

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

### 3180

Vragen van de leden **Kuik** en **Slootweg** (beiden CDA) aan de Minister van Justitie en Veiligheid en de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over *het bericht «Aantal getroffen websites met ernstig kindermisbruik in twee jaar tijd verdubbeld»* (ingezonden 12 mei 2023).

Antwoord van Minister **Yeşilgöz-Zegerius** (Justitie en Veiligheid) mede namens de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties (ontvangen 7 juli 2023). Zie ook Aanhangsel Handelingen, vergaderjaar 2022–2023, nr. 2786.

#### Vraag 1

Bent u bekend met het bericht «Aantal getroffen websites met ernstig kindermisbruik in twee jaar tijd verdubbeld»?<sup>1</sup>

#### Antwoord 1

Ja.

#### Vraag 2

Bent u het eens met de stelling dat het buitengewoon schrikbarend is dat het aantal websites met de meest ernstige vormen van kindermisbruik in twee jaar tijd is verdubbeld, namelijk naar 51.369 websites?

#### Antwoord 2

Ja; deze wereldwijde trend baart mij zorgen. Ieder jaar presenteert de Internet Watch Foundation (IWF) jaarcijfers waarin veel aandacht wordt geschonken aan enerzijds meldingen vanuit het publiek en anderzijds het eigen onderzoek van IWF naar de aanwezigheid van kinderpornografisch materiaal op het openbare deel van het internet. De aantallen die worden genoemd zijn dus afhankelijk van factoren als het aantal meldingen bij IWF en hoe eenvoudig en openbaar de toegang tot het materiaal is.

#### Vraag 3

Wat is volgens u de oorzaak van deze verdubbeling?

<sup>1</sup> NU.nl, 10 mei 2023, Aantal aangetroffen websites met ernstig kindermisbruik in twee jaar verdubbeld (<https://www.nu.nl/tech/6262984/aantal-aangetroffen-websites-met-ernstig-kindermisbruik-in-twee-jaar-verdubbeld.html>).

### Antwoord 3

Het is niet eenvoudig om een enkele oorzaak van de verdubbeling van het aantal websites met ernstige vormen van kindermisbruik aan te wijzen; zeker omdat het lijkt te gaan om een wereldwijde trend. Daarbij is duidelijk dat seksueel getint beeldmateriaal dat zelf door minderjarigen wordt gemaakt in opkomst is. Laat ik duidelijk stellen dat hierbij niet altijd hoeft te gaan om materiaal dat vrijwillig tot stand is gekomen: het is mogelijk dat minderjarigen hiervoor onder druk worden gezet of gechanteerd of ze zijn zich er niet van bewust dat ze gefilmd worden. Vanuit Nederlands perspectief zal ik me blijven inzetten voor preventie en voorlichting om minderjarigen en hun ouders en voogden meer weerbaar te maken tegen deze vorm van misbruik.

### Vraag 4

Welke redenen maken het aantrekkelijk om bijna een derde van deze websites op Nederlandse servers te hebben?

### Antwoord 4

Het valt niet met zekerheid te zeggen waarom Nederland zo aantrekkelijk lijkt te zijn. Nederland beschikt over een uitstekende digitale infrastructuur. Dat betekent dat er sprake is van snelle verbindingen en beschikbaarheid van voldoende servers en opslagruimte voor webhosting. Deze aspecten leveren de Nederlandse economie veel voordelen op, maar kunnen ook misbruikt worden door criminelen. Daartegen moet doelgericht en effectief worden opgetreden. Juist door deze belangrijke rol van Nederland als wereldwijd internetknooppunt, is de aanpak van online criminaliteitsvormen, waaronder die van online seksueel kindermisbruik, ook een prioriteit van dit kabinet.

### Vraag 5

Bent u bereid om maatregelen te nemen om verspreiding via Nederlandse servers aan te pakken? En zo ja, welke concrete maatregelen gaat u nemen?

### Antwoord 5

Ja, daar ben ik zeker toe bereid. De ambitie van het kabinet is er te allen tijde op gericht al het beeldmateriaal van online seksueel kindermisbruik van Nederlandse servers te weren. Het rapport bevestigt dat dit een omvangrijk, ernstig en lastig te bestrijden fenomeen is. Het belang van de opsporing en vervolging van dit materiaal is opgenomen in de Veiligheidsagenda 2023–2026.<sup>2</sup>

