Stichting Digitale
Infrastructuur Nederland

De Minister van Justitie en Veiligheid
p/a Ministerie van Justitie en Veiligheid
Postbus 20301
2500 EH DEN HAAG

Datum: Den Haag, 13 april 2021
Betreft: Internetconsultatie 'Autoriteit KP'

Geachte heer Grapperhaus,

U ontvangt deze reactie op de consultatie "het Wetsvoorstel Wet Bestuursrechtelijke aanpak online kinderpornografisch materiaal" of "Wetsvoorstel"; namens DINL en de bij haar aangesloten partijen. De reactie bevat drie delen, deel I gaat in op de Memorie van Toelichting en een aantal artikelen van het Wetsvoorstel, deel II gaat dieper in op de voorgestelde 'content autoriteit' en in deel III stippen we nog een aantal losse punten aan.

Wat vooraf ging:

We zijn u zeer erkentelijk dat u het volume aan kinderporno ("KP") meldingen mbt KP gehost in Nederland op de kaart hebt gezet. Medio 2018 zijn we op uw initiatief samengekomen voor een meeting om de problematiek gezamenlijk aan te pakken en op te lossen. Uit die bijeenkomst en het vervolg zijn een aantal actielijnen voortgekomen.

Ten eerste is er de verbetering van de gedragscode 'Notice en Takedown" ("NTD"), de regeling die nu vrijwel alle Nederlandse hosting- en internet toegang partijen onderschrijven en hanteren. Onderschrijvers van de NTD spannen zich nu in om binnen 24 uur na een melding van het EOKM, die in het addendum als "trusted flagger" wordt benoemd, de content offline te hebben.

Als tweede actielijn heeft u de TU Delft opdracht gegeven kwantitatief onderzoek te doen naar de hoeveelheid meldingen. Belangrijke vragen als: waar komen de meldingen vandaan, over welke content gaat het, en vooral hoe lang is de content nog steeds beschikbaar *nadat* de melding is verzonden door het EOKM. De verwachting was dat het 'KP' probleem speelde bij veel hosting partijen en dat daarvoor ook een generiek instrument nodig zou zijn om het probleem te tackelen.

Als derde is daarom besloten een 'hash checker' ter beschikking te stellen aan websites die slachtoffer zijn van veel 'KP' uploads. De Politie zou hashes, een soort digitale vingerafdrukken ter beschikking stellen, zodat bepaalde websites, waar het EOKM veel meldingen over krijgt, hun uploads (maar ook al geuploade plaatjes) kunnen checken tegen deze database. Deze service is inmiddels al 18 miljard keer geraadpleegd en dat leverde 7 miljoen 'hits' op.

Als laatste was u erg geïnteresseerd in een zogenoemde 'content autoriteit'. Deze autoriteit hanteert een bestuursrechtelijk handhavingsinstrument om partijen die niet met het EOKM samen werken, toch te dwingen (KP) content offline te halen.

Stichting Digitale Infrastructuur Nederland
Overgoo 13 / Postbus 262
2260 AG Leidschendam
T: +31707621070
E: info@dinl.nl

Na deze kick-off hebben er regelmatig nog verschillende meetings plaatsgevonden, de zogenaamde 'Ronde Tafel KP'. Deze meetings hebben we als sector als erg prettig en constructief ervaren, en los van deze consultatie, vinden we het belangrijk om deze samenwerking permanent te maken - zodat we tijdig en adequaat gezamenlijk kunnen reageren op eventuele nieuwe ontwikkelingen rond deze problematiek.

Deel I : De wetsartikelen en memorie van toelichting

Artikel 1 ("Aanbieder van hostingdiensten"):

De omschrijving van hosting en de toepasselijkheid van artikel 14 van de richtlijn inzake elektronische handel gaat naar ons oordeel voorbij aan de huidige praktijk. In uw definitie is: '*de aard van de aangeboden dienst doorslaggevend. Ook aanbieders wier activiteiten gedeeltelijk bestaan uit hosting zijn derhalve, voor zover zij dergelijke activiteiten ontplooien, aan te merken als aanbieder van hostingdiensten. Onder de reikwijdte van deze definitie vallen onder meer aanbieders van serverruimte zoals datacentra, maar ook social media platforms, video streaming services en internet service providers, voor zover zij op hun* ***eigen servers ruimte aanbieden voor het opslaan van gegevens****, zoals (onderdelen van) websites, losse afbeeldingen of videobestanden. De opslag dient enige duur van betekenis te hebben'* De sleutel ligt daarom bij het begrip 'eigen servers ruimte aanbieden voor het opslaan van gegevens'. Voor shared en managed hosting gaat dit in nagenoeg alle gevallen op, terwijl dit bij dedicated hosting juist niet opgaat.

Unmanaged dedicated hosting partijen leveren in feite een 'Infrastructure as a Service' dienst ("IaaS"). Deze dienst valt uit te splitsen in een aantal componenten: racks+ power+cooling, compute en connectiviteit. De IaaS partij zelf heeft geen logische toegang tot de server van de klant, deze kan dus niet inloggen en een plaatje verwijderen. Omdat de IaaS partij geen wachtwoord van de server heeft zijn de mogelijkheden voor deze intermediair beperkt. De IaaS partij heeft dezelfde mogelijkheden als een access partij: deze kan de verbinding aan/uit zetten, er is geen mogelijkheid om individuele content te verwijderen of ontoegankelijk te maken (zoals bij traditionele hosting). Alleen al daarom valt IaaS onder 'mere conduit', en een verruiming door uw ministerie waarmee ook bepaalde mere conduit partijen onder artikel 14 zouden gaan vallen, in plaats van onder 12 lijkt ons juridisch onhoudbaar.

