Tweede Kamer der Staten-Generaal
tav de woordvoerders Justitie en Veiligheid
via: cie.jv@tweedekamer.nl

Den Haag, 18 augustus 2023

Bezoek- en postadres
Dr. Kuyperstraat 5
2514 BA Den Haag

T 070-3053333
E info@nlconnect.org
I www.nlconnect.org

Betreft: reactie vereniging NLconnect op Wetsvoorstel bestuursrechtelijke aanpak online kinderpornografisch materiaal

Geachte woordvoerder,

Op 12 juni jl. is door de regering het wetsvoorstel bestuursrechtelijke aanpak online kinderpornografisch materiaal (verder: Child Sexual Abuse Material, CSAM) naar de Tweede Kamer gestuurd (Kamerstuk 36 377). Blijkens de agenda van uw commissie sluit op donderdag 7 september aanstaande de termijn voor de schriftelijke inbreng voor het verslag.

Graag maken wij enkele opmerkingen bij dit wetsvoorstel en verzoeken u deze in uw inbreng bij het verslag mee te nemen. We steunen vanzelfsprekend van harte het doel van dit wetsvoorstel, maar merken op dat enkele bepalingen niet zullen bijdragen aan het uit de lucht halen van CSAM. Het gaat daarbij met name de bepaling van artikel 6 lid 2, op basis waarvan internetproviders DNS-blokkades moeten inrichten. We constateren dat de regering veel verwacht van dit instrument, maar weten uit ervaring dat het helaas niets uithaalt tegen de verspreiding van illegale online content. Het is daarom beter om energie te steken in instrumenten die wel effect sorteren. Hiervoor doen we suggesties. Het wetsvoorstel sluit verder ook slecht aan op de uitganspunten van de Verordening terroristische online-inhoud (verder: TOI-verordening).

NLconnect behartigt de belangen van ruim 80 partijen uit de gehele keten van organisaties die breedbandnetwerken aanleggen en exploiteren, elektronische communicatiediensten aanbieden alsmede uiteenlopende bedrijven die aan deze keten toeleveren. Als glasvezel- en breedbandbranche is het onze ambitie om de voorsprong die ons land heeft op het gebied van digitale connectiviteit te behouden en uit te bouwen. Wij zijn van mening dat een toekomstvaste (glasvezel)-infrastructuur en hoogwaardige digitale (media- en andere) toepassingen van levensbelang zijn voor ons vestigingsklimaat, onze maatschappij en de zich snel ontwikkelende digitale economie. Een veilig en vrij internet is daarbij instrumenteel en daar komen wij dan ook actief voor op.

De goede Nederlandse digitale infrastructuur brengt ons land veel, maar heeft ook een keerzijde: er gebeuren online veel onrechtmatige zaken, die natuurlijk actief (moeten) worden voorkomen en bestreden. Voorliggend conceptwetsvoorstel richt zich in dat kader op een belangrijk negatief deelaspect, namelijk het gegeven dat relatief veel CSAM vanuit ons land wordt gehost. NLconnect steunt uiteraard het doel om het internet te schonen van dergelijke abjecte content. En vanzelfsprekend delen we ook de verontrusting over het aantal meldingen van CSAM.

Zelfregulering
Onze leden beschouwen het als hun medeverantwoordelijkheid om binnen hun rol en mogelijkheden en binnen de kaders van de wet bij te dragen aan de bestrijding van illegale online content. Zij geven daar in de dagelijkse praktijk op uiteenlopende manieren invulling aan. Terecht wordt in de MvT in dit kader ook verwezen naar de gedragscode voor 'notice-and-takedown' (NTD), die reeds in 2008 in werking trad en waarvan onze rechtsvoorganger NLkabel mede-initiatiefnemer was. De code bevat uniforme procesafspraken over hoe te handelen bij meldingen van onrechtmatige content. In Nederland gehoste content kan als gevolg van deze afspraken door de hostingprovider snel en effectief van het internet worden verwijderd. Omdat we de aanpak in de code nog steeds steunen heeft NLconnect eind 2019 ook de aangescherpte code ondertekend. Hierin werd de rol van het EOKM als betrouwbare melder over CSAM versterkt, en is ingezet op het vrijwillig verwijderen van dit type materiaal door hosters binnen een termijn van 24 uur.

