



EUROPESE
COMMISSIE

Straatsburg, 10.2.2026
COM(2026) 71 final

**MEDEDELING VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT, DE
RAAD, HET EUROPEES ECONOMISCH EN SOCIAAL COMITÉ EN HET COMITÉ
VAN DE REGIO'S**

Actieplan tegen cyberpesten

"Veiliger online, samen sterker"

1. Inleiding

“Techbedrijven zijn geen liefdadigheidsinstellingen. Maar ouders leven dag aan dag met de daarmee samenhangende risico’s en schade: cyberpesten. Aanmoediging van zelfbeschadiging. Onlinekinderlokkers. Verslavende algoritmen. Het is aan ons om de komende generatie te beschermen.”

Voorzitter Von der Leyen, toespraak tijdens het evenement op hoog niveau “Protecting Children in the Digital Age” 2025

De digitale transformatie heeft de samenleving radicaal veranderd. Ze biedt kinderen en jongeren enorme mogelijkheden om hun vaardigheden en creativiteit te ontwikkelen. Tegenwoordig gebruikt 97 % van de jongeren in de EU [dagelijks het internet](#), en voor gebruikers tussen 15 en 24 jaar zijn socialemediaplatforms [de meest gebruikte informatiebron](#) (65 %). Samen met AI-instrumenten, videogames, berichtenapps en onlinegemeenschappen zorgen ze voor verbinding en maken ze contacten mogelijk.

Deze platforms brengen echter ook risico’s met zich mee: blootstelling aan onlinekinderlokkers, aanmoediging van zelfbeschadiging, verslavende algoritmen, gevaarlijke online-uitdagingen en cyberpesten.

De grondrechten, [met inbegrip van de kinderrechten](#), zijn essentieel voor de waarden van de EU en moeten zowel online als offline worden geëerbiedigd. Kinderen en jongeren hebben het recht om veilig informatie te zoeken, te leren, verbonden te zijn en betrokken leden van de samenleving te worden. De vrijheden en mogelijkheden van de digitale wereld moeten daarom gepaard gaan met onze vastberadenheid om onze kinderen en jongeren te beschermen en mondiger te maken. De belofte van het digitale tijdperk mag niet worden ondermijnd door gedrag dat vernedert, uitsluit of schaadt.

Cyberpesten ondermijnt het vertrouwen en schaadt het gevoel van eigenwaarde. Het sluit mensen uit en beperkt hun potentieel. Het ondermijnt onze gedeelde ambitie van een levendig, inclusief en digitaal Europa voor onze kinderen en jongeren.

Sociale media zijn een primair kanaal waarlangs kinderen en adolescenten worden blootgesteld aan cyberpesten, en er zijn steeds meer aanwijzingen dat hun blootstelling aan ongepaste online-inhoud blijvende, schadelijke gevolgen heeft. De EU beschikt reeds over een uitgebreid [rechts- en beleidskader](#) om kinderen online te beschermen en mondiger te maken, en daarvan is de [digitaledienstenverordening](#) het belangrijkste instrument.

Zoals aangekondigd in de Staat van de Unie van 2025, vraagt voorzitter Von der Leyen deskundig advies over leeftijdsbeperkingen op sociale media in Europa in het licht van onlinerisico’s, en de aanbevelingen in dat verband worden in de zomer van 2026 verwacht. Een aantal lidstaten overweegt stappen te ondernemen om afdwingbare minimumleeftijden voor toegang tot sociale media in te voeren, alsook vereisten voor ouderlijke toestemming en controle. Daarbij gaat het onder meer over het afstemmen van leeftijdsdrempels voor toegang tot sociale media op de digitale toestemmingsleeftijd, het verplicht stellen van privacy door

standaardinstellingen voor minderjarigen en het opzetten van oplossingen voor anonieme leeftijdsverificatie.

Een gecoördineerde Europese aanpak van leeftijdsdrempels zou ervoor zorgen dat alle Europese kinderen gelijke bescherming krijgen en zou juridische versnippering op de eengemaakte digitale markt voorkomen. Het deskundigenpanel zal de weg vrijmaken voor een gecoördineerde, mogelijk wetgevende Europese aanpak van leeftijdsdrempels en een empirisch onderbouwde bewustmakingscampagne, waardoor ouders in staat worden gesteld de toegang van hun kinderen tot online-inhoud doeltreffend te controleren.

De jongerenadviesraad heeft ook met de voorzitter van de Commissie de standpunten van jongeren over deze kwestie gedeeld. De Commissie test samen met de lidstaten een [oplossing voor leeftijdsverificatie](#) die gebruiksvriendelijk is, de privacy beschermt en een “referentienorm” voor leeftijdsverificatie online vaststelt. Het Europees Parlement heeft [opgeroepen](#) tot een geharmoniseerde Europese digitale leeftijdsgrens van 16 jaar voor toegang tot sociale media, videoplatforms en AI-chatbots, waarbij 13- tot 16-jarigen toegang krijgen met toestemming van de ouders.

De Commissie zal ook een EU-breed onderzoek starten om een empirisch onderbouwd debat op gang te brengen over de impact van sociale media en overmatig schermgebruik op het welzijn en de geestelijke gezondheid van jongeren.

Voor kinderen die online zijn, blijft cyberpesten een grote bedreiging die een gecoördineerde respons op EU- en nationaal niveau vereist. De verantwoordelijkheid van onlineplatforms om veiligheid door ontwerp (safety-by-design) te waarborgen, komt op de eerste plaats. Om cyberpesten aan te pakken, is samenwerking op alle bestuursniveaus nodig, met inbegrip van regelgevende en rechtshandavingsautoriteiten, alsook een maatschappijbrede aanpak, waarbij ouders, professionals, opvoeders, het maatschappelijk middenveld en de jongeren zelf worden betrokken.

Zoals aangekondigd in de [politieke beleidslijnen 2024-2029 van de Commissie](#), bevat deze mededeling een gericht actieplan om de toenemende trend van onlinemisbruik krachtig te bestrijden. Het is in de eerste plaats gericht op kinderen en jongeren, ook rekening houdend met de toegenomen kwetsbaarheid van bepaalde groepen. Veel van de voorgestelde maatregelen zullen echter helpen om cyberpesten onder de bredere bevolking aan te pakken.

De Commissie zal alle instrumenten waarover zij beschikt, gebruiken om de digitaledienstenverordening aan te vullen en ervoor te zorgen dat digitale platforms hun volledige verantwoordelijkheid nemen voor het opsporen en bestrijden van cyberpesten. Zij zal alle lidstaten ondersteunen bij het overnemen van de beste praktijken die in de EU beschikbaar zijn, teneinde hun strijd tegen cyberpesten zo doeltreffend mogelijk te maken. Zij zal ook de inspanningen opvoeren om met informatie alle geledingen van de samenleving te bereiken en het bewustzijn te vergroten over hoe cyberpesten eruitziet, hoe cyberpesten kan worden voorkomen en hoe slachtoffers kunnen worden ondersteund.

