Confidentieel, niet openbaar maken aub

Ministerie van Justitie & Veiligheid
Elektronische indiening per https://www.internetconsultatie.nl/autoriteitkp

Onderwerp: **Consultatie Wet bestuursrechtelijke aanpak van online kinderpornografisch materiaal**

Geachte heer, mevrouw,

Middels onderstaande reactie maakt VodafoneZiggo graag gebruik van de door de Minister van Justitie en Veiligheid (hierna: J&V) geboden gelegenheid om te reageren op de consultatie **bestuursrechtelijke aanpak van online kinderpornografisch materiaal**.

We zetten graag eerst een aantal algemene punten uiteen, alvorens puntsgewijs door de concepttekst en memorie van toelichting te gaan.

Algemeen

Algemeen en waterbedeffect

Allereerst wensen we, middels dit schrijven, te benadrukken dat VodafoneZiggo te allen tijde het vervaardigen, bekijken en verspreiden van kinderpornografisch materiaal (verder gebruiken we ook de internationale term CSAM – child sexual abuse material) ten strengste afkeurt, en dat we onbehoedzame gebruikers van het internet ervoor moeten beschermen dat ze met dit materiaal in aanraking komen door het materiaal bij de bron (dat is bij hostingpartijen) te verwijderen. We vragen de Minister daarbij in te zetten op een zeer gedegen internationale samenwerking, zodat ook hostingpartijen die zich in andere landen bevinden in actie komen en het materiaal van hun servers verwijderen. Bovendien is het zaak om het probleem achter CSAM - seksueel misbruik en mensenhandel - adequaat aan te pakken.

In het licht van het conceptwetsvoorstel bestuursrechtelijke aanpak online kinderporno, moeten we tegelijkertijd ook reëel zijn en bezien dat de meeste gebruikers van dit type content willens en wetens ernaar op zoek gaan. Dat betekent ook dat als het openbare deel van het internet geschoond is van CSAM, er een zeer gerede kans bestaat, dat een groot deel van deze content via dan wel het darkweb, dan wel via VPN (virtual private networks)-verbindingen, dan wel via proxies alsnog verder verspreid wordt. Bovendien is er dan veel minder zicht op waar dit CSAM staat, en hoe lang dit vervolgens online staat. Dat betekent dat we het probleem achter dit probleem, namelijk (seksueel) misbruik van kinderen en mogelijke mensenhandel minder goed kunnen aanpakken en daarom moet ook de inzet blijven op het tegengaan van het misbruik en het produceren van CSAM.

Bovendien is de aanpak van CSAM per definitie een internationaal probleem. We moeten onszelf niet voor de gek houden en denken dat als dit type content van

Nederlandse servers en datacenters verdwenen is, het probleem opgelost is. Er bestaat dan ook een gerede kans dat het probleem zich naar andere landen zal gaan verplaatsen (*'waterbed effect'*). Het is dan ook van zeer groot belang dat het Ministerie en de op te richten Autoriteit kinderporno (Autoriteit KP) zich hard maken om Europese samenwerking met autoriteiten in andere lidstaten van de EU te bestendigen, verbeteren en versnellen, zoals ook in de Memorie van Toelichting (MvT) is aangegeven[1].

Verwijdering CSAM bij de bron

Uit artikel 9, 'Aanwijzing' van het wetsvoorstel blijkt dat ook Internet Access Providers (IAPs, ook wel Internet Service Providers/ ISPs genoemd), zoals VodafoneZiggo worden aangesproken om maatregelen te treffen: *'De Autoriteit kan een aanbieder van een communicatiedienst die online kinderpornografisch materiaal doorgeeft of heeft opgeslagen een aanwijzing geven alle redelijkerwijs te nemen maatregelen te treffen om dit materiaal ontoegankelijk te maken.* IAPs zijn als *mere conduit* partijen[2], als toegangsintermediairs in de keten van partijen die het *world wide web* faciliteren, niet bij machte om materiaal van het internet zondermeer te verwijderen. Daarmee vereist een dergelijke artikel het de facto filteren, dan wel blokkeren van een website URL door een IAP.

VodafoneZiggo staat de aanpak van het verwijderen van CSAM bij de bron voor. Dat betekent dat dit materiaal wordt verwijderd op de server waar dit materiaal opgeslagen staat. Het verheugt VodafoneZiggo dat dit uitgangspunt ook het vertrekpunt van de wetgever lijkt te zijn geweest bij het schrijven van het onderhavige conceptwetsvoorstel. Verwijderen bij de bron is naar mening van VodafoneZiggo ook altijd het uitgangspunt geweest voor de gesprekken die de afgelopen twee jaar gevoerd zijn met vertegenwoordigers van de sector, de politie, de TU Delft en het Ministerie in het kader van de publiek-private samenwerking om het CSAM-probleem aan te pakken.

