Ministerie van Justitie en Veiligheid

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

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

Den Haag,12-4-2021

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

Geachte heer/mevrouw,

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. Veel leden van NLconnect bieden in hun hoedanigheid van internet access provider breedbandige toegang tot internet aan eindgebruikers, via onder meer vaste en mobiele netwerken. Voor hen is voorliggend conceptwetsvoorstel in huidige vorm direct relevant. We stellen het bijzonder op prijs in de gelegenheid te worden gesteld te reageren op deze consultatie.

Als branche is het onze ambitie om de voorsprong die ons land heeft op het gebied van digitale connectiviteit te behouden en uit te bouwen door er voor te zorgen dat elke Nederlander en elk Nederlands bedrijf de beschikking heeft over uitmuntende en veilige breedbandverbindingen. 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 wij komen daar dan ook actief voor op.

Online illegaliteit bij de bron aanpakken
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 dat relatief veel kinderpornografisch materiaal (verder Child Sexual Abuse Material, CSAM) vanuit ons land wordt gehost. NLconnect steunt uiteraard het doel van voorliggend concept-wetsvoorstel om het internet te schonen van dergelijke abjecte content. En vanzelfsprekend delen we ook de verontrusting over de snelle groei van CSAM op internet, waarvan de minister in de MvT melding maakt. Daarbij hanteren wij als uitgangspunt dat online illegaliteit bij de bron moet worden aangepakt. We constateren dat dit concept-wetsvoorstel niet op alle punten goed aansluit bij dit uitgangspunt.

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 een van onze rechtsvoorgangers - NLkabel - mede-initiatiefnemer was. De code bevat uniforme procesafspraken over hoe te handelen bij meldingen van onrechtmatige content. In Nederland gehoste content kan door 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 is de rol van het EOKM als betrouwbare melder over CSAM versterkt, en wordt ingezet op het vrijwillig verwijderen van dit type materiaal binnen een termijn van 24 uur.

Getuige de MvT (p.3) is het wetsvoorstel bedoeld als sluitstuk van deze specifieke zelfregulering. Daarbij wordt verwezen naar de 'CSAM Hosting Monitor' van de TU Delft. Uit deze monitor blijkt dat de hostingindustrie CSAM in 84% van de gevallen binnen 24 uur heeft verwijderd en in 12% van de gevallen tussen 24 en 48 uur tot verwijdering overgaat. 4% blijft langer dan 48 uur online, in sommige gevallen meer dan een week. Uit de monitor blijkt ook dat het onbekend is waarom sommige url's langer dan 48 uur blijven bestaan: 'deze providers en domeineigenaren hebben soms meer dan 90% van de URL's binnen 24 uur verwijderd, dus ze negeren de NTD's niet categorisch', zo stellen de auteur op pagina 22 van de monitor van september 2020. Er lijkt op basis hiervan dus geen sprake te zijn van structureel onwillige hostingpartijen. Uit de monitor blijkt echter ook dat CSAM zich concentreert bij een zeer selecte groep hostingpartijen, hetgeen wel een zekere mate van 'bad hosting' doet vermoeden. Wij delen de mening dat een bindende aanwijzing richting de betreffende hostingpartijen van toegevoegde waarde kan zijn, wanneer dat effectief leidt tot een hoger percentage van snelle verwijdering van CSAM. Ook de verplichting in artikel 8 voor hostingaanbieders om passende en evenredige maatregelen te nemen om de opslag en doorgifte van CSAM te beperken (de zorgplicht) lijkt ons in dat kader gepast.