Met dit actieplan nodigt de Commissie de lidstaten, regionale en lokale autoriteiten, onlineplatforms, het maatschappelijk middenveld, onderwijsinstellingen, gezinnen, en kinderen en jongeren zelf uit om zich in te zetten voor een gezamenlijke inspanning: ervoor

zorgen dat de digitale ruimte veilig, respectvol, inclusief en ondersteunend is. De Commissie stelt voor dat onze Unie eensgezind opkomt voor het geestelijk welzijn en de waardigheid van alle kinderen en jongeren.

2. Cyberpesten: het probleem

Cyberpesten treft kinderen overal: 18,3 % van de kinderen wereldwijd heeft te maken gehad met cyberpesten via instant messaging, berichten op sociale media, e-mails of tekstberichten. Cyberpesten gebeurt niet alleen via tekst, maar ook via audiovisuele inhoud zoals [foto's of video's](#) die online worden gedeeld.

In Europa geeft ongeveer [een op de zes kinderen](#) in de leeftijd van 11 tot 15 jaar aan het slachtoffer te zijn geweest van cyberpesten en geeft ongeveer een op de acht toe anderen te pesten. Tussen 2018 en 2022 steeg het aantal [gecyberpeste adolescenten](#) met een kwart voor jongens en bijna een kwart voor meisjes. De afgelopen vijf jaar is cyberpesten steeds [de belangrijkste reden](#) geweest om contact op te nemen met de hulplijnen van de centra voor een veiliger internet (SIC's).

De 6 343 respondenten van 12 tot 17 jaar die voor dit actieplan werden geraadpleegd, meldden [wijdverbreide blootstelling aan cyberpesten](#): 1 op de 4 kinderen en tieners in de leeftijd van 12 tot 17 jaar heeft persoonlijk te maken gehad met cyberpesten, en meer dan 1 op de 3 is getuige geweest van cyberpesten.

2.1 Wat is cyberpesten?

Digitale technologieën hebben de mogelijkheden voor verbinding vergroot, maar ook de onlinerisico's, zoals sociale uitsluiting, haatmisdrijven, intimidatie, vernedering en misbruik, die fysieke grenzen kunnen overschrijden en de klok rond kunnen aanhouden.

Met het oog op dit actieplan is de Commissie voornemens **een gemeenschappelijke definitie van cyberpesten** te bevorderen:

Met cyberpesten wordt **gedrag bedoeld dat wordt gesteld met behulp van digitale technologieën, met als voornaamste doel of gevolg dat met name kinderen of jongeren herhaaldelijk of voortdurend worden vernederd, sociaal uitgesloten, misbruikt, geïntimideerd of benadeeld.**

Herhaling wordt gezien als een [belangrijk kenmerk](#) van pesten en cyberpesten. Het heeft betrekking op de aanhoudende gevolgen voor het slachtoffer, dat ook kan vrezen dat een eenmalige gebeurtenis herhaaldelijk online kan worden gedeeld, waardoor het trauma wordt verlengd en het slachtoffer opnieuw slachtoffer wordt zonder verdere directe betrokkenheid van de dader.

Machtsongelijkheid staat centraal bij pesten, maar kan zich online anders manifesteren. Bij traditioneel pesten is machtsongelijkheid vaak het gevolg van fysieke kracht, sociale status of groepsnormen. Bij cyberpesten is het ook het gevolg van ongelijke niveaus van digitale invloed, digitale vaardigheden, toegang tot technologie of controle over inhoud.

Cyberpesten is steeds moeilijker aan te pakken, aangezien het zich op elk moment en overal op persoonlijke apparaten kan voordoen, zonder fysieke aanwezigheid van de dader. Bovendien vindt het ook plaats via niet openbaar beschikbare kanalen.

De meest voorkomende vormen van cyberpesten zijn onder meer gemene of kwetsende opmerkingen, het online verspreiden van geruchten of het delen van beschamende of vernederende berichten.

De anonimiteit, het brede bereik van het publiek en de mogelijkheid om op elk moment privéberichten naar personen te sturen, vergroten de schade van traditioneel pesten. Bovendien bevorderen digitale omgevingen morele onverschilligheid, verminderde empathie en online ongeremdheid, waardoor de belemmeringen voor online-agressie worden verminderd.

Schadelijke inhoud kan voor onbepaalde tijd online blijven. Hij kan voortdurend worden geraadpleegd en opnieuw worden gedeeld, of viraal worden gemaakt, wat de schade vergroot, revictimisatie veroorzaakt en het herstel belemmert. Met deze factoren moet rekening worden gehouden bij het verlenen van doeltreffende steun. Dit vergroot het potentiële publiek en maakt een continuüm van agressie tussen fysieke en onlineruimten of omgekeerd mogelijk.

De huidige snelle digitale ontwikkeling betekent dat de omgevingen en instrumenten die worden gebruikt om schade toe te brengen, voortdurend veranderen. Om flexibiliteit te waarborgen, moeten de nieuwste technologieën worden gebruikt om deze op te sporen en aan te pakken.

Hoewel artificiële intelligentie (AI) kan helpen bij het opsporen van cyberpesten, vergroten de toenemende toepassing van AI, met name generatieve AI (GenAI), en de integratie ervan in online-apps en -diensten met name de risico's en instrumenten van cyberpesten of creëren zelfs nieuwe risico's en instrumenten. Deepfakes zijn bijvoorbeeld in opkomst en leiden in toenemende mate tot misbruik van seksueel expliciete deepfakes, dat voor het overgrote deel gericht is tegen vrouwen en meisjes, onder meer in gevallen van cyberpesten, en waarbij schadelijk gedrag strafbaar wordt wanneer het gaat om het creëren van beelden die seksueel misbruik van kinderen of gendergerelateerd cybergeweld vormen. Dit introduceert een extra dimensie van schade die niet alleen de reputatie schaadt, maar, net als ander cyberpesten, ook kan leiden tot psychologische trauma's, wat onderstreept dat deze opkomende risico's dringend op EU-niveau moeten worden gemonitord en aangepakt.

Cyberpesten en haatmisdrijven kunnen elkaar overlappen wanneer cyberpesten wordt ingegeven door haat of aanzet tot geweld en haat, en gericht is tegen personen door te verwijzen naar bepaalde beschermde kenmerken. [Kaderbesluit 2008/913/JBZ van de Raad](#) verplicht de lidstaten het publiekelijk aanzetten tot geweld of haat tegen een groep personen, of een lid van zo'n groep, die wordt gedefinieerd op basis van ras, huidskleur, godsdienst, afstamming, dan wel etnische afkomst, strafbaar te stellen. De lidstaten moeten er ook voor zorgen dat aanvullende straffen worden opgelegd voor strafbare feiten die worden gepleegd met racistische of xenofobe motieven.

Cyberpesten kan overlappen met seksueel misbruik van kinderen in de zin van [Richtlijn 93/2011](#) ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie.