Het is echter niet eenvoudig om het opslaan of online plaatsen van illegale content aan te pakken. Het is middels de EU-Richtlijn Elektronische Handel verboden om aan internettussenpersonen een algehele monitoringsverplichting op te leggen. Veel Nederlandse datacentra verhuren opslagruimte en verzorgen de aansluiting daarvan op het internet. Hun klanten plaatsen daar hun netwerkapparatuur, servers en opslagruimte voor webhosting. Deze hostingdiensten worden vaak doorverhuurd aan tussenpersonen in andere landen (die de webhosting daar veelal onder een eigen merk leveren), die vervolgens weer webruimte verhuren aan privépersonen of organisaties. Datacentra hebben daarom niet altijd zicht op wie aan het eind van de keten precies gebruik maken van hun diensten en welke content wordt gehost. De inzet bij de bestrijding van illegale content gaat voor een belangrijk deel uit van zelfregulering door de internetsector. De Nederlandse overheid werkt reeds jaren samen met de internetsector aan de bestrijding van illegale content online. Zo is al in 2008 een Notice-and-Takedown-gedragscode (NTD) overeengekomen tussen overheden, internetaanbieders, hostingbedrijven, en andere tussenpersonen.<sup>3</sup> Daar is in 2018 een addendum op gekomen voor het verbeteren van de bestrijding van materiaal van online kindermisbruik. Materiaal dat door het in de NTD-gedragscode als «trusted flagger» aangewezen Expertisebureau Online Kindermisbruik (EOKM) als strafbaar wordt aangemerkt, wordt hierdoor in de meeste gevallen al binnen 24 uur na het ontvangen van een verzoek daartoe verwijderd door hostingpartijen. Aanvullend bevat de in 2021 geactualiseerde Gedragscode Abusebestrijding

<sup>2</sup> Kamerstuk 28 684, nr. 717.

<sup>3</sup> <https://www.noticeandtakedowncode.nl>.

maatregelen die hostingproviders kunnen nemen tegen misbruik van hun diensten voor meerdere vormen van illegale activiteiten. Zoals reeds bekend bij uw Kamer, heeft het kabinet de oprichting van een Autoriteit online Terroristisch en Kinderpornografisch Materiaal (ATKM) aangekondigd. Deze Autoriteit krijgt de wettelijke bevoegdheid aanbieders van hostingdiensten op bestuursrechtelijke basis te verplichten online kinderpornografisch en/of terroristisch materiaal op hun server ontoegankelijk te maken of te verwijderen danwel deze partijen op te dragen passende en evenredige maatregelen te treffen om de opslag en doorgifte van online kinderpornografisch en/of terroristisch materiaal via hun diensten te beperken. Hiermee krijgt de Autoriteit middelen om in te grijpen indien de zelfregulering hapert, bijvoorbeeld wanneer een *hoster* weigert gehoor te geven aan een verwijderverzoek van illegale content in het zelfreguleringskader. Het wetsvoorstel dat voorziet in de wettelijke grondslag van deze autoriteit voor de handhaving met betrekking tot kinderpornografisch materiaal, is begin juni bij de Tweede Kamer ingediend.

#### Vraag 6

Welke consequenties kunnen websites verwachten die online kindermisbruik op hun sites tonen, als het gaat om controle en sancties?

#### Antwoord 6

Om bestuursrechtelijk te kunnen handhaven heeft het kabinet de oprichting van een Autoriteit online Terroristisch en Kinderpornografisch Materiaal (ATKM) aangekondigd. Het wetsvoorstel is op 12 juni jl. naar uw Kamer verzonden.

Deze Autoriteit krijgt de wettelijke bevoegdheid aanbieders van hostingdiensten op bestuursrechtelijke basis te verplichten online kinderpornografisch en/of terroristisch materiaal op hun server ontoegankelijk te maken of te verwijderen danwel deze partijen op te dragen passende en evenredige maatregelen te treffen om de opslag en doorgifte van online kinderpornografisch en/of terroristisch materiaal via hun diensten te beperken. Doen ze dat niet, dan kunnen er boetes worden opgelegd. Hiermee krijgt de Autoriteit middelen om in te grijpen indien de zelfregulering hapert, bijvoorbeeld wanneer een *hoster* weigert gehoor te geven aan een verwijderverzoek van illegale content in het zelfreguleringskader.

In geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid, Sv kan de officier van justitie met een machtiging van de rechter-commissaris aan een aanbieder van een communicatiedienst bevelen om gegevens ontoegankelijk te maken als dit noodzakelijk is ter beëindiging van een strafbaar feit. Dit is geregeld in artikel 125p Sv. In artikel 54a Sr is vervolgens bepaald dat als een aanbieder voldoet aan dat bevel, de aanbieder niet wordt vervolgd. Mocht er toch geen uitvoering worden gegeven aan een dergelijk bevel dan is vervolging voor het niet opvolgen daarvan mogelijk. Dat is geregeld in artikel 184 Sr.