Maatregelen tegen bad hosting
Getuige de MvT (p.4) is het wetsvoorstel bedoeld als sluitstuk van deze zelfregulering. Daarbij wordt (in voetnoot 9 van de MvT) verwezen naar de 'CSAM Hosting Monitor' van de TU Delft. Uit deze monitor blijkt dat CSAM zich concentreert bij een zeer selecte groep hostingpartijen, zogenaamde 'bad hosters'. Wij delen de mening dat een bindende aanwijzing richting dergelijke hostingpartijen van toegevoegde waarde kan zijn, wanneer dat effectief leidt tot een hoger percentage van snelle verwijdering van CSAM. Met het voorgestelde artikel 6 lid 1 krijgt de Autoriteit Online Terroristisch en Kinderpornografisch Materiaal (verder: ATKM) deze bevoegdheid. Ook de verplichting in (artikel 7) voor hostingaanbieders om passende en evenredige maatregelen te nemen om de opslag en doorgifte van online kinderpornografisch materiaal te beperken (de zorgplicht) lijkt ons in dat kader gepast.

Ons uitgangspunt is dan ook dat illegale online content zoals CSAM altijd bestreden moet worden bij de bron. Elke aanpak moet gericht zijn op het opsporen en vervolgen van illegale aanbieders en uiteindelijk op het uit de lucht halen van de illegale content. Een aanpak die zich richt op hostingpartijen sluit daarbij aan.

Een DNS-blokkade haalt geen enkele CSAM offline
Ruim 20 leden van NLconnect bieden in hun hoedanigheid van Internet Access Provider (verder: IAP) breedbandige toegang tot internet aan eindgebruikers, via onder meer vaste en mobiele netwerken. Zij zijn alleen betrokken bij het neutraal vervoeren van data en hebben geen invloed op de inhoud van websites. Onze leden het dus niet in hun macht om gegevens daadwerkelijk te (laten) verwijderen. De snelle groei van kinderpornografisch materiaal op internet is dan ook niet te wijten aan enige nalatigheid van IAP's.

In het wetsvoorstel wordt in lid 2 van artikel 6 echter voorgesteld dat de ATKM straks IAP's kan bevelen om websites met CSAM te blokkeren. Op pagina 42 van de MvT valt te lezen dat webblokkades op DNS-niveau worden beoogd.

Wij zijn geen voorstander van deze bepaling omdat de betreffende CSAM dan gewoon online blijft staan en dus niet aan de bron wordt verwijderd. Blokkades van CSAM zijn bovendien zeer eenvoudig te omzeilen. We beschouwen lid 2 van artikel 6 dan ook als symptoombestrijding. Dat lijkt ons een volstrekt verkeerde aanpak van een omvangrijk en ernstig probleem.

Uit de MvT vallen twee argumenten te destilleren waarom is gekozen voor het instrument van de DNS-blokkade:

1. Beoogd wordt te verhinderen of bemoeilijken dat CSAM binnen Nederland wordt verspreid (pagina 31);
2. Beoogd wordt verspreiding te voorkomen van CSAM die niet op Nederlands grondgebied wordt gehost (op pagina 45), waarbij het soms niet mogelijk is om de betrokken in het buitenland gevestigde hostingpartij te identificeren (pagina 53).

Beide argumenten zijn weinig overtuigend:

1. Een DNS-blokkade verhindert of bemoeilijkt nauwelijks want blokkades zijn niet effectief. Gebruikers die bewust onrechtmatige inhoud willen zien laten zich helaas door geen enkele webblokkade tegengehouden. Zij kunnen eenvoudig een andere DNS-server selecteren, Tor gebruiken, een VPN gebruiken of een webproxy of proxy-extensie gebruiken om bij de content te komen. Die wordt tenslotte niet offline gehaald. Bij CSAM zal dat in nog sterkere mate gelden dan bij andere illegale online content: de doelgroep bestaat hier niet uit 'toevallige passanten' of 'gewone consumenten' met beperkte technische kennis, maar uit pedoseksuelen die doelgericht op zoek zijn naar CSAM. In het verleden (rond 2006) hebben enkele IAP's op verzoek van politie en Justitie (DNS-) blokkades ingevoerd, op basis van een zwarte lijst met webadressen die werd bijgehouden door het Meldpunt Kinderporno. In 2011 is men daarmee weer gestopt, omdat deze vorm van blokkade geen effectief instrument bleek te zijn. Naast de gebruikers kunnen ook de aanbieders van CSAM zeer eenvoudig blokkades omzeilen, bijvoorbeeld door de IP-adressen achter de domeinnamen te wijzigen of door hun servers te verplaatsen. Dit kan binnen een zeer kort tijdsbestek. Kortom: blokkeren is bijna letterlijk als 'dweilen met de kraan open'.
2. Wie buitenlandse hostingpartijen wil identificeren en aanpakken moet inzetten op internationale opsporingscapaciteit en vervolging, bijvoorbeeld door meer tijd, geld en effort te stoppen in Europol en Interpol en andere internationale samenwerking richting 'bad hosters. Dat is de enige manier om de CSAM effectief offline te halen.