Ook de Notice-and-Take-Down (NTD)-code, die uit 2008[3] stamt, wordt nog steeds door betrokken partijen uit de internetketen als zelfreguleringsmechanisme gehanteerd om *onbetwist onrechtmatig materiaal* van het internet te verwijderen. Eind 2019 is deze code aangescherpt met een bepaling betrekking hebbend op het verwijderen van CSAM. Deze code werkt ook op basis van het verwijderen van materiaal bij de bron.

De nieuw op te richten Autoriteit KP zal zich tevens gaan richten op het ontoegankelijk maken van online terroristisch content (TCO), waarmee Nederland aan de implementatie van de aanstaande verordening ter voorkoming van de verspreiding van terroristische online inhoud (COM/2018/640 final) gehoor geeft. Ook het voorstel van de Europese Commissie voor deze verordening bevat uitsluitend bepalingen die gericht zijn op het verwijderen van content bij de bron, c.q. bij hostingproviders, en voorziet niet in het blokkeren van content door IAP's. Het ligt dus om die reden voor de hand om de werkingssfeer van de Autoriteit te beperken tot activiteiten in de hostingsector.

---

[1] Memorie van Toelichting wetsvoorstel bestuursrechtelijke aanpak kinderporno, p7

[2] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')

[3] https://www.noticeandtakedowncode.nl.

VodafoneZiggo constateert dat het voorliggende conceptwetsvoorstel niet op alle punten goed aansluit bij het uitgangspunt om het internet te schonen bij de bron, dat wil zeggen CSAM te verwijderen op servers van hostingproviders. Wij roepen het ministerie dan ook om het wetsvoorstel op dit punt te wijzigen.

Blokkeren is niet effectief

VodafoneZiggo is geen voorstander van het structureel blokkeren van websites op Domain Name Server (DNS) niveau om CSAM ontoegankelijk te maken, omdat het materiaal in digitale vorm zeer snel verspreid en vermenigvuldigd kan worden. Uit onderzoek en eerdere ervaring uit de sector blijkt dat het blokkeren van een enkele website in dit kader weinig effect zal sorteren.

Bovendien laat men door het blokkeren van website op DNS-niveau de bron intact, wat weer kansen biedt voor de verdere verspreiding van CSAM via andere onlinekanalen, zoals bijvoorbeeld het darkweb. Zo bezien is het blokkeren van websites dan ook symptoombestrijding in plaats het echt aanpakken van de oorzaak.

Een blokkade van internetverkeer is ook schadelijk en kan leiden tot 'over-blocking': achter één IP-adres kunnen namelijk verschillende websites zitten, die mogelijk ten onrechte onbereikbaar worden gemaakt. DNS-blokkades ondermijnen bovendien de methode om te communiceren via DNS, waarmee fragmentatie van het internet op de loer ligt.

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 doorgaans niet uit 'toevallige passanten' of 'gewone consumenten' met beperkte technische kennis, maar uit mensen met pedoseksuele gevoelens, die doelgericht op zoek zijn naar CSAM.

Het soort blokkades wordt in het wetsvoorstel niet nader omschreven, omdat de Minister niet de methode van het ontoegankelijk maken wil voorschrijven, maar voor IAPs ligt DNS- en IP-blokkades voor de hand. In het verleden (rond 2006) hebben enkele access providers op verzoek van politie en Justitie (URL-)blokkades ingevoerd, 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 gemakkelijk zijn te omzeilen door bijvoorbeeld een andere DNS-server in te stellen, door gebruik te maken van Tor-browsers, een VPN, web proxy of proxy-extensie. Met andere woorden: blokkeren is dweilen met de kraan open.

VodafoneZiggo roept het ministerie op om af te zien van het blokkeren van websites als kernonderdeel van de voorliggende wetgeving.

Getrapte aanpak en ultimum remedium

Zoals bovenstaand betoogd, ziet VodafoneZiggo niets in het blokkeren van websites als onderdeel van dit wetsvoorstel (neergelegd in art. 9, *Aanwijzing*). Indien het ministerie toch van mening is om het blokkeren van websites in te brengen in haar aanpak van online CSAM, zou VodafoneZiggo er voor willen pleiten om expliciet in de wetgeving op

te nemen dat het blokkeren van een websites een **ultimum remedium** is en als zodanig ook zal moeten worden ingezet door de nieuw op te richten toezichthouder.

