Ministerie van Justitie en Veiligheid

> Retouradres Postbus 20301 2500 EH Den Haag

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Onze referentie
8235575

Uw referentie
2026Z21771

Datum	23 november 2026
Betreft	Antwoorden Kamervragen over deepfake pornografie van vrouwelijke politici

In antwoord op uw brief van 9 oktober 2026 deel ik u mee, mede namens de minister van Binnenlandse Zaken, dat de schriftelijke vragen van de leden Becker, Rajkowski (beiden VVD), Beckerman, Dobbe (beiden SP), Coenradie (JA21), Van Dijk (CDA), Kostic, Ouwehand en Teunissen (allen PvdD), Kröger, Westerveld (beiden PRO), Van der Plas, Wiersma (beiden BBB) en Podt, Synhaeve (beiden D66), inzake deepfake pornografie van vrouwelijke politici worden beantwoord zoals aangegeven in de bijlage bij deze brief.

De Minister van Justitie en Veiligheid,

D.M. van Weel

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum
23 november 2026

Onze referentie
8235575

Vragen van de leden Kröger (PRO), Van der Plas (BBB), Inge van Dijk (CDA), Wiersma (BBB), Westerveld (PRO), Kostić (PvdD), Synhaeve (D66), Becker (VVD), Beckerman, Dobbe (beiden SP), Ouwehand (PvdD), Rajkowski (VVD), Teunissen (PvdD), Coenradie (JA21) en Podt (D66) aan de ministers van Binnenlandse Zaken, van Justitie en Veiligheid en van Buitenlandse Zaken over deepfake pornografie van vrouwelijke politici (ingezonden 9 oktober 2026, 2026Z21771)

Vraag 1
Bent u bekend met het rapport 'Who Gets Deepfaked? Measuring the exposure of European parliamentarians in deepfake pornography', het rapport 'Targeted and Ignored. Sexualised Deepfakes of Women MEPs and the Failure of Platform Responses', het artikel 'Unicum: vrouwelijke Kamerleden slaan handen ineen in strijd tegen gruwelijk online seksueel misbruik' en het statement 'AI kent geen grenzen. Wij wel.' dat 15 vrouwelijke Tweede Kamerleden van acht verschillende politieke partijen hebben uitgestuurd? [1, 2, 3]

Antwoord op vraag 1
Ja.

Vraag 2
Wat zegt het volgens u dat vrouwelijke parlementariërs in Europa 33 keer vaker slachtoffer zijn van deepfake pornografie dan mannen en dat zeker een kwart van de vrouwelijke parlementariërs in Nederland hier slachtoffer van is?

Antwoord op vraag 2
Het zijn zeer zorgelijke cijfers. Deepfakes van vrouwelijke parlementariërs zijn een vorm van seksueel geweld die de politiek voor vrouwen tot een onveilige omgeving maakt. Ook bij andere vormen van geweld, agressie en intimidatie zien we dat vrouwen onevenredig worden getroffen. Dit bedreigt het functioneren van onze democratie waarin het cruciaal is dat iedereen op basis van gelijkwaardigheid mee moet kunnen doen.

[1] Agora, september 2026, 'Who Gets Deepfaked? Measuring the exposure of European parliamentarians in deepfake pornography.', (Who Gets Deepfaked? Measuring the exposure of European parliamentarians in deepfake pornography. - Agora Digitale Transformation)
[2] Agora, oktober 2026, 'Targeted and Ignored. Sexualised Deepfakes of Women MEPs and the Failure of Platform Responses.', (Targeted and Ignored. Sexualised Deepfakes of Women MEPs and the Failure of Platform Responses. - Agora Digitale Transformation)
[3] Algemeen Dagblad, 24 september 2026, 'Unicum: vrouwelijke Kamerleden slaan handen ineen in strijd tegen gruwelijk online seksueel misbruik', (Unicum: vrouwelijke Kamerleden slaan handen ineen in strijd tegen gruwelijk online seksueel misbruik | Nieuws | AD.nl)

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum
23 november 2026

Onze referentie
8235575

Vraag 3
Bent u het ermee eens dat dergelijke cijfers schrikbarend zijn? Kunt u zich voorstellen dat dit een chilling effect heeft op vrouwen die politiek actief willen worden? Zo ja, wat gaat u eraan doen? Zo nee, waarom niet?

