und junge Menschen in Europa zu schaffen. Er wird laufende EU-Initiativen in den Bereichen sichereres Internet, Verantwortung von Plattformen, digitale Fähigkeiten und Bildung, Stärkung der Rolle von Kindern und jungen Menschen, Datenerhebung und internationale Zusammenarbeit ergänzen und ihnen neue Impulse geben.

Die Kommission ersucht das Europäische Parlament und den Rat, den Aktionsplan zu billigen und bei dessen Umsetzung zusammenzuarbeiten. Die Kommission fordert den Ausschuss der Regionen und den Europäischen Wirtschafts- und Sozialausschuss auf, den Dialog mit den lokalen und regionalen Behörden, den Wirtschafts- und Sozialpartnern und der Zivilgesellschaft zu fördern.

ANHANG: Zentrale Maßnahmen und Zeitplan

Säule I: Koordinierter EU-Ansatz beim Schutz

Die Kommission wird	
bei der Überarbeitung **der Leitlinien zum Schutz Minderjähriger im Rahmen des Gesetzes über digitale Dienste** den Fokus auf die Bekämpfung von Cybermobbing ausweiten;	2026
Leitlinien zu vertrauenswürdigen Hinweisgebern im Rahmen des Gesetzes über digitale Dienste erlassen, die dazu beitragen werden, die Rolle dieser Hinweisgeber bei der Bekämpfung rechtswidriger Inhalte, z. B. von rechtswidrigem Cybermobbing, zu klären;	bis zum 2. Quartal 2026
Möglichkeiten zur Bekämpfung von Cybermobbing auf Video-Sharing-Plattformen bewerten, und zwar während der laufenden **Evaluierung der Richtlinie über audiovisuelle Mediendienste** und ihrer Überarbeitung;	bis zum 3. Quartal 2026
die **wirksame Umsetzung der Bestimmungen der KI-Verordnung zu verbotenen KI-Praktiken**, auch im Hinblick auf ihren Einsatz zum Zwecke des Cybermobbings, unterstützen;	ab dem 3. Quartal 2026
die **wirksame Umsetzung der in der KI-Verordnung vorgeschriebenen Transparenzpflichten hinsichtlich der Markierung und Kennzeichnung von KI-generierten Inhalten** erleichtern, auch in Bezug auf Cybermobbing.	ab dem 3. Quartal 2026

Die Mitgliedstaaten werden aufgefordert,
umfassende nationale Pläne zur Bekämpfung von Mobbing, einschließlich Cybermobbing, einzuführen, insbesondere mit der Unterstützung des EU-Netzes für die Rechte des Kindes;
kohärente, vergleichbare Daten über Cybermobbing zu erheben, was durch das Netz der Safer-Internet-Zentren und die Plattform „Besseres Internet für Kinder“ erleichtert wird.

Säule II: Prävention und Sensibilisierung

Die Kommission wird	
Cybermobbing bei der **Aktualisierung der Leitlinien für Lehrkräfte und pädagogische Fachkräfte zur Bekämpfung von Desinformation und zur Förderung der digitalen Kompetenz** berücksichtigen;	bis zum 2. Quartal 2026

die **staatsbürgerliche Bildung in Schulen stärken**, und zwar durch einen Kompetenzrahmen und Leitlinien für die Unionsbürgerschaft;	2027

die digitale Kompetenz, die Prävention von Cybermobbing und das digitale Wohlbefinden durch **den Fahrplan für die Zukunft der digitalen Bildung und Kompetenzen bis 2030** stärken;	bis zum 3. Quartal 2026
im bevorstehenden **EU-Aktionsplan zum Schutz von Kindern vor Kriminalität** einen Beitrag zur Prävention von Cybermobbing leisten;	bis zum 3. Quartal 2026
Ressourcen und Schulungen zum Thema Cybermobbing für Schulen sowie für die nichtformale und informelle Bildung, die für Menschen mit Behinderungen zugänglich sind, ausbauen, und zwar über die BIK-Plattform, die SIC und das Europäische Jugendportal;	ab dem 2. Quartal 2026
die Gruppe im Rahmen der „Offenen Methode der Koordinierung“ zur Bekämpfung von Hetze im Sport bei ihrer Arbeit an **Empfehlungen zur Bekämpfung von Cybermobbing im Sportumfeld** unterstützen.	bis zum 4. Quartal 2026

Die Mitgliedstaaten werden aufgefordert,
die Prävention und frühzeitige Erkennung von Cybermobbing durch **Leitlinien und Schulungen für Interessenträger** wie pädagogisches Fachpersonal, Betreuungspersonen und Fachkräfte, die in unterschiedlichen Bereichen mit Kindern arbeiten zu stärken;
die **Beteiligung von Kindern** an der Politikgestaltung und der Umsetzung von Maßnahmen zum Wohlergehen von Kindern **zu stärken**.

Säule III: Meldung und umfassende Unterstützung

Die Kommission wird	
die Einführung **einer barrierefreien Online-Sicherheits-App** in allen Mitgliedstaaten unterstützen;	ab dem 3. Quartal 2026
Opfer im Kindesalter und Online-Viktimisierung, die auch Cybermobbing umfassen kann in der nächsten **EU-Strategie für die Rechte von Opfern** berücksichtigen.	2026

Die Mitgliedstaaten werden aufgefordert,
ihre jeweiligen nationalen Umstände zu prüfen, um **eine nationale Online-Sicherheits-App** zur Verfügung zu stellen und – auf der Grundlage erfolgreicher bestehender nationaler Praxismodelle – ein solches Modell an die nationalen Umstände anzupassen;
sicherzustellen, dass das Melden über die nationale Online-Sicherheits-App in **ein ganzheitliches und gut funktionierendes Unterstützungs-Ökosystem** integriert wird;
die nationale Online-Sicherheits-App den Online-Plattformen zur Integration in ihre Melde- und Benutzerunterstützungsinstrumente **zur Verfügung zu stellen**;
bei den einschlägigen Interessenträgern **für die nationale Online-Sicherheits-App zu werben**;
Tools zu fördern, die von den Datenschutzbehörden in ihren Landessprachen für Kinder **entwickelt wurden**, damit diese sich vor Online-Risiken wie Cybermobbing schützen können.