Kortom: wie denkt dat een DNS-blokkade iets zal opleveren in de strijd tegen CSAM komt helaas bedrogen uit. Om bovenstaande reden zijn we ook van mening dat de door de Europese Commissie voorgestelde concept-Verordening over het tegengaan van online seksueel kindermisbruik op dit punt onvolkomen is. Ook dit voorstel bevat in de artikelen 16, 17 en 18 een optie om DNS-blokkades op te leggen. Nederland moet zich daar in

onze ogen tegen verzetten.[1] Van symbolische maatregelen die geen effect hebben moeten we als samenleving wegblijven.

De volle inzet van de regering moet in onze ogen gericht zijn op aanpak van bad hosters en grotere internationale capaciteit voor opsporing en vervolging van CSAM van 'producenten' en actieve verspreiders en aanbieders van strafbaar beeldmateriaal. Ook kan worden gedacht aan een wettelijke verplichting voor hostingpartijen om potentiële klanten te screenen, aangezien die nu nog ontbreekt.[2]

Disproportionele kosten voor kleine IAP's

De meeste IAP's die lid zijn van NLconnect zijn kleine of middelgrote ondernemingen, met hooguit enkele tienduizenden eindgebruikers. Op basis van rechterlijke bevelen, het 'Convenant Blokkeren Websites' van eind 2021 en EU-sancties tegen Rusland en Belarus worden momenteel door deze IAP's enkele websites geblokkeerd. Het gaat om websites die content bevatten die volgens de rechter inbreuk maken op het auteursrecht of de naburige rechten of die onderdeel zijn van de EU-sancties.

Deze blokkades worden handmatig doorgevoerd. De snelheid van handelen is daarbij uit de aard der zaak laag. Uitgangspunt in de MvT (pagina 42) is echter dat de aanwijzing door de ATKM geautomatiseerd plaatsvindt. IAP's zullen de DNS-blokkades dus ook moeten automatiseren. Zij zijn daar momenteel niet op ingericht. In de MvT wordt gemeld dat de incidentele kosten voor de implementatie hiervan zo'n € 20.000 tot € 30.000 Euro zullen bedragen. Structureel zal het beheer van de geautomatiseerde DNS-blokkades tussen € 1.000 en € 6.000 per maand kosten, mits het aantal aanwijzingen niet meer dan 5 per maand bedraagt. Het komt ons voor dat deze bedragen moeten worden gelezen als bedragen per IAP. Genoemde bedragen vormen een serieuze belasting voor deze MKB-ondernemingen. We verzoeken u aandacht te vragen voor compensatie van deze belasting danwel voor vrijstelling voor kleinere IAP's met relatief weinig klanten. Een dergelijke uitzondering voor micro- en kleine online platforms is bijvoorbeeld opgenomen in artikel 19 van de Digitaledienstenverordening. Een soortgelijke uitzondering zou hier kunnen (moeten) worden gemaakt voor kleinere IAP's.

TOI-verordening vraagt niet om DNS-blokkade

De oprichting van de ATKM als bestuursorgaan was reeds noodzakelijk in verband met de uitvoering van de TOI-verordening en de Kamer ging eerder al akkoord met de Uitvoeringswet TOI. De TOI-verordening heeft tot doel om misbruik van hostingdiensten voor terroristische doeleinden tegen te gaan. Voor dat doel bevat de verordening onder meer verschillende zorgplichten die door aanbieders van hostingdiensten moeten worden nagekomen om de verspreiding van terroristische online-inhoud tegen te gaan en, zo nodig, de snelle verwijdering of blokkering van dergelijke inhoud te garanderen.

De TOI-verordening bevat uitsluitend bepalingen aangaande hostingproviders en dus niet richting IAP's en de ATKM heeft op basis van de TOI dus geen bevoegdheid om DNS-blokkades bij IAP's te bevelen. Het ligt voor de hand om de werkingssfeer van de ATKM ook op het vlak van CSAM te beperken tot de activiteiten in de hostingsector.

---

[1] NLconnect is overigens ook geen voorstander van de in de concept-Verordening voorgestelde maatregel van 'client side scanning', maar om de reden dat die maatregel - zeker voor nummergebaseerde diensten - disproportioneel is en ongericht inbreuk maakt op privacy en veiligheid en vertrouwelijkheid van communicatie.