Antwoord op vraag 3
Het zijn inderdaad zeer zorgelijke cijfers. Het is evident dat agressie, bedreiging en intimidatie het werkplezier van vrouwelijke politici aantasten en voor een gevoel van onveiligheid zorgen. Ook de intentie van vrouwen om in het ambt te blijven of op te gaan voor herverkiezing wordt hierdoor negatief beïnvloed. Het is goed voorstelbaar dat het vrouwen ook meer afschrikt om politiek actief te worden.

Het kabinet werkt op diverse manieren aan het verbeteren van de positie van vrouwen in het decentraal openbaar bestuur. Zo wordt bijvoorbeeld het mentornetwerk van Stem op een Vrouw gefinancierd om aspirant-politica's te ondersteunen in het waarmaken van hun ambitie. Mentornetwerken kunnen belangrijk zijn in het bieden van de juiste ondersteuning voor vrouwelijke politici.

Om decentrale politieke ambtsdragers te ondersteunen bij het omgaan met agressie, bedreiging en intimidatie zijn vanuit het programma Weerbaar Bestuur diverse voorzieningen beschikbaar. Daarnaast zijn de Eenduidige Landelijke Afspraken (ELA) dit jaar herzien om strafrechtelijke opvolging te verbeteren. Deze maand wordt de Monitor Integriteit en Veiligheid 2026 met beleidsreactie aan uw Kamer aangeboden. Aan de hand van de resultaten van deze monitor zal het kabinet nagaan welke aanvullende maatregelen voor vrouwen en andere ondervertegenwoordigde groepen in het openbaar bestuur effectief zijn en hoe deze groepen beter bereikt kunnen worden.

Vraag 4
Deelt u de opvatting dat deepfake pornografie een groot maatschappelijk probleem is dat heel veel vrouwen in Nederland treft, waaronder ook vrouwen die niet het platform hebben van vrouwelijke Tweede Kamerleden en vrouwelijke BN'ers? Wat doet het volgens u met de positie van de vrouw in onze maatschappij dat deepfake pornografie zo gemakkelijk te genereren is, dat het eenmaal gemaakt niet tot nauwelijks van het internet verdwijnt en dat zeer grote aantallen vrouwen slachtoffer zijn van dit soort video's?

Antwoord op vraag 4
Ik deel de opvatting dat seksuele deepfakes (zonder toestemming van degene van wie de deepfake wordt gemaakt) een maatschappelijk probleem zijn. Ik zie ook dat het veel mensen in Nederland treft, waarvan het overgrote deel vrouwen. Het is zeer kwalijk dat dit soort beelden zo eenvoudig te genereren en te verspreiden zijn, en dat het zo moeilijk is om de beelden die eenmaal online staan weer te verwijderen. Dit maakt niet alleen het bestrijden hiervan complex, maar maakt ook de impact op slachtoffers (potentieel)

groot. Het gemak waarmee dergelijke beelden te maken zijn, en de mogelijkheid om dergelijke beelden in relatieve anonimiteit te maken en verspreiden maakt het voor daders eenvoudiger om te weinig of niet bij deze impact stil te staan. Daarmee ben ik van mening dat het genereren van deepfake pornografie de positie van de vrouw in onze maatschappij schaadt.

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum
23 november 2026

Onze referentie
8235575

Vraag 5
Deelt u de mening van de onderzoekers van de twee rapporten dat naast goede wetgeving om deepfakepornografie te verbieden er ook sprak moet zijn van strikte handhaving? Zo ja, hoe gaat u daarvoor zorgen? Zo nee, waarom niet?