[Richtlijn \(EU\) 2024/1385](#) ter bestrijding van geweld tegen vrouwen en huiselijk geweld verplicht de lidstaten ervoor te zorgen dat het online aanzetten tot geweld of haat op basis van gender strafbaar wordt gesteld. Ook andere strafbare feiten in verband met cybergeweld, die vaak plaatsvinden in het kader van cyberpesten, worden strafbaar gesteld: het zonder instemming delen van intiem of gemanipuleerd materiaal, cyberstalking en cyberintimidatie. De richtlijn bevat ook bepalingen om de snelle verwijdering van illegaal materiaal met betrekking tot cybergeweld mogelijk te maken.

2.2 Groepen die het risico lopen op cyberpesten

Cyberpesten komt veel voor bij **schoolgaande kinderen en adolescenten**, vooral omdat hun online-activiteiten toenemen.

Meisjes en jonge vrouwen worden blootgesteld aan pestgedrag van seksistische en misogyne aard en worden in onevenredige mate getroffen, bijvoorbeeld door het [zonder toestemming delen van intieme beelden](#) en [seksueel expliciete deepfakes](#).

Kwetsbare groepen worden in onevenredige mate blootgesteld aan cyberpesten, aangezien cyberpesten gericht kan zijn op een persoon omdat hij of zij wordt geacht tot dergelijke groepen te behoren.

Kinderen uit huishoudens met een laag inkomen zijn [meer](#) blootgesteld aan cyberpesten dan hun leeftijdsgenoten.

Kinderen en jongeren met een handicap zijn [vaker online slachtoffer](#), ook van seksueel en genderbaseerd geweld. Sommigen trekken zich zelfs uit de digitale ruimte terug als gevolg van voortdurend misbruik.

Etnische en religieuze minderheden, migranten en vluchtelingen lopen een verhoogd risico op racistische of discriminerende pesterijen. [Roma en andere raciale of etnische minderheden](#) worden bijvoorbeeld in het bijzonder blootgesteld aan online-intimidatie en illegale haatzaaiende uitlatingen in verband met systemische uitsluiting, en 90 % van de [Joodse Europeanen](#) gaf aan het afgelopen jaar online te maken te hebben gehad met antisemitisme.

Van de **lhbtq+-personen** wordt 63 % vaak geconfronteerd met gewelddadige online-inhoud tegen de [lhbtq+-gemeenschap](#). Bovendien meldde 11 % dat het afgelopen jaar aanstootgevende of bedreigende opmerkingen over hen op het internet waren geplaatst, en twee derde van hen heeft tijdens hun schooltijd te maken gehad met spot of intimidatie.

De in dit actieplan voorgestelde maatregelen zullen bijdragen tot de aanpak van cyberpesten voor alle slachtoffers. Bij de uitvoering zal rekening worden gehouden met de hierboven geschetste gelijkheidsoverwegingen om het effect van de acties te vergroten.

2.3 De gevolgen van cyberpesten

Cyberpesten kan ernstige en langdurige gevolgen hebben, zowel voor individuen als voor de samenleving in het algemeen. Op korte termijn kan cyberpesten een eerste stap zijn in de richting van ernstigere vormen van criminaliteit of misbruik, waaronder seksueel misbruik.

[Slachtoffers van cyberpesten](#) lopen een verhoogd risico op angst, depressie, eenzaamheid, zelfbeschadiging en zelfmoordgedrag, en zijn vatbaarder voor gedragsproblemen, waaronder schadelijk copinggedrag. Bovendien kunnen degenen die te maken krijgen met cyberpesten, zelf aan cyberpesten gaan doen, al was het maar in een poging om hun rol als slachtoffer te ontlopen. Dit vereist een zorgvuldige en kindvriendelijke respons.

Cyberpesten kan ook schadelijk zijn voor de schoolprestaties, het welzijn van leerlingen en de schoolomgeving. Dit kan langetermijnevolgen hebben voor onderwijs- en loopbaantrajecten, alsook voor het algemene welzijn van leerlingen of studenten, en hun tevredenheid met het leven.

De gevolgen voor kinderen en jongeren kunnen dus verstrekkend zijn voor de samenleving, waardoor de bestaande ongelijkheden worden verergerd.

3. Volgende stappen

Er is behoefte aan een robuustere, consistentere en beter gecoördineerde EU-respons op cyberpesten, die de inspanningen op het gebied van preventie en digitale geletterdheid versterkt en meldingen en slachtofferhulp in de hele Unie verbetert en vereenvoudigt. Onze visie is een Europa waar elk kind en elke jongere kan opgroeien zonder cyberpesten, beschermd in zijn waardigheid en mondig genoeg om te gedijen in een digitale wereld die de Europese waarden eerbiedigt. Daartoe is dit actieplan gebaseerd op drie onderling verbonden pijlers: een gecoördineerde EU-aanpak, preventie en bewustmaking, en melding en ondersteuning.

Deze oproep tot actie wordt gesteund door de publieke opinie: [meer dan 9 op de 10 Europeanen](#) vinden dat overheidsinstanties dringend maatregelen moeten nemen om kinderen tegen cyberpesten te beschermen. Uit de [openbare raadpleging](#) ter ondersteuning van dit plan is gebleken dat er sterke steun is voor programma's voor digitale geletterdheid en empathie-opbouw op scholen en in lerarenopleidingen, en voor betere meldingsinstrumenten en ondersteuningsdiensten voor slachtoffers.

3.1 Pijler I: Een gecoördineerde EU-aanpak van bescherming

De Commissie zal ten volle gebruikmaken van de bestaande beleids- en rechtsinstrumenten en in het kader van toekomstige initiatieven nagaan welke mogelijkheden er zijn om cyberpesten te bestrijden. Bovendien **wordt de lidstaten verzocht gemeenschappelijke doelstellingen om te zetten in doeltreffende nationale maatregelen en een geïntegreerd en goed functionerend ecosysteem op te bouwen om cyberpesten aan te pakken.**

De digitaaldienstenverordening blijft van cruciaal belang voor de handhavingsinspanningen en verplicht aanbieders van voor minderjarigen toegankelijke onlineplatforms om te zorgen voor een hoog niveau van privacy, veiligheid en beveiliging van minderjarigen op hun dienst.

Voorts bevatten de [richtsnoeren inzake de onlinebescherming van minderjarigen in het kader van de digitaaldienstenverordening](#) maatregelen die aanbieders van onlineplatforms moeten nemen om aan die verplichting te voldoen, met inbegrip van passende maatregelen om het risico te verminderen dat minderjarigen worden blootgesteld aan schadelijke inhoud, zoals het

ontwerpen van aanbevelingssystemen in het belang van de minderjarigen, of aan schadelijk gedrag, met inbegrip van contactgerelateerde risico's als gevolg van interacties met leeftijdsgenoten. Om slachtoffers van cyberpesten te beschermen, omvatten deze richtsnoeren verder maatregelen voor gebruikerscontrole en mondigheid, kindvriendelijke meldingsmechanismen en klachteninstrumenten, evenals inhoudsmoderatie in de officiële talen van de lidstaat waar de dienst wordt verleend. De digitaledienstenverordening verplicht aanbieders van onlineplatforms ook om gemakkelijk toegankelijke en gebruiksvriendelijke mechanismen in te voeren waarmee alle gebruikers, met inbegrip van minderjarigen, illegale inhoud kunnen melden, zoals bepaalde vormen van haatzaaiende uitlatingen of kinderpornografie. Afhankelijk van de nationale wetgeving kunnen vormen van cyberpesten ook illegaal zijn. Aanbieders moeten onmiddellijk na ontvangst van dergelijke meldingen besluiten nemen.