Uit het huidige concept blijkt namelijk nog niet dat er een duidelijk volgordelijkheid dient te worden aangehouden door de toezichthouder. Dus: eerst verwijdering van CSAM bij de bron en pas als een webhoster, of datacenter (al dan niet in het buitenland) niet reageert op een verzoek en/of sommatie tot verwijdering, men pas zou kunnen overgaan tot het blokkeren van dit materiaal middels een DNS-blokkade in Nederland.

Deze getrapte aanpak van het probleem wordt op dit moment nog niet gehanteerd in de conceptwetgeving, terwijl deze wel in de MvT wordt aangehaald. De MvT spreekt ter illustratie op pagina 4 van *'De aanwijzing wordt daarom primair gericht tot aanbieders van hostingdiensten. Slechts als het niet mogelijk blijkt de betrokken aanbieder van hostingdiensten te identificeren of daar een aanwijzing aan te geven, wordt de aanwijzing gericht tot een andere aanbieder van een communicatiedienst, zoals een betrokken internet access provider'.*
Daarnaast, tevens op pagina 8: *'Gelet op het uitgangspunt dat kinderpornografisch materiaal zoveel mogelijk moet worden verwijderd, wordt de aanwijzing primair gericht tot aanbieders van hostingdiensten: een aanbieder van een communicatiedienst bestaande uit de opslag van gegevens die van een ander afkomstig zijn'.*
In het conceptwetsvoorstel zien we echter dat IAPs in artikel 9 de eerst aangesproken partij lijken te zijn: *'De Autoriteit kan een aanbieder van een communicatiedienst die online kinderpornografisch materiaal doorgeeft of heeft opgeslagen een aanwijzing geven alle redelijkerwijs te nemen maatregelen te treffen om dit materiaal ontoegankelijk te maken'.*

Indien het absoluut noodzakelijk is om tot het blokkeren van websites over te gaan, pleit VodafoneZiggo voor het aanbrengen van een meer getrapte aanpak. Hierbij moet het voor de nieuwe toezichthouder duidelijk zijn dat de inzet van haar bevoegdheid om het blokkeren van websites te eisen een absoluut ultimum remedium is, en slechts in zeer uitzonderlijke gevallen, waarbij (internationale) aanpak bij de bron faalt, mogelijk is.

VodafoneZiggo hecht er waarde aan te onderstrepen dat de huidige aanpak in publiek-private samenwerkingsverband (PPS)-, samen met de internetsector en overheid tot de nodige successen heeft geleid in de aanpak van online kinderpornografisch materiaal. Zo hebben we een hash-check-server kunnen introduceren, hebben we, gezamenlijk met de TU Delft, een CSAM-monitor kunnen laten bouwen, en hebben we de toevoeging van de aanpak CSAM in de NTD-code kunnen inbrengen. We zouden dan ook graag zien dat deze PPS-aanpak z'n vervolg krijgt in toekomstige bestrijding van dit type content onder de vlag van de nieuwe Autoriteit KP. Om continuïteit van dit overleg te garanderen zou VodafoneZiggo willen voorstellen om de huidige PPS-constructie verder te institutionaliseren door een Raad van Advies in te stellen, die de Autoriteit KP van advies kan voorzien op allerlei terreinen rondom het thema CSAM. Daarmee verzekeren we ons ook van het feit dat vakinhoudelijke experts vanuit de markt in nauw contact staan met de toezichthouder. Dit is zeer belangrijk in een snel veranderende technisch complexe omgeving.

Artikelsgewijs

- **Art. 7, Afstemming** – VodafoneZiggo zou graag zien dat hier een element wordt toegevoegd, namelijk een Raad van Advies, bestaande uit vertegenwoordigers van de keten van internet faciliterende bedrijven. Hiermee zou de PPS-constructie waarmee de afgelopen twee jaar onder auspiciën van het ministerie van Justitie succesvol aan de aanpak van online CSAM gewerkt is, kunnen worden geïnstitutionaliseerd.

- Art. 9, **Aanwijzing** – VodafoneZiggo zou in lid 1 het woord 'doorgeeft' willen laten vervallen, zodat het duidelijk is dat de eerste aangesprokene partij de hosting bedrijven zijn. Lid 1 komt er dan als volgt uit te zien:
'*De Autoriteit kan een aanbieder van een communicatiedienst die online kinderpornografisch materiaal heeft opgeslagen een aanwijzing geven alle redelijkerwijs te nemen maatregelen te treffen om dit materiaal ontoegankelijk te maken.*'