Access providers ten onrechte in discussie betrokken
In voorliggend concept wordt voorgesteld om een nieuw op te richten zelfstandig bestuursorgaan - de 'Autoriteit aanpak online kinderpornografisch materiaal' - de bevoegdheid te geven om aanbieders van communicatiediensten een bindende aanwijzing te geven om online CSAM ontoegankelijk te maken wanneer dit via hun diensten wordt opgeslagen of doorgegeven. Het gaat getuige pagina 2 van de MvT om een aanwijzing richting aanbieders die nalaten 'uit eigen beweging' actie te ondernemen tegen online CSAM en om de 'weigering van een aantal tussenpersonen om tegen dit type materiaal op te treden'. Die weigering noopt tot 'een aanvullend instrumentarium, specifiek toegesneden op de bestrijding van online kinderpornografisch materiaal dat in Nederland wordt opgeslagen of doorgegeven.' Op pagina 4 van de MvT wordt expliciet gesteld dat de aanwijzing weliswaar primair is gericht op aanbieders van hostingdiensten, maar ook zal gelden voor caching en voor 'mere conduit' internet access providers, overigens zonder in de wet of de toelichting te regelen dat deze bevoegdheid alleen als ultimum remedium kan worden ingezet. Access providers worden in de opsomming op pagina 4 zelfs genoemd als eerste categorie van partijen op wie het voorstel zich richt!

NLconnect maakt ernstig bezwaar tegen de manier waarop 'bad hosters' en access providers hier door de minister als tussenpersonen over één kam worden geschoren. De snelle groei van CSAM op internet is niet te wijten aan enige nalatigheid van access providers. Uit de CSAM Hosting Monitor blijkt ook *op geen enkele wijze* dat access

providers nalatig zouden zijn. Er is dus geen aanleiding voor een bindende aanwijzing richting access providers. Toch schrijft de minister in de MvT in de context van deze monitor dat ‘de voorliggende bestuursrechtelijke maatregel (…) daarom onmisbaar (is) om alle betrokken bedrijven te bewegen dit type materiaal op zo kort mogelijke termijn ontoegankelijk te maken’, zonder onderscheid te maken tussen hosting- en access providers. Op pagina 22 van de MvT wordt deze onvoldragen redenering herhaald. We achten deze passages onbehoorlijk: access providers worden door de minister zonder opgaaf van reden in hun goede naam aangetast. Wij verwachten in het definitieve voorstel reparatie van deze faux pas.

Op dezelfde pagina van de MvT wordt gesteld dat het concept-wetsvoorstel ‘is gericht op aanbieders die geen of onvoldoende invulling aan de zelfregulering geven’ en dat aanbieders die ‘binnen de zelfregulering adequaat op (CSAM) handelen’ buiten beeld blijven. Voor zover het internet access providers betreft zijn deze stellingen onjuist: het wetsvoorstel is in huidige vorm ook gericht op toegangsaanbieders, die voldoende invulling geven aan de zelfregulering en die adequaat op CSAM handelen. We verzoeken dit aan te passen. Het ‘uit eigen beweging actie ondernemen’ waar de minister over spreekt is voor access providers natuurlijk - en terecht - bij wet verboden. Het zou neerkomen op censuur. De verordening netneutraliteit stelt dat alle internetverkeer gelijk moet worden behandeld en dat access providers internetverkeer niet mogen beperken of beïnvloeden. We doen een dringend verzoek om de tekst van wet en toelichting zodanig aan te passen dat deze - in lijn met de aanleiding voor het voorstel en met de CSAM Hosting Monitor - alleen van toepassing is op hostingproviders.

Evaluatie
Zoals gezegd nemen internet access providers graag hun verantwoordelijkheid om binnen hun rol en mogelijkheden bij te dragen aan de bestrijding van illegale online content en CSAM in het bijzonder. Wanneer uit objectief onderzoek zou blijken dat het strikt noodzakelijk is dat zij - als sluitstuk – toch onder de werkingssfeer van dit voorstel zouden moeten komen te vallen, dan berusten wij daarin. In het voorstel wordt dit bewijs echter niet geleverd en wij kennen ook geen onderzoeken die daarop wijzen.

Wij kunnen ons voorstellen dat - nadat er enige tijd wordt gewerkt met de zorgplicht en met bindende aanwijzingen richting hostingpartijen - een evaluatie wordt verricht om te bezien of de maatregelen het gewenste effect hebben en of wellicht verdere maatregelen nodig zijn. Op dat moment kan ook worden bezien in hoeverre de op pagina 14 van de MvT voorziene samenwerking van de nieuwe Autoriteit met vergelijkbare Autoriteiten in het buitenland vruchten heeft afgeworpen en leidt tot verwijdering van CSAM die in het buitenland wordt gehost. Hoewel een monitor is ingericht, ontbreekt een formele evaluatiebepaling en duidelijk evaluatiemoment. Wij adviseren die toe te voegen.