Antwoord op vraag 5
Ik deel de mening dat wetgeving ook handhaving behoeft om de wet kracht bij te zetten. Dat valt in dit kader uiteen in twee vormen van handhaving: de strafrechtelijke handhaving door politie en het Openbaar Ministerie, en bestuursrechtelijke handhaving door de Autoriteit Persoonsgegevens.

Het vervaardigen, verspreiden en bezitten van beeldmateriaal van seksueel kindermisbruik en misbruik van seksueel beeldmateriaal zijn seksuele misdrijven die een grote impact hebben op slachtoffers en hun omgeving. De inspanningen van politie en OM zijn erop gericht om degenen die zich hieraan schuldig maken op te sporen en te vervolgen. De realiteit is dat rechtshandhaving in het digitale domein uitdagingen met zich mee brengt en dat politie en OM bij de aanpak van (online) seksuele misdrijven keuzes moeten maken vanwege de beperkte capaciteit waarmee zij te maken hebben. Conform de ambities uit het coalitieakkoord geeft dit kabinet een impuls aan de operationele slagkracht van de politie voor de aanpak van online seksuele misdrijven. Vanuit de envelop voor nationale veiligheid in het coalitieakkoord is een bedrag dat oploopt naar structureel 462 miljoen euro vanaf 2030 bestemd voor de politie. Daarvan is in de ontwerpbegroting vanaf 2027 een bedrag oplopend naar structureel 15 miljoen euro vanaf 2030 gereserveerd voor de aanpak van online seksuele misdrijven. Daarbij wordt steeds voorrang gegeven aan feiten met minderjarige slachtoffers en zaken met een grote impact, bijvoorbeeld vanwege het aantal slachtoffers.

In de AI-verordening is een verbod opgenomen op het in de handel brengen, het in gebruik stellen, of het gebruiken van ieder AI-systeem dat materiaal van seksueel kindermisbruik of realistische beelden van intieme delen of van personen die expliciete seksuele gedragingen verrichten zonder toestemming genereert of bewerkt. Het Europese AI Office, als onderdeel van de Europese Commissie, is onder de verordening exclusief bevoegd om toezicht te houden en te handhaven in twee gevallen: ten eerste wanneer een dergelijk AI-systeem gebaseerd is op AI modellen voor algemene doeleinden waarbij zowel het model als het systeem zijn ontwikkeld door dezelfde aanbieder en ten tweede wanneer deze systemen een overeenkomstig Verordening (EU) 2022/2065 aangewezen zeer groot onlineplatform of zeer grote onlinezoekmachine

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum
23 november 2026

Onze referentie
8235575

vormen of daarin zijn geïntegreerd. Het Europese AI Office zal voor deze systemen direct kunnen handhaven vanaf december dit jaar. In andere gevallen kan nationaal toezicht worden gehouden. De beoogd markttoezichtautoriteiten dienen via een uitvoeringswet te worden aangewezen en krijgen daarmee handhavingsbevoegdheden. De conceptuitvoeringswet AI-verordening is in consultatie geweest. Momenteel worden alle reacties die op de conceptuitvoeringswet zijn binnengekomen verwerkt en wordt de wet klaar gemaakt ter aanbieding voor advisering door de Raad van State.

In Nederland is de Autoriteit Persoonsgegevens (AP) de beoogd markttoezichtautoriteit voor verboden AI-praktijken. De AP bereidt zich op dit moment voor op de werkzaamheden die volgen uit de UAIV. Op dit moment heeft de AP mogelijkheden om te handhaven op basis van haar bestaande bevoegdheden onder de Algemene Verordening Gegevensbescherming (AVG) indien persoonsgegevens zijn verwerkt zonder verwerkingsgrondslag, zoals bij onwenselijke deepfakes zonder toestemming van de betrokkene. Als uit onderzoek op basis van de AVG blijkt dat er een overtreding is, heeft de AP maatregelen en sancties ter beschikking om een boete, een last onder dwangsom, een verwerkingsverbod of een berisping op te leggen. Het is aan de AP, als onafhankelijke toezichterhouder, om te beoordelen of zij in individuele gevallen een (rechtmatigheids)onderzoek doet en handhavend optreedt.

