# Tweede Kamer der Staten-Generaal

**2**

Vergaderjaar 2025–2026 **Aanhangsel van de Handelingen**


**Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden**

## 1677

Vragen van het lid **Michon-Derkzen** (VVD) aan de Minister van Justitie en Veiligheid over *het bericht «Honderden Nederlandse kinderen slachtoffer van website voor afpersers»* (ingezonden 12 februari 2026).

Antwoord van Minister **Van Weel** (Justitie en Veiligheid) (ontvangen 20 april 2026). Zie ook Aanhangsel Handelingen, vergaderjaar 2025–2026, nr. 1229.

Vraag 1
Bent u bekend met het artikel van RTL Nieuws waaruit blijkt dat een website actief is waarop persoonsgegevens van honderden Nederlanders, waaronder kinderen, staan met als doel om met deze persoonsgegevens de betrokkene af te persen en/of en intimideren?[1]

Antwoord 1
Ja.

Vraag 2
Deelt u de opvatting dat een dergelijke website, dat evident is ingericht om de persoonlijke levenssfeer van personen waaronder minderjarigen te schenden, per direct offline gehaald zou moeten worden?

Antwoord 2
Het misbruiken van persoonsgegevens met afpersing en intimidatie als doel is een zeer ernstig probleem, in het bijzonder in het geval van minderjarigen. Misbruik van persoonsgegevens kan een ingrijpend effect hebben op het slachtoffer en heeft vaak grote gevolgen. Misbruik van persoonsgegevens en de verspreiding van (schadelijke) illegale content online is een complex probleem. Door het grensoverschrijdende karakter en de anonimiteit en snelheid die het internet gebruikers biedt, vormt het aanpakken van kwalijke websites een uitdaging voor de handhaving. Online dienen mensen zich net zo goed aan de regels te houden als offline. Het huidige instrumentarium is erop gericht om de veiligheid van de online omgeving te vergroten en dergelijke schendingen van de persoonlijke levenssfeer van personen tegen te gaan. Allereerst wordt zelfregulatie door de internetsector gestimuleerd.

[1] RTL Nieuws, 9 februari 2026, Honderden Nederlandse kinderen slachtoffer van website voor afpersers (www.rtl.nl/nieuws/binnenland/artikel/5563275/honderden-nederlandse-kinderen-slachtoffer-van-website-voor).