Dit actieplan zal als input dienen voor de komende herziening en actualisering van de richtsnoeren inzake de onlinebescherming van minderjarigen in het kader van de digitaledienstenverordening. De richtsnoeren kunnen aanbieders van onlineplatforms met name helpen efficiëntere meldingsinstrumenten te ontwerpen, bijvoorbeeld met betrekking tot hun zichtbaarheid, technische toegankelijkheid en taalregeling, en doeltreffende technologieën te gebruiken om blootstelling aan cyberpesten te voorkomen. De richtsnoeren kunnen aanbieders ook helpen bij het ontwerpen van passende maatregelen om te reageren op meldingen van minderjarigen, bijvoorbeeld door gebruikers te ondersteunen bij het opslaan van informatie die als bewijsmateriaal kan dienen.

De digitaledienstenverordening voorziet ook in de mogelijkheid om te beschikken over [“betrouwbare flaggers”](#), deskundige entiteiten waarvan de meldingen voorrang moeten krijgen. Deze bepalingen kunnen worden gebruikt om cyberpesten aan te pakken, waarbij betrouwbare flaggers bijdragen tot het aanpakken van de verspreiding van illegale inhoud waarmee wordt gecyberpest. De Commissie zal richtsnoeren over betrouwbare flaggers uitvaardigen om hun rol bij de bestrijding van illegale inhoud, met inbegrip van illegaal cyberpesten, te helpen verduidelijken. Deze richtsnoeren zullen ook bijdragen tot de verduidelijking van de verplichtingen van aanbieders van onlineplatforms met betrekking tot meldingen van betrouwbare flaggers.

Cyberpesten kan ook plaatsvinden via audiovisuele online-inhoud. De [richtlijn audiovisuele mediadiensten](#) bevat algemene voorschriften om minderjarigen, met name online, te beschermen tegen schadelijke inhoud die hun lichamelijke, geestelijke of morele ontwikkeling kan aantasten. Daaronder valt ook inhoud waarmee wordt gecyberpest. Op grond van de richtlijn audiovisuele mediadiensten moeten videoplatforms passende maatregelen nemen om te voorkomen dat minderjarigen toegang krijgen tot schadelijke inhoud door normen voor media-inhoud op te nemen in de algemene voorwaarden of systemen voor ouderlijk toezicht en beoordeling van inhoud. Voorts zijn de lidstaten verplicht de menselijke waardigheid te beschermen bij de uitvoering van de richtlijn audiovisuele mediadiensten. Bij de lopende evaluatie en herziening van de richtlijn zal worden beoordeeld hoe doeltreffend videoplatforms deze regels hebben toegepast en of er meer moet worden gedaan om minderjarigen te beschermen tegen schadelijke online-inhoud, onder meer met betrekking tot cyberpesten, en in overeenstemming met de digitaledienstenverordening.

De [verordening artificiële intelligentie](#) verbiedt AI-systemen die personen manipuleren of misleiden door kwetsbaarheden in verband met hun leeftijd uit te buiten om hun gedrag te verstoren, en daarbij aanzienlijke schade veroorzaken. Deze verbodsbepalingen kunnen cyberpesten voorkomen. De Commissie heeft [richtsnoeren inzake de verboden AI-praktijken](#) vastgesteld om een consistente en doeltreffende uitvoering in de hele Unie te vergemakkelijken. De AI-verordening bevat ook transparantievereisten, waaronder de verplichting om gebruikers te informeren wanneer zij met AI interageren en om door AI gegenereerde of gemanipuleerde inhoud, zoals deepfakes, duidelijk aan te merken om misleiding te voorkomen.

Bovendien moet dit beleid worden aangevuld met het verzamelen van gegevens over cyberpesten, dat momenteel inconsistent is, waardoor een volledig inzicht in de trends in de lidstaten wordt belemmerd. Naar aanleiding van de oproep in het kader van de openbare raadpleging zal de Commissie het verzamelen van consistente en vergelijkbare gegevens over cyberpesten in de hele EU vergemakkelijken, bijvoorbeeld door richtsnoeren vast te stellen, zoals een gemeenschappelijk kader voor gegevensverzameling en indicatoren, en door EU-brede enquêtes te houden via het platform “Better Internet for Kids” (BIK), in samenwerking met andere mechanismen voor de participatie van kinderen en jongeren. Er zullen voldoende middelen ter beschikking worden gesteld om het netwerk van [centra voor een veiliger internet \(SIC's\)](#) in staat te stellen deze extra taken op zich te nemen en de continuïteit van deze werkzaamheden op lange termijn te waarborgen.

De Commissie zal:

1. bij de **herziening van de richtsnoeren inzake de onlinebescherming van minderjarigen in het kader van de digitaledienstenverordening** meer aandacht besteden aan de bestrijding van cyberpesten, met name wat betreft maatregelen om blootstelling aan schadelijke inhoud verder te voorkomen, en de meldingssystemen van onlineplatforms te verbeteren — gepland voor **2026**;
2. **richtsnoeren inzake betrouwbare flaggers in het kader van de digitaledienstenverordening vaststellen** om de rol ervan bij de bestrijding van illegale inhoud, met inbegrip van inhoud waarmee wordt gecyberpest, te helpen verduidelijken – **uiterlijk in het tweede kwartaal van 2026**;
3. manieren beoordelen om cyberpesten op videoplatforms aan te pakken in het kader van de lopende **evaluatie van de richtlijn audiovisuele mediadiensten en de herziening ervan** — **uiterlijk in het derde kwartaal van 2026**;
4. **de doeltreffende uitvoering van de bepalingen van de AI-verordening inzake verboden AI-praktijken ondersteunen**, ook wanneer deze worden gebruikt voor cyberpesten, door middel van coördinatie binnen de AI-board en de richtsnoeren van de Commissie inzake verboden AI-praktijken — **vanaf het derde kwartaal van 2026**;
5. **de doeltreffende uitvoering van de transparantieverplichtingen van de AI-verordening vergemakkelijken, onder meer door middel van een praktijkcode**

voor het aanmerken en labelen van door AI gegenereerde inhoud, die tot doel heeft de naleving van de transparantieplichtingen van de AI-verordening met betrekking tot het aanmerken en labelen van door AI gegenereerde inhoud te ondersteunen, ook wanneer deze wordt gebruikt voor cyberpesten — **vanaf het derde kwartaal van 2026**.