Vraag 6
Kunt u ook per voorstel apart ingaan op de beleidsvoorstellen die de onderzoekers in hun twee rapporten doen om deepfake pornografie te bestrijden? Kunt u tevens aangeven welk van deze voorstellen nationaal kunnen worden opgepakt en voor welke van deze voorstellen u zich in Europees verband wilt inzetten?

Antwoord op vraag 6
In de rapporten wordt een aantal beleidsvoorstellen gedaan. Deze heb ik hieronder vertaald en opgesomd. Ik ga per punt in op de verschillende aanbevelingen, maar omdat enkelen een thematisch cluster zijn, verwijs ik in beantwoording ook naar wat ik elders reeds beschrijf.

1. *Verantwoording op productniveau, ongeacht de omvang van de aanbieder. Openstaande vragen zijn onder meer de handhavingscapaciteit ten aanzien van kleine of open-sourceplatforms, het omgaan met aanbieders en gebruikers van dergelijke platforms die buiten de EU gevestigd zijn, en het misbruik van open-weight modellen op machinelearning-marktplaatsen zoals HuggingFace en CivitAI om lokale, offline deepfake AIG-NCII-productie te faciliteren. Gelijkenissen van personen zijn met open-weight modellen op dergelijke platforms misbruikt. Wij stellen dat dit misbruik aantoont dat de bestaande veiligheidsmaatregelen onredelijk en ontoereikend zijn.*

Het nieuwe verbod in de AI-verordening is van toepassing op het in handel brengen, het in gebruik stellen en gebruiken van alle AI-systemen waar vaak aan gerefereerd wordt als ‘nudifier apps’. Het maakt daarbij niet uit via welk kanaal deze systemen worden aangeboden of bereikbaar zijn, inclusief via zogeheten gateway-sites.

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum
23 november 2026

Onze referentie
8235575

Platformaanbieders, ook indien zij als doorgeefluik fungeren, behoren geen verboden functionaliteit aan te bieden of te faciliteren. Het verbod onder artikel 5 van de AI-verordening ondervangt ook open-weight modellen. De reden hiervoor is dat het voor de classificatie niet uitmaakt op basis van welke modellen deze systemen ontwikkeld zijn. Het verbod geldt voor alle AI-systemen die zijn ontwikkeld voor de in dat artikel genoemde praktijken. Deze onderwerpen zijn geen onderdeel geweest van de onderhandelingsgesprekken over de Omnibus.

2. *Behandel gateways als "deployers" (gebruiksverantwoordelijke). Wij stellen dat gateways die de persoonlijke gegevens en niet-naaktportretten van gekozen politici vermelden en er direct naast linken naar een verboden nudifier-app, geen legitiem doel dienen anders dan het bevorderen van de creatie van AIG-NCII, en daarom als deployers moeten worden aangepakt in overeenstemming met de Omnibus.*

Zie de reactie op voorstel 1.

3. *Productietools: vereis toestemmingsgebonden vangrails op model- en interfaceniveau, dus beperkingen op wat een systeem zal genereren, in plaats van uitsluitend te vertrouwen op post-hoc contentmoderatie door hostingplatforms. Daarnaast kan snelle adoptie van protocollen zoals C2PA, die tot doel hebben de herkomst van content te certificeren en misbruik te voorkomen, in zekere mate het misbruiken van publiek toegankelijke content van parlementariërs als grondstof temperen.*

Wat betreft het voorstel over op toestemming gebaseerde waarborgen op model-niveau, acht het kabinet het van belang om eerst de AI-verordening volledig in werking te laten treden en vervolgens effectief te handhaven voordat nieuwe regels worden geïntroduceerd. Het nieuwe verbod in de AI-verordening zorgt er al voor dat ontwikkelaars geen systemen op de markt mogen brengen waarbij materiaal van seksueel kindermisbruik of realistische beelden van intieme delen of van personen die expliciete seksuele gedragingen verrichten zonder toestemming worden gegenereerd of bewerkt.