[2] Antwoorden op vragen van het lid Van Haga over websites met kindermisbruik op Nederlandse servers, nr 2023Z08243, vraag 5

Borging van gelaagde aanpak
In hoofdstuk 3 van de Digitaledienstenverordening wordt een helder onderscheid gemaakt tussen de verschillende soorten tussenpersonen in de online wereld en de verplichtingen die bij hun verschillende rollen horen. Qua verplichtingen geldt in de Digitaledienstenverordening een gelaagdheid die volgt uit de 'afstand' die partijen hebben tot de betreffende content. De meeste verplichtingen gelden voor online platforms (Meta, Google, TikTok, Snap, WeTransfer etc), die een rechtstreekse relatie hebben met (rechts)personen die content plaatsen en ook eigen voorwaarden hanteren voor wat betreft het modereren van content. Minder verplichtingen gelden voor partijen die geen rechtstreekse relatie met eindgebruikers hebben maar alleen data opslaan, zoals hosters. Voor 'mere conduit' diensten als Internet Access gelden nog weer minder verplichtingen dan voor hostingdiensten. Naar analogie zou hetzelfde moeten gelden inzake CSAM.

Het is ons onhelder waarom in voorliggend voorstel wat dat betreft niet beter bij de Digitaledienstenverordening wordt aangesloten. Op pagina 5 van de MvT wordt wel uiteengezet dat de aanwijzing van de ATKM primair wordt gericht tot aanbieders van hostingdiensten en deze slechts als dat in een individueel geval niet mogelijk blijkt kan worden gericht tot IAP's. Op pagina 11 van de MvT wordt gesproken van 'uitzonderlijke gevallen' waarbij een andere vorm van ontoegankelijkmaking aan de orde is dan het verwijderen van de CSAM. De verwachting wordt dus gewekt dat de DNS-blokkade niet vaak zal worden opgelegd. Er zijn op dit vlak echter geen harde waarborgen in de wet opgenomen. Volstaan wordt met de opmerking dat 'de beginselen van evenredigheid en zorgvuldigheid in elk individueel geval grenzen stellen aan de bevoegdheidsuitoefening'. Voor ons is dat onvoldoende borging. Zo is ons onhelder welke bewijslast de ATKM moet leveren dat ze eerst alles heeft gedaan om de CSAM offline te halen, alvorens een aanwijzing op IAP's te richten.

Vallen alternatieve DNS-providers ook onder de reikwijdte?
Het is ons ook onhelder of alternatieve DNS-providers onder de reikwijdte vallen van 138g Wetboek van Strafvordering. Indien een IAP op basis van artikel 6 lid 2 van deze wet straks een aanwijzing krijgt van de ATKM om CSAM ontoegankelijk te maken, dan zal de IAP moeten overgaan tot een blokkade op DNS-niveau. Echter: IAP's zijn niet de enige partijen die DNS-servers beheren. Veel eindgebruikers maken gebruik van alternatieve DNS-servers zoals Google Public DNS, Cloudflare en OpenDNS. Ook gebruiken veel eindgebruikers DNS over HTTPS, waarbij de DNS-resolver is ingebouwd in de webbrowser, zoals Google Chrome, Microsoft Edge, Firefox en Opera.

Wanneer de Kamer onverhoopt instemt met artikel 6 lid 2, dan moet in onze optiek ook geregeld of in elk geval verduidelijkt worden dat alternatieve DNS-aanbieders onder de reikwijdte vallen. Het moet dus helder worden dat de ATKM deze providers op dezelfde wijze behandelt als IAP's, zoals overigens wel adequaat is geregeld en toegelicht in de Digitaledienstenverordening.

Meldingen en relatie tot Offlimits (EOKM)
Ten slotte vragen we ons af hoe de Autoriteit zich gaat verhouden tot het Meldpunt Kinderporno van het Expertisebureau Online Kindermisbruik (verder: EOKM) als betrouwbare melder (trusted flagger) in het systeem van zelfregulering.

In onze optiek kan de regering hier niet volstaan met de mededeling (op pagina 21 en 22 van de MvT) dat de ATKM 'afspraken zal maken met het EOKM over de wijze van

samenwerking en afstemming’. Deze afspraken hadden in onze ogen voorafgaand aan indiening van het wetsvoorstel reeds dienen te zijn gemaakt, opdat volstrekt helder is welke melding straks bij welk loket gedaan dient te worden.

Conform de MvT is het straks mogelijk om (veronderstelde) CSAM bij de ATKM te melden. Maar het EOKM blijft ook actief. Hoe voorkomt de regering dan dat meldingen voortaan direct bij de ATKM worden gedaan en het systeem van zelfregulering de facto wordt ondermijnd en uitgehold, terwijl het de intentie van dit wetsvoorstel is om louter te dienen als sluitstuk van die zelfregulering? Welke meldingen dienen waar binnen te komen en hoe waarborgen ATKM en EOKM dat straks samen?

Overigens draagt het EOKM sinds 8 juni van dit jaar de naam ‘Offlimits’. Hoewel die naamwisseling al was doorgevoerd voordat de wet aan de Kamer werd gestuurd is de toelichting er nog niet op aangepast.

Vanzelfsprekend altijd bereid tot nadere toelichting,

Met vriendelijke groet,

Mathieu Andriessen
directeur