De lidstaten wordt verzocht:

1. **uitgebreide nationale plannen ter bestrijding van pesten, met inbegrip van cyberpesten** op te stellen, met de steun van het EU-netwerk voor kinderrechten in overeenstemming met de [mededeling van de Commissie en de aanbeveling over geïntegreerde systemen voor kinderbescherming](#);
2. de in dit actieplan voorgestelde gemeenschappelijke definitie van cyberpesten te gebruiken om **consistente, vergelijkbare gegevens over cyberpesten te verzamelen**, gefaciliteerd door de steun van de Commissie via het netwerk van centra voor een veiliger internet en het platform “Better Internet for Kids”, en gezamenlijk te werken aan gemeenschappelijke normen voor de aanpak van cyberpesten in de hele EU.

3.2 Pijler II: preventie en bewustmaking

Cyberpesten kan het best worden bestreden door op te treden voordat zich schadelijke incidenten voordoen. Om cyberpesten te voorkomen, zijn vanaf jonge leeftijd gezonde digitale praktijken nodig. Het betekent dat kinderen, jongeren en volwassenen moeten worden toegerust met de vaardigheden en het vertrouwen om over onlineriesico's te spreken en deze te herkennen. Het is ook belangrijk om de onderliggende attitudes aan te pakken die kunnen leiden tot schadelijk onlinegedrag.

Om doeltreffend te zijn, moeten bij preventie-inspanningen omstanders, leeftijdsgenoten, daders, ouders, verzorgers, opvoeders en de bredere schoolgemeenschap worden betrokken, met de steun van alle relevante actoren, met name maatschappelijke organisaties. Dit werd gesteund door 62 % van de respondenten van de openbare raadpleging, die benadrukten dat de beroepsopleiding van opvoeders, rechtshandhavers en maatschappelijk werkers moet worden ondersteund.

Preventie- en bewustmakingsinitiatieven moeten ook plaatsvinden in informele en niet-formele leeromgevingen, zoals jeugdcentra, sportclubs en gemeenschapsomgevingen, waar kinderen en jongeren een groot deel van hun tijd doorbrengen. Dergelijke initiatieven moeten ook de preventie en bestrijding van alle vormen van discriminatie omvatten, in synergie met de gelijkheidsstrategieën van de EU.

Digitaal onderwijs en digitale geletterdheid zijn steeds meer nodig om veilig en verantwoord door de onlinewereld te navigeren. Het informeren van kinderen en jongeren over het belang van respectvolle en verantwoordelijke houding in digitale omgevingen kan het aantal gevallen van opzettelijke of onopzettelijke schade verminderen. Dit is ook een preventieve maatregel in het kader van de richtlijn ter bestrijding van geweld tegen vrouwen en huiselijk geweld.

Kinderen en jongeren, met inbegrip van kinderen en jongeren met speciale behoeften, met een handicap of in kwetsbare situaties, moeten actief worden betrokken bij het ontwerp en de uitvoering van bewustmakingsactiviteiten die hen mondiger maken, inclusief en toegankelijk zijn en de stilte rond cyberpesten doorbreken.

De Commissie zal op EU-niveau een reeks preventie- en bewustmakingsinstrumenten beschikbaar stellen, die zijn ontwikkeld in samenwerking met kinderen en jongeren, ouders, opvoeders, professionals op het gebied van geestelijke gezondheid, de lidstaten en maatschappelijke organisaties.

In het kader van het actieplan voor digitaal onderwijs (2021-2027) zal de Commissie haar [richtsnoeren voor leerkrachten en onderwijsactoren inzake het aanpakken van desinformatie en het bevorderen van digitale geletterdheid](#) via onderwijs en opleiding actualiseren. Daarnaast zullen, zoals aangekondigd in de [mededeling over het Europees schild voor de democratie](#), de ontwikkelingen op het gebied van AI en sociale media bij die actualisering worden meegenomen en zal die ook lesmateriaal en activiteiten over cyberpesten omvatten, met aandacht voor inclusie en diversiteit. De Europese Commissie zal ook een competentiekader voor EU-burgerschap ontwikkelen, evenals richtsnoeren om de burgerschapsvorming op scholen te verbeteren.

Bovendien zullen digitale geletterdheid, de preventie van cyberpesten en digitaal welzijn aandachtspunten zijn in de routekaart voor de toekomst van digitaal onderwijs en digitale vaardigheden voor 2030. De routekaart 2030 moet ervoor zorgen dat jongeren worden ondersteund bij het opbouwen van gezonde onlinegewoonten en worden geïnformeerd over het verantwoord gebruik van digitale apparaten, zowel binnen als buiten de klas.

Deze werkzaamheden op het gebied van digitale geletterdheid bouwen voort op initiatieven die de Commissie uitvoert via het Erasmus+-programma en het Europees Solidariteitskorps, het Europees platform voor schoolonderwijs (ESEP) en eTwinning. In het kader van het ESEP zal de Commissie een betere en permanente zichtbaarheid mogelijk maken van al het materiaal dat nuttig is voor scholen op het gebied van pesten, met inbegrip van cyberpesten. Vanaf de Erasmus+-oproep 2026 zullen de prioriteiten op het gebied van welzijn op school worden versterkt om projecten ter bestrijding van pesten en cyberpesten beter te ondersteunen, te monitoren en aan te moedigen.

Het EU-netwerk voor de preventie van seksueel misbruik van kinderen zal bijdragen tot de bevordering van de voorlichting en het bewustzijn van kinderen met betrekking tot seksueel misbruik van kinderen, onder meer door initiatieven te onderzoeken om te helpen voorkomen dat gevallen van cyberpesten escaleren tot crimineel gedrag (bv. de verspreiding van materiaal over seksueel misbruik van kinderen). Daarnaast zal de preventie van cyberpesten in aanmerking worden genomen in het komende EU-actieplan voor de bescherming van kinderen tegen criminaliteit. Het actieplan zal tot doel hebben een samenhangend en alomvattend antwoord te bieden op de verschillende risico's waarmee kinderen worden geconfronteerd in verband met criminaliteit, zowel online als offline.

Het platform “Better Internet for Kids” (BIK) en zijn netwerk van SIC's bieden ondersteunende instrumenten voor kinderen, ouders, opvoeders en professionals op EU- (BIK) en nationaal

(SIC's) niveau. Deze middelen zullen verder worden uitgebreid om de capaciteit te versterken, meer belanghebbenden te bereiken en te reageren op nieuwe problemen op het gebied van cyberpesten.

Aangezien scholen een sleutelrol spelen bij het voorkomen van cyberpesten, zullen bewustmakingsactiviteiten worden uitgevoerd met de steun van de SIC's en het BIK-platform, te beginnen met de jaarlijkse “back-to-school” -campagne aan het begin van elk nieuw schooljaar, om leerkrachten en kinderen uit te rusten met opleidingsmateriaal, instrumenten en informatie over hoe cyberpesten kan worden voorkomen en gemeld.