4. *Beschouw tijdige de-indexering als een "redelijke veiligheidsmaatregel". Automatische en collectieve de-indexering na de inbeslagname van een AIG-NCII-domein kan bijvoorbeeld worden ondersteund door het AVG-recht om vergeten te worden (art. 17) of de DSA-plichten inzake risicodetectie (art. 34) en risicobeperking (art. 35), in plaats van individuele verwijderingsverzoeken. De vertraging tussen het verwijderen van content of een domein en de de-indexering is buiten onze audits van de blootstelling van nationale Kamerleden en Europarlementariërs goed onderzocht en zou in het geval van AIG-NCII eenvoudigweg geen maandenlang proces mogen zijn. Zoekaanbieders moeten er ook voor zorgen dat herplaatsingen van niet-consensueel materiaal automatisch worden verwijderd.*

Doorgaans zullen ontoegankelijk gemaakte domeinen vanzelf uit zoekresultaten verdwijnen of minder zichtbaar worden, afhankelijk van de gehanteerde

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum
23 november 2026

Onze referentie
8235575

indexeringstechniek van de zoekmachine. Ik ben bereid dit onderwerp te agenderen in de doorlopende dialoog met de internetsector om de moderatiepraktijk op dit gebied beter te begrijpen evenals de bijkomende uitdagingen.

5. *Hosting- en indexeringsinfrastructuur: vermeldingen in zoekindexen kunnen langer blijven bestaan dan de content waarnaar zij verwijzen. Het offline halen van een domein garandeert niet dat een genoemde persoon ophoudt in de zoekresultaten voor die content te verschijnen. De persistentie van indexen moet daarom als een afzonderlijk governance-doel worden behandeld, los van de daadwerkelijke hosting van content. Reputatieschade en psychologische effecten door herinneringen aan eerder misbruik houden vaak lang aan nadat het misbruik zelf is gestopt.*

Zie reactie op voorstel 4.

6. *Onderzoek de "redelijke veiligheidsmaatregelen" in de productieketen. Betaalverwerkers, appstores, content delivery networks (CDN's), webhosts, domeinregistrars en webprivacy-diensten zouden due-diligence-plichten moeten hebben ten aanzien van nudifier-apps, gatewaywebsites en dergelijke. Deze diensten profiteren van de creatie van AIG-NCII maar dragen geen verantwoordelijkheid voor hun rol bij de ondersteuning van de creatie en verspreiding* van dergelijke content.

Voor zover online aanbieders kwalificeren als tussenhandeldienst onder de Digital Services Act (DSA), is deze EU-verordening van toepassing. De DSA voorziet in de regulering van de verantwoordelijkheid en aansprakelijkheid van tussenhandeldiensten die een belangrijk deel van de genoemde keten vormen. Op grond van de DSA zijn hostingdiensten en online platformen gehouden om illegale online content te verwijderen zodra zij kennis hiervan krijgen. Daarnaast dienen online platformen maatregelen te nemen tegen misbruik van hun diensten, zoals via schorsing van afnemers die frequent kennelijk illegale online content verstrekken. Zeer grote online platformen en zoekmachines (zogenoemde VLOP's en VLOSE's) zijn aanvullend verplicht om de zogenoemde systeemrisico's van hun dienst te identificeren en te mitigeren, waar de verspreiding van illegale online content, eventuele negatieve effecten met betrekking tot gendergerelateerd geweld, en ernstige negatieve gevolgen voor het lichamelijke en geestelijke welzijn van de persoon onder vallen.

Het zou goed zijn als partijen zich proactief opstellen om misbruik van hun eigen infrastructuur te voorkomen. Een wettelijke verplichting van het Know Your Customer-beleid (KYC) zou een goede maatregel kunnen zijn om bad hosting tegen te gaan. Op dit moment zijn hostingdiensten niet verplicht om een KYC beleid te voeren, en kiezen sommige hostingdiensten er bewust voor om bijvoorbeeld de Gedragscode Abusebestrijding niet te ondertekenen. Om ervoor te zorgen dat het KYC-beleid door de gehele sector wordt toegepast, bestaat de wens om dit wettelijk te verplichten voor alle hostingdiensten. Het kabinet zet daarom in op een Europese aanpak en de versterking van de samenwerking op internationaal niveau. In dit kader wordt de samenwerking

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum
23 november 2026

Onze referentie
8235575

gezocht met lidstaten die de hostingproblematiek herkennen en wordt dit op Europees niveau aangekaart.