ah-tk-20252026-1677
ISSN 0921 - 7398
's-Gravenhage 2026

Vanuit de sector zijn er meerdere initiatieven, zoals de Gedragscode Abusebestrijding en de Gedragscode Notice and Take Down, om schadelijke content tegen te gaan. Daarnaast zijn er bestuursrechtelijke, strafrechtelijke en civielrechtelijke mogelijkheden. Ook is doxing sinds 1 januari 2024 strafbaar gesteld (artikel 285d Wetboek van Strafrecht). Dit artikel maakt het ongevraagd verzamelen, verspreiden of openbaar maken van persoonsgegevens met het doel iemand te intimideren of lastig te vallen strafbaar.
De verantwoordelijkheid en aansprakelijkheid van online aanbieders van tussenhandeldiensten is gereguleerd via de digitaledienstenverordening (Digital Services Act – DSA). Deze EU-verordening bevat diverse zorgvuldigheidsverplichtingen die onder meer moeten helpen om illegale content tegen te gaan. Zo moet er bij een melding van illegale content prompt actie worden ondernomen. De Autoriteit Consument en Markt (ACM) is in Nederland de primaire toezichthouder op de naleving van de DSA door online aanbieders die in Nederland zijn gevestigd. De ACM werkt voor het toezicht en de handhaving op de DSA, waar nodig, samen met de Europese Commissie en andere lidstaten.
Strafrechtelijk heeft de officier van justitie de mogelijkheid om in specifieke gevallen een aanbieder van een communicatiedienst te bevelen om gegevens ontoegankelijk te maken. In het geval van buitenlandse online aanbieders dient gebruik te worden gemaakt van een rechtshulpverzoek. Dit is vaak tijdrovend, omdat de verantwoordelijke hostingpartij niet altijd kan worden achterhaald en/of worden bereikt. De uitkomst ervan is afhankelijk van de medewerking van het land waaraan het verzoek is gericht. Indien een online aanbieder geen gevolg geeft aan bevelen van de officier van justitie, dan voorziet het strafrecht in de mogelijkheid tot strafvervolging van de aanbieder voor het strafbaar feit dat is begaan. Omdat strafrechtelijk optreden vaak complex en tijdrovend is, en gezien het internationale component afhankelijk is van de bereidheid tot coöperatie van andere landen, zet de politie ook in op alternatieve mogelijkheden, zoals naming and shaming en preventie.[2]
De Autoriteit Persoonsgegevens (hierna: AP) is de toezichthouder op de naleving van de Algemene Verordening Gegevensbescherming (hierna: AVG). De AP beoordeelt uit eigen beweging dan wel op verzoek of in voorkomende gevallen wordt voldaan aan de AVG. Wanneer de AP een overtreding constateert, kan de AP een bestuurlijke boete of dwangsom opleggen, en bevelen tot het stopzetten van gegevensverwerkingen.
Personen kunnen zich ook tot de civiele rechter wenden. Oordeelt deze dat de betreffende content onrechtmatig is, bijvoorbeeld wegens onbevoegd gebruik van persoonsgegevens, dan kan de civiele rechter verwijdering daarvan bevelen.
Om slachtoffers laagdrempelige hulp en een handelingsperspectief te bieden, faciliteert het Ministerie van Justitie en Veiligheid Stichting Offlimits. Via de hulplijn van Offlimits kunnen slachtoffers illegale online content melden. Offlimits beoordeelt deze meldingen en kan, indien sprake is van illegale content, melding doen bij de desbetreffende internettussenpersoon via wie de content beschikbaar is. Offlimits is door de ACM op grond van de DSA aangewezen als betrouwbare flagger.

Vraag 3
Klopt het dat deze website al geruime tijd bekend is bij politie? Zo ja, welke concrete acties zijn sindsdien ondernomen om de website offline te halen of de hostingprovider(s) op te sporen?

Antwoord 3
De politie doet geen mededelingen over lopende onderzoeken.
In het algemeen zijn er, zoals in het antwoord op vraag twee aangegeven, verschillende maatregelen die hostingproviders, de ACM, AP, de politie en het Openbaar Ministerie (OM) kunnen nemen om een website met illegale content offline te krijgen en/of om de hostingproviders van een website op te

[2] Een voorbeeld hiervan is de publicatie van de jaarlijkse resellerbrief: een brief van de politie aan Nederlandse hostingproviders waarin zij adviseert een eventuele overeenkomst met bepaalde resellers (veelal zogenoemde bulletproof hosters) te herzien. Deze brief is recent weer verstuurd (Politie.nl, 12 maart 2026, Politie waarschuwt hostingsector voor hosting resellers: https://www.politie.nl/nieuws/2026/maart/11/11-politie-waarschuwt-hostingsector-voor-hosting-resellers.html).

sporen. Zoals aangegeven in het antwoord op vraag twee, kan de handhaving bij hostingproviders in het buitenland uitdagend zijn vanwege jurisdictie, omdat medewerking mede afhankelijk is van het land waar de dienst is gevestigd.

Vraag 4
Hoeveel aangiften zijn bij de politie bekend die direct te relateren zijn aan deze specifieke website? Wat gebeurt er met deze aangiften? Hoe worden de slachtoffers geïnformeerd over de voortgang van de behandeling van deze aangiften?