- Indien er toch voor gekozen wordt door het ministerie om ook IAP's een rol te laten spelen het ontoegankelijk maken van CSAM, dan zou VodafoneZiggo de suggestie willen aandragen om duidelijk te laten blijken dat de toezichthouder hier een getrapte aanpak dient te hanteren. VodafoneZiggo doet in dat geval de suggestie om een additioneel lid in te voegen tussen lid 3 en lid 4, met de volgende tekst: '*Indien een aanwijzing, dan wel het opleggen van boetes, of dwangsom, dan wel de communicatie met andere internationale toezichthouders niet leidt tot het verwijderen van het bepaalde online kinderpornografisch materiaal, dan kan de Autoriteit KP als ultimum remedium, verzoeken aan de communicatiedienst, die online kinderpornografisch materiaal doorgeeft, deze ontoegankelijk te maken.*'

- Art. 14, **Behoud van materiaal** – in het eerste lid wordt een verplichting opgelegd aan de Aanbieder van hostingdiensten, dan wel een aanbieder van communicatiediensten, om een kopie van het door de aanbieder ontoegankelijk gemaakte materiaal te verstrekken aan de Autoriteit. Teneinde aan deze verplichting te kunnen voldoen, voor zover al mogelijk, zal de betreffende aanbieder dit materiaal moeten verwerken (opslaan, verzenden). Deze verplichting staat op bijzonder gespannen voet met lid 1 Art. 240b Wetboek van Strafrecht. Daarbij kan tevens worden opgemerkt dat medewerkers van VodafoneZiggo tijdens dit verwerken mogelijk ongewild en ongewenst in aanraking komen met CSAM. Deze confrontatie van VodafoneZiggo medewerkers met CSAM is uitermate ongewenst. Medewerkers zijn hiervoor niet getraind en het omgaan met schokkend materiaal vergt professionele begeleiding, die de gemiddelde Aanbieder van hostingdiensten en aanbieder van communicatiediensten, waaronder VodafoneZiggo, niet kan geven.

- **MvT, hoofstuk 2.2.** (**'Hoofdlijnen van het voorstel'**) Ook in opsomming op pagina 4, in hoofdstuk 2.2 van de toelichting, wordt wat ons betreft niet de juiste volgordelijkheid aangehouden. Ook hier begint de wetgever met het benoemen van het blokkeren van websites als eerste mogelijkheid om online CSAM ontoegankelijk te maken, in plaats van de aanpak van hosting providers primair leidend te laten zijn. Men zou in de opsomming gesteld in dit hoofdstuk moeten

beginnen met Hosting, dan Caching, dan pas, als ultimum remedium, het blokkeren van websites door een IAP. In de alinea daarna, wordt het in onze ogen wel juist aangedragen: *'De aanwijzing wordt daarom primair gericht tot aanbieders van hostingdiensten. Slechts als het niet mogelijk blijkt de betrokken aanbieder van hostingdiensten te identificeren of daar een aanwijzing aan te geven, wordt de aanwijzing gericht tot een andere aanbieder van een communicatiedienst, zoals een betrokken internet access provider.'* (p.4, Memorie van Toelichting).

- Uit de MvT (voetnoot 9) blijkt dat de Digital Services Act nog niet is 'meegenomen' in het wetsvoorstel. VodafoneZiggo raadt aan om dat wel te doen, al was het maar om alvast te anticiperen op deze aanstaande Europese wetgeving. In de huidige DSA-voorstellen wordt een helder onderscheid gemaakt tussen de verschillende soorten tussenpersonen in de keten van internet faciliterende bedrijven en de verplichtingen die bij de verschillende rollen horen. Ook in deze voorstellen geldt voor mere conduit diensten als internet toegang een ander (en lichter) regime, dan afzonderlijk voor hostingdiensten en voor online platforms geldt. Wij zijn van mening dat in analogie hetzelfde zou moeten gelden met betrekking tot CSAM.

- MvT, hoofdstuk 3.2 ('Aanwijzing') van de toelichting, laat ook zien, dat een van de voornaamste redenen voor de wetgever om ook IAP's aan te spreken was, dat sommige content in het buitenland gehost wordt en dus buiten de territoriale landsgrenzen en directe invloedsfeer van Nederland valt. Ook dan lijkt blokkeren een niet proportioneel middel, dat bovendien niet voorkomt dat CSAM materiaal elders op het internet opduikt, al dan niet beschikbaar gesteld middels een andere URL, of zelfs nog sneller, via een proxy, dan wel een mirror link van de originele te blokkeren website. Een vele malen effectievere aanpak zou zijn, om ook hier de competente lidstaat binnen de EU (of daar buiten) aan te spreken, zodat lokale autoriteiten ter plekke kunnen handelen en een hoster kunnen dwingen om deze content offline te halen. Hiervoor is, net als met online terrorismecontent, een Europese aanpak noodzakelijk, die op het moment van schrijven van deze consultatie reactie in de maak is.

Voor eventueel nadere toelichting zijn wij uiteraard bereikbaar.

Met vriendelijke groet,

Director Regulatory, Policy and Public Affairs VodafoneZiggo