In Nederland houdt de Autoriteit Consument en Markt (ACM) primair toezicht op de naleving van de DSA voor hier gevestigde tussenhandeldiensten. Voor de zogenoemde VLOP's en VLOSE's ligt het toezicht primair bij de Europese Commissie. Zo kondigde bijvoorbeeld de Europese Commissie in januari 2026 aan te onderzoeken of X voldoet aan haar verplichtingen onder de DSA inzake het beheersen van risico's rond de verspreiding van illegale inhoud in de EU, waaronder gemanipuleerde seksueel expliciete afbeeldingen. In dit kader zie ik dit beleidsvoorstel als ondersteuning van het huidige beleid en de lopende handhavingsinspanningen.

7. *Verleg de last weg van slachtoffers. Dat betekent dat toezichthouders uit eigen beweging optreden, collectieve rechtsbescherming wordt ingezet (AVG art. 80, DSA art. 86) en dat preventieve handhavingsacties worden gemeten in plaats van het tellen van post-hoc verwijderingen.*

Slachtoffers zouden niet de last moeten dragen van het tegengaan van seksuele deepfakes. Zoals ik hierboven schets: het zou goed zijn als partijen zich proactief zouden opstellen om dergelijke illegale beelden op hun infrastructuur te voorkomen. Daarbij is het ook zo dat handhavingsautoriteiten in beginsel ook eigenstandig kunnen handhaven, zonder dat daar een aangifte of melding aan vooraf gaat. Het handelen volgens collectieve rechtsbescherming is een mogelijkheid die de DSA en de AVG bieden, en organisaties zonder winstoogmerk die statutair het openbaar belang dienen kunnen daar gebruik van maken.

8. *Handhaving, niet alleen wetstekst: trackers die alleen registreren of er een wet bestaat, missen waarschijnlijk de variabele die bescherming beter voorspelt. Het bijhouden van vervolgingen, reactietijden voor verwijderverzoeken en de beschikbare handhavingscapaciteit zou beleidsmakers een veel nauwkeuriger beeld geven dan louter de aanwezigheid van wetgeving. Bovendien zou het behandelen van gateways en andere 'toolkits' als afzonderlijke handhavingsdoelen, gelijkwaardig aan afbeeldende content, volgens onze telling minstens 97 kansen voor zelf samengestelde deepfake-NCII wegnemen (het totaal aantal door ons gevonden gateways).*

De evaluatie van beleid wordt gebaseerd op het maatschappelijk effect, niet op het al dan niet hebben van een bepaalde maatregel of interventie, waar ik een wet onder schaar. De maatregel moet uiteindelijk leiden tot een verandering van de situatie. Dat laat onverlet dat een wet, zoals een verbod op AI-toepassingen die deepfakes maken, of een strafbaarstelling van seksuele deepfakes, een normerend effect heeft in de samenleving. U kunt in mijn brief van 16 oktober jl. lezen dat de aanpak van seksuele deepfakes breed is, en niet enkel leunt op opsporing en vervolging van strafbare feiten.

Zoals ik hierboven onder aanbeveling 1 benoem, maakt het bij het verbod op nudify-apps niet uit via welk kanaal deze systemen worden aangeboden of bereikbaar zijn,

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum
23 november 2026

Onze referentie
8235575

inclusief via zogeheten gateway-sites. Platformaanbieders, ook indien zij als doorgeefluik fungeren, behoren geen verboden functionaliteit aan te bieden of te faciliteren.