Indien een tussenpersoon bewust criminaliteit faciliteert, zoals beeldmateriaal van online seksueel kindermisbruik, kan deze strafrechtelijk aansprakelijk worden gehouden. Zo heeft het Gerechtshof in Den Haag bepaald dat een telecommunicatiedienstprovider die zich ervan bewust is dat zijn klanten crimineel gedrag vertonen en/of criminele content aanwezig hebben dan wel verspreiden, en deze klanten daarbij desalniettemin faciliteert, mogelijk strafrechtelijk aansprakelijk kan worden gehouden, ook als de officier van justitie niet vooraf een verwijderbevel heeft afgegeven.<sup>4</sup> Of daar sprake van is, dient per geval te worden beoordeeld.

#### Vraag 7

Het jaarrapport van de Internet Watch Foundation (IWF) laat zien dat online kindermisbruik steeds zichtbaarder wordt en niet meer weggestopt is op het *dark web*: is het voor de opsporingsdiensten dan juist niet makkelijker om online kindermisbruik offline te laten halen en de websites en dader(s) te sanctioneren? Zo nee, waarom niet?

<sup>4</sup> ECLI:NL:GHDHA:2022:1550.

#### Antwoord 7

De mogelijkheden voor handhaving die opsporingsdiensten hebben op het openbare internet lijken inderdaad groter omdat hostingdiensten beter bereikbaar zijn. Daartegenover staat dat veel van het beeldmateriaal wordt gedeeld via interpersoonlijke communicatiediensten, private chats of beveiligde fora die versleuteld zijn via end-to-end encryptie.<sup>5</sup> Dat maakt de opsporing lastig.

Voor de afspraken in de Veiligheidsagenda is leidend dat opsporingscapaciteit wordt ingezet daar waar het maatschappelijk effect daarvan het grootst is. Dit is wanneer slachtoffers ontzet worden uit acute misbruiksituaties, zowel nationaal als internationaal. Dit kan door het opsporen en vervolgen van daders, het verstoren van de netwerken die seksueel kindermisbruik aanjagen of het tegengaan van het reizen van daders die voor het plegen van seksueel kindermisbruik naar het buitenland gaan. Daarom zal de komende jaren gefocust worden op opsporingsonderzoeken in categorie A (vervaardigers en misbruikers) en categorie B (keyplayers en netwerken).

De politie draagt bij aan de bereidheid van slachtoffers om zich te melden bij organisaties die hen kunnen helpen, bijvoorbeeld bij het offline halen van beeldmateriaal. De politie doet dit bijvoorbeeld door het ondersteunen van deze hulporganisaties of het uitvoeren van voorlichtingscampagnes.

#### Vraag 8

Hoeveel online kindermisbruik is dit jaar verwijderd en hoeveel websites zijn gesanctioneerd voor het vertonen van online kindermisbruik?

#### Antwoord 8

Onlangs heb ik uw Kamer een brief gestuurd waarin enkele aspecten rondom de bevoegdheden van de ATKM nader worden toegelicht en de resultaten van de jaarlijkse TU Delft Monitor over het hosten van materiaal van online seksueel kindermisbruik worden meegenomen.<sup>6</sup> Ik herhaal dat het erop lijkt dat het totale volume van dergelijk materiaal dat aangetroffen is verlaagd is, maar dat er een teruggang lijkt te zijn in verwijderingssnelheid. Dat baart mij zorgen. Daarnaast is het landschap qua hostingbedrijven veranderd; bekende hostingbedrijven zetten zich meer in om materiaal van online seksueel kindermisbruik te verwijderen, maar nieuwe partijen lijken zich volgens de TU Delft monitor minder bewust van de regels en afspraken te zijn. Ook dat laat zien dat een doorlopende samenwerking en overleg met de sector van groot belang is.

Offlimits, voorheen bekend als het Expertisebureau Online Kindermisbruik, houdt een overzicht bij van ontvangen meldingen, de beoordeling daarvan en het aantal verzoeken tot verwijdering die vervolgens worden gedaan. Het meest recente overzicht is te vinden in het jaarverslag van 2021.<sup>7</sup> In dat jaar zijn in totaal 236.743 meldingen binnen Nederland gedaan, waarbij het bij 212.556 van de meldingen inderdaad ging om illegale inhoud waarvoor een verwijderverzoek is gedaan.

In beginsel zijn platformen en websites niet aansprakelijk voor de inhoud die zij laten zien. Zij hebben volgens de EU-Richtlijn Elektronische handel onder voorwaarden een vrijstelling van aansprakelijkheid. De strafrechtelijke sanctienering ziet daarom met name op degenen die het materiaal van seksueel kindermisbruik online hebben gezet, niet op websites zelf. Over 2022 zijn geen cijfers bekend van het sanctioneren van websites.

#### Vraag 9

Hoe kunt u ervoor zorgen dat de makers en verspreiders van online kindermisbruik sneller en harder worden bestraft?