Werkwijze Autoriteit onhelder
De nieuw op te richten Autoriteit zal zich tevens gaan richten op de ontoegankelijkmaking van online terroristisch materiaal. Dit ter implementatie van de aanstaande verordening ter voorkoming van de verspreiding van terroristische online-inhoud. Ook het voorstel van de Europese Commissie voor deze verordening (COM/2018/640 final) en het recente standpunt van de Raad hierover (14308/1/2020 – C9-0113/2021 – 2018/0331(COD)) bevatten uitsluitend bepalingen aangaande hostingproviders en dus niet richting access providers. Randnummer 13 van het standpunt van de Raad sluit caching-, DNS- en ‘mere conduit’ providers zelfs expliciet uit. Het ligt dus ook om die reden voor de hand om de werkingssfeer van de Autoriteit te beperken tot de activiteiten in de hostingsector.

We vragen u verder om in de MvT nader te duiden hoe de Autoriteit zich gaat verhouden tot het huidige stelsel en tot EOKM als betrouwbare melder, anders dan te volstaan met de mededeling dat ‘over samenwerking afspraken zullen worden gemaakt’. Deze afspraken moeten in onze ogen voorafgaand aan indiening van het wetsvoorstel reeds zijn gemaakt en duidelijk zijn gecommuniceerd. Gaan bijvoorbeeld met het oog op de snelle verwijdering van CSAM voortaan alle meldingen vanuit het EOKM richting hostingaanbieders direct via de Autoriteit als verzoek en zo nodig sommatie? Zo niet, op welke wijze kan de Autoriteit dan bijdragen aan de met het wetsvoorstel beoogde snelle verwijdering? Of vervangt de Autoriteit het EOKM geheel? Het wordt ook mogelijk om (verondersteld) online CSAM bij de Autoriteit te melden. We verzoeken nader te duiden welke lacune hiermee beoogd wordt opgevuld te worden ten opzichte van het bestaande stelsel.

Blokkeren is niet effectief
In de artikelsgewijze toelichting op artikel 1 wordt expliciet gemaakt dat CSAM ontoegankelijk kan worden gemaakt door het blokkeren van toegang. ‘Blokkering kan bijvoorbeeld aan de orde zijn als de desbetreffende aanbieder van een communicatiedienst het niet in zijn macht heeft het materiaal te verwijderen’, zo wordt gesteld. Bij access providers ligt dat per definitie niet in hun macht. De facto wordt hier dus voorgesteld dat de nieuw op te richten Autoriteit aan access providers aanwijzingen kan geven om bepaalde content te blokkeren.

Los van de vraag of er aanleiding is voor een dergelijke maatregel - quod non - , is NLconnect daarvan geen voorstander. Illegaliteit online moet bij de bron aangepakt worden. Bij filteren en blokkeren wordt eindgebruikers de toegang tot aanwezige content ontzegd. Dat betekent dat CSAM gewoon online blijft en dus niet aan de bron wordt verwijderd. Dat lijkt ons een volstrekt verkeerde aanpak.

Een blokkade van internetverkeer is ook potentieel schadelijk: achter één IP-adres kunnen verschillende websites zitten die mogelijk ten onrechte onbereikbaar worden gemaakt. En DNS-blokkades ondermijnen de methode om te communiceren via DNS, waarmee fragmentatie van het internet op de loer ligt.

Blokkades zijn ook niet effectief. Uit de praktijk rond auteursrechtelijk beschermd materiaal is bekend dat gebruikers die de betreffende onrechtmatige content bewust willen consumeren zich niet door een blokkade laten tegenhouden. Bij CSAM zal dat in nog sterkere mate gelden: de doelgroep bestaat hier niet uit ‘toevallige passanten’ met beperkte technische kennis of ‘gewone consumenten’, maar uit pedoseksuelen die doelgericht op zoek zijn naar CSAM.