9. *Versterk de handhavingscapaciteit. Om effectieve toezicht te waarborgen, moeten lidstaten de middelen voor toezichthouders aanzienlijk vergroten om te voldoen aan hun verplichtingen uit art. 50 DSA en art. 70 AI Act. Op EU-niveau moet een onafhankelijke handhavingsautoriteit worden opgericht om middelen te bundelen en politieke inmenging te voorkomen.*

Bij de totstandkoming van de Uitvoeringswet digitaledienstenverordening is een uitvoerbaarheids- en handhaafbaarheidstoets uitgevoerd voor het toezicht op de DSA. Op basis hiervan zijn middelen vrijgemaakt voor de ACM en AP. De ACM heeft voorgesteld om de omvang van de financiering na drie jaar te evalueren en zo nodig te herzien.
Het kabinet vindt het van belang dat de beoogde markttoezichthouders in staat zijn om effectief toezicht te kunnen houden op naleving van de AI-verordening. De beoogd markttoezichtautoriteiten dienen via een uitvoeringswet te worden aangewezen en krijgen daarmee handhavingsbevoegdheden. De conceptuitvoeringswet AI-verordening is in consultatie geweest. Momenteel worden alle reacties die op de conceptuitvoeringswet zijn binnengekomen verwerkt en wordt de wet klaar gemaakt ter aanbieding voor advisering door de Raad van State. De beoogd markttoezichtautoriteiten hebben in juni in beeld gebracht welke capaciteit, expertise en bevoegdheden de nieuwe taken in de conceptuitvoeringswet vergen en wat de gevolgen zijn voor het bestaande takenpakket. De toetsen van de toezichthouders worden betrokken bij de reguliere begrotingsbesluitvorming.

10. *Vergroot de afschrikking via persoonlijke aansprakelijkheid. Nudifier-apps maken deel uit van een lucratief ecosysteem, waarin regulatoire boetes vaak slechts een ingecalculeerde bedrijfskostenpost zijn. Wij bepleiten dat senior beslissers persoonlijk aansprakelijk worden gehouden voor de systemische schade die hun AI-modellen veroorzaken, met name als grove nalatigheid of opzettelijke niet-naleving kan worden bewezen.*

Het kabinet benadrukt dat ontwikkelaars van AI-systemen en AI-modellen verantwoordelijk zijn voor het identificeren en mitigeren van mogelijke risico's via veiligheidsmaatregelen en beheersingsmechanismen. Deze verantwoordelijkheid geldt als producten op de markt zijn gekomen, maar ook voor de ontwikkel- en testfase. Op het moment dat een ondernemer in strijd handelt met deze normen, is deze ondernemer onder voorwaarden civielrechtelijk aansprakelijk jegens derden voor de schade die zij hierdoor lijden en gehouden om deze schade te vergoeden. Als de onderneming wordt gedreven door een rechtspersoon, geldt dat de rechtspersoon jegens deze derden aansprakelijk is. Bestuurders van de rechtspersoon kunnen persoonlijk aansprakelijk worden gesteld voor het onrechtmatig handelen van de rechtspersoon, wanneer hen daarvan persoonlijk een ernstig verwijt kan worden gemaakt. Of een bestuurder persoonlijk een ernstig verwijt kan worden gemaakt, is

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum
23 november 2026

Onze referentie
8235575

afhankelijk van de aard en ernst van de normschending en de overige omstandigheden van het geval. In algemene zin kan worden aangenomen dat daarvan sprake is als een bestuurder binnen de onderneming actief tegenwerkt dat voornoemde verantwoordelijkheid voor het identificeren en mitigeren van mogelijke risico's daadwerkelijk plaatsvindt. Daarmee biedt het huidige recht dus al mogelijkheden om ondernemers, rechtspersonen en onder omstandigheden ook bestuurders persoonlijk aansprakelijk te stellen in geval van grove nalatigheid of opzettelijke niet-naleving van normen.