Antwoord 4
De politie doet geen mededelingen over lopende onderzoeken.
Slachtoffers worden in het algemeen via MijnSlachtofferzaak.nl op de hoogte gehouden over de voortgang van de behandeling van hun aangifte. Met MijnSlachtofferzaak biedt de overheid slachtoffers en nabestaanden één plek waar zij alle berichten over de zaak kunnen inzien. In dit online dossier treft een slachtoffer alle informatie van de politie over de zaak, en ook het OM, Slachtofferhulp Nederland en Centraal Justitieel Incassobureau (CJIB) informeren hier slachtoffers. Tenslotte informeert ook Schadefonds Geweldsmisdrijven het slachtoffer op MijnSlachtofferzaak over een eventuele tegemoetkoming.

Vraag 5
Hoe ziet de internationale samenwerking eruit bij dergelijke verwerpelijke websites die door hostingbedrijven worden gerund buiten Nederland?

Antwoord 5
De aanpak van bad hosting is zeer complex en tijdrovend vanwege het internationale en volatiele karakter van de hostingindustrie. Al jaren werken de Nederlandse politie, het Openbaar Ministerie en verschillende publieke en private partners samen om de netwerken van hosting providers op te schonen. Vanaf de tweede helft van 2025 is dit ook een speerpunt geworden van het European Cybercrime Centre (EC3) van Europol. Steeds meer landen sluiten aan bij de zogeheten brede bestrijding van schadelijke hosting. Voor strafrechtelijke samenwerking gelden internationale verdragen. Informatie uit het buitenland wordt verkregen op basis van rechtshulpverzoeken, al dan niet voorafgaand aan een bevriezingsbevel.
Daarnaast wordt binnen het project Cleannetworks in samenwerking met de Stichting Nationale Beheersorganisatie Internet Providers (NBIP) het project en de Gedragscode Abusebestrijding verder gestimuleerd op Europees niveau. Voor dit project heeft het Ministerie van Justitie en Veiligheid een Europese subsidie toegekend gekregen. Hierover bent u eerder in de Kamerbrief Integrale aanpak cybercrime geïnformeerd. Binnen het project is de verdere uitbreiding en focus op de Europese markt een belangrijk onderdeel. Misbruik van de digitale infrastructuur is immers grensoverschrijdend en alleen door ons ook buiten de Nederlandse markt te richten kan het meer gericht worden tegengegaan. Hiermee streeft de overheid naar een gelijk speelveld van de sector binnen de EU met dezelfde voorwaarden en voorkomt oneerlijke concurrentie voor de Nederlandse sector.

Vraag 6
Kunt u aangeven of en zo ja welke juridische of technische belemmeringen bestaan om de hostingpartij te dwingen een website waar strafbare feiten op plaatsvinden offline te halen?

Antwoord 6
In het algemeen is het lastig voor Nederlandse autoriteiten om een buitenlandse website die gehost wordt in het buitenland, offline te krijgen. Dit kan bijvoorbeeld komen omdat niet bekend is welke hostingdienst erachter zit of niet bekend is waar de hostingdienst gevestigd is. Hierover bent u ook geïnformeerd in Kamerbrief «Voortgang integrale aanpak cybercrime» in het onderdeel over de verkenning naar de aanpak van bad hosting.[3] Deze

[3] Kamerstukken II, 2024/25, 26 643, nr. 1357

verkenning is gezamenlijk met het Ministerie van Economische Zaken en Klimaat uitgevoerd. In deze verkenning is gekeken naar maatregelen die kunnen worden genomen tegen malafide hosters. Uw Kamer wordt vóór de zomer nader geïnformeerd over de aanpak bad hosting middels een voortgangsbrief over dit onderwerp.

Vraag 7
Wordt er door politie proactief gemonitord op websites of platforms waar doxing plaatsvindt, vergelijkbaar met de aanpak bij kinderporno of terrorisme? Waarom wel of waarom niet?