Via Europese platforms zullen middelen en opleidingen over cyberpesten voor niet-formeel en informeel onderwijs beschikbaar zijn. Het gaat onder meer om de Europese Jongerensite, het centrale loket voor bewustmaking en bevordering van kansen voor jongeren, en het Europees platform voor schoolonderwijs, het ontmoetingspunt voor de schoolonderwijsgemeenschap en de Leerhoek, waar leerkrachten en onderwijsprofessionals kunnen beschikken over middelen en toolkits voor EU-initiatieven.

Evenementen zoals de Europese Jeugdweek en de Europese Week van de Sport vergemakkelijken de betrokkenheid bij uiteenlopende onderwerpen, waaronder de bestrijding van cyberpesten. De Groep open coördinatiemethode voor de bestrijding van haatzaaiende uitlatingen in de sport, die is opgericht in het kader van het EU-werkplan voor sport, werkt aan aanbevelingen voor de lidstaten en belanghebbenden voor de sportomgeving in het algemeen, ook online. Het verslag wordt eind 2026 verwacht en zal aanbevelingen bevatten om cyberpesten tegen te gaan.

De Commissie zal:

- 6. cyberpesten aanpakken bij de actualisering van de richtsnoeren voor leerkrachten en onderwijsactoren inzake het aanpakken van desinformatie en het bevorderen van digitale geletterdheid via onderwijs en opleiding — uiterlijk in het tweede kwartaal van 2026;**
- 7. de burgerschapsvorming op scholen versterken door middel van een competentiekader voor EU-burgerschap en richtsnoeren — in 2027;**
- 8. digitale competentie, preventie van cyberpesten en digitaal welzijn versterken door middel van de routekaart voor de toekomst van digitaal onderwijs en digitale vaardigheden 2030 — uiterlijk in het derde kwartaal van 2026;**
- 9. bijdragen aan de preventie van cyberpesten in het komende EU-actieplan voor de bescherming van kinderen tegen criminaliteit — uiterlijk in het derde kwartaal van 2026;**
- 10. de middelen en opleidingen op het gebied van cyberpesten uitbreiden voor scholen en voor niet-formeel en informeel onderwijs, toegankelijk voor personen met een handicap, via het BIK-platform, de SIC's, de Europese Jongerensite en het Europees platform voor schoolonderwijs — vanaf het tweede kwartaal van 2026;**

11. de Groep open coördinatiemethode voor de bestrijding van haatzaaiende uitlatingen in de sport ondersteunen bij haar werkzaamheden met betrekking tot **aanbevelingen voor de bestrijding van cyberpesten in de sportomgeving** — verslag verwacht uiterlijk in **het vierde kwartaal van 2026**.

De lidstaten wordt verzocht:

3. de preventie en vroegtijdige opsporing van cyberpesten te versterken met **duidelijke richtsnoeren en opleiding voor belanghebbenden** zoals opvoeders, verzorgers en professionals die met kinderen werken op verschillende gebieden (bv. gezondheid, sport, justitie, rechtshandhaving);
4. **de participatie van kinderen te versterken** in de beleidsvorming en de uitvoering van maatregelen voor kindervelzijn.

3.3 Pijler III: melding en uitgebreide ondersteuning

Slachtoffers van cyberpesten moeten over duidelijke, betrouwbare en toegankelijke kanalen beschikken om misbruik te melden en hulp te krijgen, onder meer voor cyberpesten via particuliere berichten. Om doeltreffend te zijn, moeten de ondersteunende inspanningen verder gaan dan het helpen van alleen slachtoffers van cyberpesten zodat ook omstanders, ouders, ouders, verzorgers, opvoeders en de bredere schoolgemeenschap worden bereikt.

De Commissie zal coherente, EU-brede meldingsmogelijkheden en slachtofferhulp bevorderen. Meldingen moeten snel leiden tot multidisciplinaire ondersteuning, zowel online als offline. Alle relevante autoriteiten op alle niveaus, particuliere actoren, maatschappelijke organisaties, ouders, verzorgers, en de kinderen en jongeren zelf moeten daarbij worden betrokken.

Voortbouwend op de inzichten die via verschillende gerichte raadplegingen zijn verzameld, **zal de Commissie de uitrol van een app voor onlineveiligheid in alle lidstaten ondersteunen**, op basis van succesvolle bestaande nationale praktijkmodellen, zoals de Franse *3018 app*. De app zal een veilig, gebruiksvriendelijk en vertrouwelijk instrument bieden waarmee kinderen en jongeren:

- i. **cyberpesten gemakkelijk kunnen melden** via een **hulplijn**;
- ii. **bewijsmateriaal veilig kunnen opslaan en doorgeven** in overeenstemming met de nationale rechtskaders, en
- iii. **bijstand op maat kunnen krijgen door middel van gecoördineerde doorverwijzingen** naar bijvoorbeeld rechtshandavings-, onderwijs- en kinderschermingsdiensten.

De Commissie zal de lidstaten waar nodig en relevant ondersteunen om:

- i. **de app aan te passen aan de nationale context en behoeften** (bv. vertaling, branding, verbinding met relevante nationale ondersteuningsdiensten en platforms

voor melding), functies aan te bieden zoals veilige melding, bewaring van bewijsmateriaal in overeenstemming met het nationale recht en gegarandeerde vertrouwelijkheid;

- ii. **te zorgen voor interoperabiliteit** met bestaande infrastructuur en ondersteuningssystemen, en
- iii. **de bevordering te ondersteunen** van het gebruik van de app door de lidstaten, gebruikers en onlineplatforms.

Onlineplatforms blijven verantwoordelijk voor het opzetten van doeltreffende meldingsmechanismen. Dit kan neerkomen op een van de maatregelen die zijn genomen om de naleving van de verplichtingen van de digitaaldienstenverordening inzake de bescherming van minderjarigen te waarborgen. Als aanvulling op deze inspanningen zal de app ter beschikking worden gesteld van onlineplatforms om te worden geïntegreerd in hun meldings- en gebruikersondersteuningsinstrumenten, onder meer via applicatieprogramma-interfaces (API's), waardoor het melden en het reageren efficiënt en effectief worden gemaakt.

Het succes van de app hangt af van de beschikbaarheid van ondersteuning en follow-up door de nationale autoriteiten. De lidstaten zullen een belangrijke rol spelen bij het waarborgen dat meldingen die via de app worden gedaan, offline gecoördineerde ondersteuning krijgen (bv. juridische, sociale, psychologische en educatieve ondersteuning) alsook bij het communiceren over de voordelen van de app. De app zal streven naar synergieën met beproefde meldingsmechanismen in de lidstaten voor het online melden van kinderpornografie en geweld tegen vrouwen, alsook met EU-, nationale en internationale hulplijnen, met name kinderpornografie (116 111) en meldpunten voor vermiste kinderen (116 000).