#### Antwoord 9

Zoals aangegeven in de beantwoording op de vragen 5 en 6 hierboven heeft de aanpak van online kindermisbruik hoge prioriteit. Deze aanpak is in de eerste plaats gericht op het effectief opsporen en vervolgen van daders via het strafrecht. Om te voorkomen dat eenmaal gepubliceerd strafbaar

<sup>5</sup> <https://annualreport2022.iwf.org.uk/>.

<sup>6</sup> Brief toelichting ATKM en TU Delft monitor, 7 juli 2023.

<sup>7</sup> EOKM-jaarverslag2021-A5-NL-DEF-interactief.pdf (offlimits.nl).

materiaal op het internet blijft staan of blijft rondgaan, wat voor slachtoffers eveneens zeer schadelijk is, richt mijn aanpak zich daarnaast op de snelle verwijdering ervan. Ik verwijs u in dit kader naar mijn beantwoording van vraag 5.

#### Vraag 10

In hoeverre kunnen de Digital Services Act en het voorstel voor nieuwe Europese wetgeving tegen online kindermisbruik voorkomen dat online kindermisbruik wordt verspreid en op het internet blijft circuleren?

#### Antwoord 10

De Digital Services Act zal de verplichtingen voor de sector met betrekking tot illegale activiteit of inhoud verscherpen. Zo moeten zeer grote onlineplatformen en zoekmachines bijvoorbeeld een risicoanalyse doen van hun systemen om te controleren in hoeverre zij vatbaar zijn voor criminele activiteiten. Vervolgens dienen ze daarop risicobeperkende maatregelen te nemen. Ook worden er minimumvereisten gesteld aan het afhandelen van meldingen over illegale content. Indien zij niet voldoen aan deze vereisten kan er op gehandhaafd worden; voor grote platformen en zoekmachines is dat de Europese Commissie; voor in Nederland gevestigde hostingbedrijven zal dat de nationale digitaaldienstencoördinator worden.

Het voorstel van de Europese Commissie voor een verordening ter voorkoming en bestrijding van seksueel kindermisbruik is erop gericht om nadere regels vast te stellen voor de specifieke illegale content die beeldmateriaal van seksueel kindermisbruik is. De onderhandelingen hierover tussen de Europese Commissie en de Europese lidstaten lopen nog.

#### Vraag 11

In welke mate wordt versleutelde end-to-end-encryptie gebruikt om online beelden van kindermisbruik te delen?

#### Antwoord 11

Vanwege het wijdverbreide gebruik van end-to-end-encryptie voor berichtenverkeer is het lastig om een compleet beeld te hebben van de hoeveelheid materiaal dat via dergelijk berichtenverkeer wordt gedeeld. Wel is het duidelijk, zoals ook het rapport van de Internet Watch Foundation aangeeft, dat er steeds meer gebruik wordt gemaakt van dergelijke interpersoonlijke communicatiediensten voor het delen van beeldmateriaal. Daarom is het van belang dat er mogelijkheden zijn om onder bepaalde omstandigheden toegang tot dit berichtenverkeer te krijgen, onder passende voorwaarden en waarborgen.

#### Vraag 12

Welke mogelijkheden hebben de Nederlandse opsporingsdiensten nu om verspreiding via versleutelde end-to-end-encryptie een halt toe te roepen?

#### Antwoord 12

De opsporingsdiensten zijn, in de meeste gevallen, sterk afhankelijk van de wijze waarop versleutelde communicatiediensten de verspreiding van dergelijk materiaal zélf trachten te voorkomen op hun platform. Bepaalde communicatiediensten doen dit bijvoorbeeld door foto- en videomatching van niet-versleutelde informatie, zoals profiel- en groepsfoto's of groepsinformatie of op basis van verdacht gedrag waarbij wordt gekeken naar metadata. Wanneer de communicatiedienst, op basis van deze technieken, een melding stuurt naar de Amerikaanse toezichthouder NCMEC (conform Amerikaanse wetgeving) en de toezichthouder deze zaak doorverwijst naar Nederland, dan kunnen Nederlandse opsporingsdiensten in bepaalde gevallen optreden tegen individuele daders.

Wanneer een vermoeden bestaat dat een persoon in bezit is van materiaal van seksueel kindermisbruik, is het voor de opsporingsdiensten in bepaalde gevallen mogelijk om toegang te krijgen tot dit materiaal – en zo de verspreiding daarvan te voorkomen. Meestal gaat het dan om toegang tot individuele apparaten, bijvoorbeeld middels een ontsleutelbevel of de bevoegdheid om binnen te dringen in een geautomatiseerd werk, zoals opgenomen in de Wet Computercriminaliteit III. Deze middelen zijn – gelet op de inbreuk die de inzet maakt op de grondrechten – alleen onder strenge

voorwaarden inzetbaar, en de uitkomsten zijn afhankelijk van een (grote) set van externe factoren.