Het soort blokkades wordt niet nader omschreven, maar vermoedelijk worden DNS- en IP-blokkades beoogd. In het verleden (rond 2006) hebben enkele access providers op verzoek van politie en Justitie (url-) blokkades ingevoerd voor CSAM, op basis van een zwarte lijst met webadressen die werd bijgehouden door het Meldpunt Kinderporno. In 2010 is men daarmee weer gestopt, omdat deze vorm van blokkade geen effectief instrument bleek te zijn. Dat geldt evenzeer voor IP- en URL-blokkades, die makkelijk zijn te omzeilen door een andere DNS-server in te stellen, door gebruik te maken van Tor, een VPN, webproxy of proxy-extensie. Blokkeren is dweilen met de kraan open.

MKB-toets ontbreekt voor access providers

Blokkades leveren ook een belasting op voor de access provider, die daar uit de aard der zaak niet op zijn ingericht. Onze verwachting is dat de impact technisch gezien wel te overzien zou zijn: routereringsmechanismen zullen moeten worden geconfigureerd om een blokkade te implementeren. Beheerstechnisch zullen wel de nodige aanpassingen moeten worden gedaan aan interne bedrijfsprocessen.

Dit alles is evenwel niet in kaart gebracht. Zo blijkt uit pagina 21 van de MvT dat er enkel een ‘panelgesprek’ heeft plaatsgevonden, waarbij een zeer beperkt aantal aanbieders van hostingsdiensten aanwezig was. Mocht de minister onverhoopt volharden in een aanwijzing die ook is gericht op aanbieders van internet access diensten, dan verzoeken we de MKB-toets opnieuw uit te voeren, met inbegrip van een ruime en representatieve vertegenwoordiging van deze laatste categorie aanbieders. Hetzelfde geldt voor de regeldruktoets, aangezien in de paragraaf over regeldruk niet expliciet in kaart wordt gebracht welke regeldruk het voorstel met zich meebrengt voor grotere en kleinere access providers.

Anticiperen op Digital Services Act
NLconnect is op basis van bovenstaande van oordeel dat blokkering geen noodzakelijke, proportionele of effectieve maatregel is in de strijd tegen CSAM. Access providers hebben dan ook een volstrekt andere rol dan hostingproviders, die wel effectief kunnen bijdragen aan verwijdering. We pleiten in dat kader ook voor betere internationale samenwerking richting ‘bad hosters’.

Uit de MvT (voetnoot 9) blijkt dat de Digital Services Act (DSA) nog niet is betrokken bij het voorstel, omdat ‘nog niet duidelijk (is) wanneer deze verordening in werking zal treden en hoe de uiteindelijke tekst zal luiden’. Dat geldt natuurlijk ook voor de verordening ter voorkoming van de verspreiding van terroristische online-inhoud, maar die is juist wel betrokken, zij het op selectieve wijze. NLconnect raadt aan om de DSA-voorstellen ook mee te nemen in anticipatie op wat komen gaat. In de huidige DSA-voorstellen wordt een helder onderscheid gemaakt tussen de verschillende soorten tussenpersonen in de onlinewereld en de verplichtingen die bij de verschillende rollen horen. Ook in deze voorstellen geldt voor mere conduit diensten als internet access een ander (en lichter) regime dan afzonderlijk voor hostingdiensten en voor online platforms geldt. Naar analogie zou hetzelfde moeten gelden inzake CSAM.

Technische suggesties
Ten slotte doen we graag een tweetal suggesties van meer technische aard:

Op pagina 8 van de MvT staat beschreven dat de betrokken dienstverlener na ontoegankelijkmaking een kopie van CSAM dient over te dragen aan de Autoriteit, ten behoeve van de bestuursrechtelijke procedure, alsook ten behoeve van een (eventuele) strafrechtelijke procedure. We nemen aan dat hier specifiek wordt gedoeld op hostingaanbieders en raden aan dat ook zo expliciet te beschrijven.

Op pagina 14 van de MvT wordt gesteld dat de Autoriteit de uitgaande aanwijzingen zal monitoren, zodat inzichtelijk wordt welke aanbieders meldingen ontvangen en binnen welke termijn deze worden opgevolgd. Hierbij wordt ook vermeld dat deze monitor al door de Technische Universiteit Delft gebouwd en werkzaam is. Voor zover het hostingaanbieders betreft is dit laatste correct, voor zover het access providers betreft niet.

Vanzelfsprekend altijd bereid tot nadere toelichting,

Met vriendelijke groet,

Mathieu Andriessen
directeur