De Commissie zal in 2026 de volgende [EU-strategie inzake de rechten van slachtoffers](#) vaststellen om de EU-regels aan te vullen met niet-wetgevende maatregelen. De strategie zal structuren voor gerichte ondersteuning (bv. medisch onderzoek, emotionele en psychologische steun) en beschermingsdiensten voor minderjarige slachtoffers, waaronder die van onlinecriminaliteit, bevorderen. Deze structuren zullen ook gericht zijn op de slachtoffers van cyberpesten in de lidstaten waar dergelijke daden volgens het nationale recht strafbaar zijn.

Op grond van de [algemene verordening gegevensbescherming](#) is het recht op wissing van persoonsgegevens met name relevant wanneer een betrokkene als kind toestemming heeft gegeven en zich mogelijk niet volledig bewust was van de risico's, onder meer in de context van cyberpesten. De Commissie zal de gegevensbeschermingsautoriteiten blijven ondersteunen bij de ontwikkeling van op kinderen gerichte instrumenten om socialemediagegevens te beschermen, gegevens- of accountdiefstal te voorkomen en de uitoefening van hun rechten mogelijk te maken.

De Commissie zal:

- 12. de uitrol in alle lidstaten ondersteunen van een toegankelijke app voor onlineveiligheid** voor gemakkelijke melding van cyberpesten, aangepast aan de nationale context, in synergie met bestaande meldingsmechanismen, zoals

hulplijnen en meldpunten, ter bevordering van multidisciplinaire ondersteuning, zowel online als offline — **vanaf het derde kwartaal van 2026;**

13. kindslachtoffers en onlineslachtofferschap, waaronder cyberpesten, aanpakken in de volgende **EU-strategie inzake de rechten van slachtoffers — 2026.**

De lidstaten wordt verzocht:

5. hun nationale context te analyseren met de bedoeling een **nationale app voor onlineveiligheid** beschikbaar te stellen met ondersteuning op maat, en, voortbouwend op succesvolle bestaande nationale praktijkmodellen, **een dergelijk model aan te passen aan de nationale omgeving**, met inbegrip van bijvoorbeeld vertaling, branding, verbinding met relevante nationale ondersteuningsdiensten en meldingsplatforms, waarbij kernkenmerken zoals veilige melding, bewaring van bewijsmateriaal in overeenstemming met het nationale recht en vertrouwelijkheid worden gewaarborgd;
6. ervoor te zorgen dat meldingen via de nationale app voor onlineveiligheid worden geïntegreerd in **een holistisch en goed functionerend ecosysteem voor casemanagement en ondersteuning**, met inbegrip van gecoördineerde ondersteuning offline (bv. juridische, politieke, sociale, psychologische en educatieve ondersteunende diensten);
7. **de nationale app voor onlineveiligheid ter beschikking te stellen van onlineplatforms om te worden geïntegreerd in hun meldings- en gebruikersondersteuningsinstrumenten**, onder meer via applicatieprogramma-interfaces (API's), waardoor het melden en het reageren efficiënt en effectief worden gemaakt;
8. **de brede toepassing en het brede gebruik van de nationale veiligheidsapp door alle relevante belanghebbenden te bevorderen;**
9. **de door de gegevensbeschermingsautoriteiten in hun nationale taal ontwikkelde instrumenten te bevorderen** waarmee kinderen zichzelf kunnen beschermen tegen onlineriesico's, zoals cyberpesten, gegevens- of accountdiefstal, pogingen tot oplichting en seksuele chantage.

4. Internationale toenadering en samenwerking tussen meerdere belanghebbenden

De EU streeft ernaar het welzijn en de rechten van kinderen binnen haar grenzen te beschermen, maar ook aanzienlijk bij te dragen tot de bevordering van een veiligere, inclusievere digitale omgeving wereldwijd. De Dag voor een Veiliger Internet is nu een wereldwijde campagne die belanghebbenden oproept gezamenlijk actie te ondernemen om van het internet een veiligere en betere plek voor iedereen te maken, met name voor kinderen en jongeren, waarbij de aandacht wordt gevestigd op belangrijke online-uitdagingen en nieuwe zorgen en trends.

Het beschermen en mondiger maken van minderjarigen online is een wereldwijde prioriteit. Dit komt tot uiting in de [internationale digitale strategie van de EU](#). Het door de EU medegefinancierde netwerk van meldpunten in de lidstaten om de verspreiding van onlinekinderpornografie aan te pakken, maakt deel uit van het [Inhope-netwerk](#), dat momenteel wereldwijd 57 meldpunten telt.

De Commissie zal blijven samenwerken met gelijkgestemde regelgevende instanties op het gebied van onlineveiligheid, met inbegrip van het voorkomen en aanpakken van cyberpesten, in het kader van administratieve regelingen (momenteel bijvoorbeeld met Ofcom in het VK en de eSafety Commissioner in Australië) en digitale partnerschappen (bijvoorbeeld met Canada, Singapore en India).

De EU zal samenwerking tegen cyberpesten in internationale fora bevorderen, in overeenstemming met het [mondiaal digitaal pact](#). VN-organisaties hebben richtsnoeren en instrumenten ontwikkeld die als goede praktijken en benchmarks kunnen worden gebruikt, onder meer van Unicef (website en opensource-API's), de Internationale Telecommunicatie-unie (richtsnoeren inzake onlinebescherming van kinderen) en de speciale vertegenwoordiger van de secretaris-generaal van de VN inzake geweld tegen kinderen. De EU steunt de contacten van de Unesco met regelgevende instanties om de Unesco-richtsnoeren inzake het beheer van onlineplatforms uit te voeren.

De EU financiert specifieke bewustmakings- en beschermingsprogramma's voor kinderen in niet-EU-landen, met name kandidaat-lidstaten en buurlanden, zowel online als offline, via het instrument NDICI – “Europa in de wereld”. De EU steunt ook de aanpassing aan de EU-regels in het kader van het toetredingsproces voor kandidaat-lidstaten en potentiële kandidaat-lidstaten, en bevordert de onlineveiligheid van kinderen en jongeren in buurlanden door kennis en beste praktijken uit te wisselen via het programma Safer Internet Centre + (SIC +).

5. Volgende stappen

De Commissie zal toezicht houden op de uitvoering van het actieplan in alle drie de pijlers, in nauwe samenwerking met de lidstaten, SIC's en andere belanghebbenden. Vooruitgang, problemen en goede praktijken zullen worden gevolgd aan de hand van bestaande instrumenten zoals de jaarlijkse BIK Policy Map, verslagen van de SIC's en regelmatige uitwisselingen via deskundigenfora, waarbij wordt gezorgd voor transparante en participatieve monitoring.

De Commissie zal met de lidstaten samenwerken om monitoringkaders op te nemen in nationale strategieën of beleidsmaatregelen inzake cyberpesten, waarbij de uitvoering, toegankelijkheid, inclusiviteit en aanpasbaarheid aan veranderende digitale contexten worden beoordeeld, met betrokkenheid van kinderen en jongeren. De bevindingen zullen op EU-niveau worden gedeeld om wederzijds leren en beleidsafstemming te ondersteunen, als input voor updates van initiatieven in het kader van BIK+ en de digitaaldienstenverordening.