Antwoord 7
Anders dan bij kinderpornografisch materiaal en terroristische content vindt door de politie en het Openbaar Ministerie niet structureel intensief onderzoek plaats naar doxing. Doxing komt vaak op naar aanleiding van concrete gebeurtenissen en valt onder de generieke opsporing. Kinderpornografisch materiaal en terroristische content zijn anders van omvang en aard. Daar wordt permanent strafrechtelijk op ingezet met onder meer specialistische teams.[4] Een permanente inzet op alle strafbare feiten is met het oog op beschikbare capaciteit binnen de opsporing niet mogelijk. Daarin moeten keuzes worden gemaakt.
Voor kinderpornografisch materiaal en terroristische content geldt bovendien dat de Autoriteit online Terroristisch en Kinderpornografisch Materiaal (ATKM), op basis van Europese en nationale wetgeving de bevoegdheid heeft om bestuursrechtelijk op te treden tegen kinderpornografisch materiaal en terroristische content. De ATKM is zodoende bevoegd een aanbieder van een hostingdienst het bevel te geven het desbetreffende materiaal ontoegankelijk te maken binnen één respectievelijk twaalf uur. De ATKM doet hiervoor zelf actief onderzoek en beoordeelt daarnaast online content aan de hand van meldingen.
Wanneer de politie een melding of aangifte van doxing ontvangt met voldoende aanknopingspunten kan er een opsporingsonderzoek worden opgestart. Het is dan ook positief dat de aanpak van doxing per 1 januari 2024 is versterkt door de strafbaarstelling hiervan in artikel 285d van het Wetboek van Strafrecht. Ook kan de officier van justitie, krachtens artikel 125p Wetboek van Strafvordering, aanbieders van communicatiediensten bevelen strafbare content (waaronder doxing), ontoegankelijk te laten maken.

Vraag 8
Acht u het wenselijk om het delict «doxing» zwaarder te gaan vervolgen, zeker wanneer het om minderjarigen gaat en het leidt tot seksuele intimidatie en ernstige psychische schade?

Antwoord 8
Het OM is verantwoordelijk voor de vervolging van strafzaken. Bij het bepalen van de strafeis kan er door het OM rekening worden gehouden met strafverzwarende omstandigheden. In de Richtlijn voor strafvordering doxing van het OM wordt er onder andere rekening gehouden met de gevolgen voor slachtoffers. Naast doxing kan er sprake zijn van een andere strafbare gedraging. Het is aan het OM om te besluiten of en op basis van welke gronden vervolging plaatsvindt.

Vraag 9
Welke extra stappen bent u bereid te nemen om kinderen online beter te beschermen tegen dit soort extreme vormen van digitale intimidatie?

Antwoord 9
Kinderen kunnen zich niet altijd zelfstandig beschermen en weerbaar opstellen in de online omgeving. Er worden verschillende maatregelen genomen om ervoor te zorgen dat de digitale leefomgeving van kinderen veilig(er) wordt en hun rechten geborgd en versterkt worden. Dit gebeurt

[4] Binnen de politie houden de gespecialiseerde Teams ter Bestrijding van Kinderpornografie en Kindersekstoerisme (TBKK) zich bezig met de opsporing en strafrechtelijke vervolging van kinderpornografisch materiaal, voor terroristische content zijn dat CTER-specialisten.

samen met Europese partners, het bedrijfsleven, maatschappelijke organisaties, ouders, verzorgers en kinderen. De maatregelen richten zich niet alleen op kinderen en ouders, maar ook op ontwikkelaars en aanbieders van online diensten en producten, en op professionals in de zorg en in het onderwijs. De voormalig Staatssecretaris van BZK heeft uw Kamer hierover op 4 september 2025 een brief gezonden waarin de strategie voor online kinderrechten is neergelegd.[5] Deze strategie wordt jaarlijks geactualiseerd; de verwachting is dat voor het zomerreces een nieuwe brief volgt.

[5] 2024–2025, 26 643, nr. 1392