11. Strafbaar stellen van het creëren van deepfakes zonder toestemming. Het huidige strafrecht richt zich op de verspreiding van deepfakes, niet op de creatie ervan. Het dichten van deze lacune via een geharmoniseerd juridisch kader in alle lidstaten zou rechtshandhavingsinstanties in staat stellen eerder in te grijpen, duidelijke rechtsgronden bieden voor het in beslag nemen van schadelijke software, en de maas in de wet sluiten waarbij daders stellen dat zij het materiaal nooit hebben gepubliceerd.

Het moet glashelder zijn dat het maken van seksuele deepfakes van kinderen of volwassenen die dat niet willen onacceptabel is. Dit is bovendien strafbaar op grond van artikelen 252 en 254ba Sr. In artikel 252 Sr zijn verschillende gedragingen ten aanzien van beeldmateriaal van seksueel kindermisbruik strafbaar gesteld, waaronder het vervaardigen, verspreiden en bezitten van dergelijk materiaal. Deze gedragingen zijn ook strafbaar als het seksueel beeldmateriaal van een (niet bestaand) kind betreft dat met behulp van artificiële intelligentie is gegenereerd. Voorts is het opzettelijk en wederrechtelijk vervaardigen van seksueel beeldmateriaal van volwassen personen strafbaar op grond van artikel 254ba Sr. Van wederrechtelijkheid is in ieder geval sprake als de afgebeelde persoon geen toestemming heeft gegeven voor het maken van het beeldmateriaal. Degene die beschikking heeft over seksueel beeldmateriaal van een ander of dergelijk materiaal openbaar maakt, terwijl hij/zij weet of redelijkerwijs moet vermoeden dat dit materiaal opzettelijk en wederrechtelijk vervaardigd is, is eveneens strafbaar. Tot slot is degene strafbaar die seksueel beeldmateriaal van een ander openbaar maakt terwijl hij/zij weet dat die openbaarmaking nadelig kan zijn voor de afgebeelde persoon. Ook voor artikel 254ba Sr geldt dat seksueel beeldmateriaal van anderen dat is gegenereerd met behulp van artificiële intelligentie onder de reikwijdte van de strafbaarstelling valt.

Vraag 7
Kunt u ingaan op de drie eisen namelijk een meldpunt waarop slachtoffers op een laagdrempelige manier melding kunnen maken van digitaal seksueel misbruik en waar ze meteen makkelijk aangifte kunnen doen (1), handhaving van het uitkleedverbod (2) en een landelijke campagne om het bewustzijn rondom deepfakes te vergroten (3)? Bent u van plan deze uit te voeren?

Antwoord op vraag 7

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum
23 november 2026

Onze referentie
8235575

Zoals ik in mijn brief van 16 oktober jl. over de aanpak van seksuele deepfakes heb geschreven, waardeer ik het initiatief van vijftien leden van uw Kamer zeer.[4] De rechtshandhavingsketen, inclusief organisaties die zich voor preventie inzetten, moet zich aanpassen op de ontwikkelingen. Seksuele deepfakes zijn in mijn ogen een serieus probleem en de aanpak daarvan vergt, hoewel er al een aantal stappen genomen zijn, een nadere analyse om te bezien welke maatregelen aan de aanpak kunnen bijdragen. In deze analyse wil ik alle (mogelijk) effectieve interventies, waaronder de voorstellen van de initiatiefneemsters, meenemen die bijdragen aan het terugdringen van dit probleem. De aanpak van een dergelijk fenomeen is gebaat bij een coherente, integrale benadering, waarbij de uiteindelijk uitgevoerde maatregelen volgen uit een analyse waar en hoe een interventie het meest kansrijk en effectief is. Ik zal de analyse delen met de Tweede Kamer zodra deze gereed is, en daarin zal worden ingegaan op (o.a.) de maatregelen zoals voorgesteld door de initiatiefneemsters.

Vraag 8
Kunt u deze vragen los van elkaar en binnen de gestelde termijn beantwoorden?

Antwoord op vraag 8
Ja, de vragen zijn zo snel mogelijk beantwoord.

[4] Aanpak seksuele deepfakes | Tweede Kamer der Staten-Generaal