De Commissie zal in 2029 de balans opmaken van dit actieplan, onder meer door middel van overleg met kinderen en jongeren.

6. Conclusies

“We willen een veilige onlineruimte voor kinderen, jongeren en de komende generatie, maar die hebben we nog niet. We hebben een aantal problemen. En die problemen gelden niet alleen voor deze generatie. De EU moet ons dus helpen ons die veilige onlineruimten te geven. Je moet ergens beginnen. We moeten dat nu doen. Voor de toekomst.”

Een citaat van kinderen die lid zijn van de EU-site voor jongereninspraak.

Kinderen en jongeren richten zich tot ons met een oproep tot hulp om onlineruimten veilig te maken, voor hen, hun leeftijdsgenoten en toekomstige generaties. We moeten de uitdaging in onze hele Unie aangaan, omdat de bescherming en het mondiger maken van onze kinderen en jongeren niet mag afhangen van een postcode.

Voortbouwend op een reeds robuust EU-instrumentarium van juridische en beleidsmaatregelen tegen onlineschade en op bijdragen van een breed scala aan belanghebbenden, zal dit actieplan een veilige, inclusieve digitale omgeving voor kinderen en jongeren in Europa helpen tot stand brengen die hen ook mondiger maakt. Het zal een aanvulling vormen op en inspiratie bieden voor lopende EU-initiatieven op het gebied van veiliger internet, platformverantwoordelijkheid, digitale vaardigheden en onderwijs, het mondiger maken van kinderen en jongeren, gegevensverzameling en internationale samenwerking.

De Commissie verzoekt het Europees Parlement en de Raad om dit actieplan goed te keuren en bij de uitvoering ervan samen te werken. De Commissie verzoekt het Comité van de Regio's en het Europees Economisch en Sociaal Comité om hierover de dialoog met lokale en regionale overheden, economische en sociale spelers en het maatschappelijk middenveld te bevorderen.

BIJLAGE: Belangrijkste acties en tijdlijn

Pijler I: een gecoördineerde EU-aanpak van bescherming

De Commissie zal:	
bij de herziening van de richtsnoeren inzake de onlinebescherming van minderjarigen in het kader van de digitaaldienstenverordening meer aandacht besteden aan de bestrijding van cyberpesten;	2026
richtsnoeren inzake betrouwbare flaggers in het kader van de digitaaldienstenverordening vaststellen om de rol ervan bij de bestrijding van illegale inhoud, met inbegrip van inhoud waarmee wordt gecyberpest, te helpen verduidelijken;	uiterlijk in het tweede kwartaal van 2026
manieren beoordelen om cyberpesten op videoplatforms aan te pakken in het kader van de lopende evaluatie van de richtlijn audiovisuele mediadiensten en de herziening ervan;	uiterlijk in het derde kwartaal van 2026
de doeltreffende uitvoering van de bepalingen van de AI-verordening inzake verboden AI-praktijken ondersteunen, ook wanneer deze worden gebruikt voor cyberpesten;	vanaf het derde kwartaal van 2026
de doeltreffende uitvoering van de transparantieplichtingen van de AI-verordening in verband met het markeren en labelen van door AI gegenereerde inhoud vergemakkelijken, ook wanneer het om cyberpesten gaat.	vanaf het derde kwartaal van 2026

De lidstaten wordt verzocht:	
uitgebreide nationale plannen ter bestrijding van pesten, met inbegrip van cyberpesten op te stellen, met name met de steun van het EU-netwerk voor kinderrechten;	
consistente, vergelijkbare gegevens over cyberpesten te verzamelen , gefaciliteerd door het netwerk van centra voor een veiliger internet en het platform “Better Internet for Kids”.	

Pijler II: preventie en bewustmaking

De Commissie zal:	
cyberpesten aanpakken bij de actualisering van de richtsnoeren voor leerkrachten en onderwijsactoren inzake het aanpakken van desinformatie en het bevorderen van digitale geletterdheid ;	uiterlijk in het tweede kwartaal van 2026
de burgerschapsvorming op scholen versterken door middel van een competentiekader voor EU-burgerschap en richtsnoeren;	2027

digitale competentie, preventie van cyberpesten en digitaal welzijn versterken door middel van de routekaart voor de toekomst van digitaal onderwijs en digitale vaardigheden 2030 ;	uiterlijk in het derde kwartaal van 2026
bijdragen aan de preventie van cyberpesten in het komende EU-actieplan voor de bescherming van kinderen tegen criminaliteit ;	uiterlijk in het derde kwartaal van 2026
de middelen en opleidingen op het gebied van cyberpesten uitbreiden voor scholen en voor niet-formeel en informeel onderwijs, toegankelijk voor personen met een handicap, via het BIK-platform, de SIC's, de Europese Jongerensite;	vanaf het tweede kwartaal van 2026
de Groep open coördinatiemethode voor de bestrijding van haatzaaiende uitlatingen in de sport ondersteunen bij haar werkzaamheden met betrekking tot aanbevelingen voor de bestrijding van cyberpesten in de sportomgeving .	uiterlijk in het vierde kwartaal van 2026

De lidstaten wordt verzocht:
de preventie en vroegtijdige opsporing van cyberpesten te versterken met richtsnoeren en opleiding voor belanghebbenden zoals opvoeders, verzorgers en professionals die met kinderen werken op verschillende gebieden;
de participatie van kinderen te versterken in de beleidsvorming en de uitvoering van maatregelen voor kinderwelzijn.

Pijler III: melding en uitgebreide ondersteuning

<u>De Commissie zal:</u>	
de uitrol in alle lidstaten ondersteunen van een toegankelijke app voor onlineveiligheid ;	vanaf het derde kwartaal van 2026
kindslachtoffers en onlineslachtofferschap, waaronder cyberpesten, aanpakken in de volgende EU-strategie inzake de rechten van slachtoffers .	2026

<u>De lidstaten wordt verzocht:</u>

hun nationale context te analyseren met de bedoeling **een nationale app voor onlineveiligheid** beschikbaar te stellen en, voortbouwend op succesvolle bestaande nationale praktijkmodellen, een dergelijk model aan te passen aan de nationale omgeving;

ervoor te zorgen dat meldingen via de nationale app voor onlineveiligheid worden geïntegreerd in **een holistisch en goed functionerend ecosysteem voor casemanagement**;

de nationale app voor onlineveiligheid ter beschikking te stellen van onlineplatforms om te worden geïntegreerd in hun meldings- en gebruikersondersteuningsinstrumenten;

de nationale app voor onlineveiligheid te promoten bij relevante belanghebbenden;

de door gegevensbeschermingsautoriteiten in hun nationale taal ontwikkelde instrumenten te bevorderen waarmee kinderen zichzelf kunnen beschermen tegen onlineriesico's, zoals cyberpesten.