Om een beroep te doen op 'mere conduit' moet er aan vier voorwaarden worden voldaan: Ten eerste moet het gaan om een dienstverlener die enkel informatie doorgeeft of toegang verleent tot een communicatienetwerk. Ten tweede mag het initiatief tot doorgifte niet uitgaan van de dienstverlener. Ten derde mag de dienstverlener de ontvanger van de doorgegeven informatie niet selecteren. Tot slot mag de dienstverlener de doorgegeven informatie niet wijzigen.

IaaS dienstverleners voldoen aan al deze voorwaarden en vallen derhalve onder artikel 12 en niet onder artikel 14. Het is onbegrijpelijk dat J&V juist deze IaaS partijen aanspreekt terwijl het 'mere conduit' juist deze partijen specifiek uitsluit. Dit bevreemd te meer omdat de gehele top 4 van de TUD monitor over

jan-jun 2020 uit unmanaged dedicated hosting providers bestaat en derhalve dus compleet buiten de reikwijdte van de wet zou vallen.

'Caching services' zijn tevens uitgezonderd in het wetsvoorstel. Daar waar het proxies van access providers betreft lijkt ons dat terecht, maar er zijn ook proxy dienstverleners die images tot een maand 'cachen' (bv 'Cloudflare'). Deze uitzondering levert het risico op dat er bewust misbruik wordt gemaakt van deze caching constructie. Immers indien een 'plaatjesboer' zijn database met plaatjes buiten Nederland plaatst en in Nederland alleen een caching server aanbiedt dan valt deze constructie buiten de reikwijdte van het Wetsvoorstel, terwijl de cached content tot wel 1 maand na verwijdering van de bronbestanden actief toegankelijk kan blijven. De andere vraag die zich voordoet: wie gaat onderzoeken of deze claim (we zijn geen website maar een cache) correct is, is dat dan een impliciete opdracht aan de IaaS partij (die geen toegang heeft tot de gebruikte servers voor caching).

Artikel 1 ("ontoegankelijk maken")

"Blokkering kan bijvoorbeeld aan de orde zijn als ***de desbetreffende aanbieder van een communicatiedienst het niet in zijn macht heeft*** *het materiaal te verwijderen. Om aan de aanwijzing tot ontoegankelijk making te voldoen, dient in een dergelijk geval de blokkering voort te duren zolang het materiaal wordt aangeboden of doorgegeven."* Hier koppelt u de aanbieder van een communicatiedienst los van de 'website', wat op zich goed is. Zoals bij "aanbieder van hostingdiensten" al genoemd: er kan door de aanbieder van een communicatiedienst niet op plaatjes niveau gefilterd worden. De enige mogelijk is de gehele verbinding van de website af te sluiten, met alle proportionaliteits vraagstukken die daarbij horen.

De autoriteit zal (daarom) waarschijnlijk moeten aangeven dat het plaatje op url https://plaatjesboer01.nl/varia/qazxdrthnmkop.jpg ontoegankelijk moet worden gemaakt, maar dat levert voor de aanbieder van een communicatiedienst het probleem op dat hij de gehele server 'plaatjesboer01.nl' moet blokkeren met alle legale content die daarbij dan tevens ontoegankelijk wordt gemaakt. Dat kan gaan om content van andere klanten, die niets met plaatjesboer01 van doen hebben. Het lijkt ons dat de handhavingsactie door de 'content autoriteit' tegen de website 'plaatjesboer01.nl' dient plaatst te vinden en niet primair bij de aanbieder van een communicatiedienst. Mocht de website geen gehoor geven dan pas zou een blokkeringsopdracht van de autoriteit aan de aanbieder van de betreffende communicatiedienst op zijn plek zijn, met dan wel de eventuele gevolgschade voor andere ondernemers of burgers.

U spreekt de hostingpartijen aan terwijl juist de (exploitanten) van deze websites het probleem zijn, en juist zij de oplossing kunnen brengen. Deze websites kunnen gebruikmaken van de hashcheck server om uploads te scannen tegen de database met bekende KP plaatjes, door hun bestaande databases met plaatjes te scannen. Zulke websites zijn 'key' in de strijd tegen KP uploads. De hostingpartij of aanbieder van een communicatiedienst kan u in contact brengen met de website beheerder/eigenaar, typisch de functie die een intermediair vervult.

Artikel 8 ("Zorgplicht"):

In het Wetsvoorstel spreekt u voornamelijk over 'hostingpartijen'. In artikel 8 is dat dan ook al gelijk problematisch, immers de KP content staat bij klanten van een hostingpartij. Deze klant heeft een of meerdere websites en op een of meerdere van die websites staat de gewraakte KP afbeelding. Binnen de richtlijn inzake elektronische handel (het e-commerce directive) is de hostingpartij niet verantwoordelijk voor de content van zijn klant, zolang hij geen weet heeft van deze content.

Er zijn, als eerder toegelicht, ook partijen die niet onder het traditionele hosting artikel vallen maar onder het 'mere conduit' artikel, immers indien een partij alleen een server en/of serverruimte en connectiviteit aanbiedt heeft zij geen logische toegang tot een server en kan derhalve geen plaatje verwijderen. De logische eigenaar van de server is in dat geval de website beheerder. De enige actie die dan mogelijk is voor aanbieder van een communicatiedienst, is om de gehele server af te sluiten, analoog aan de mogelijkheden van een internet toegangsverlener. In beide gevallen bestaat er onder het e-commerce directive geen mogelijkheid tot zelfstandig proactief scannen van content van klanten.

U spreekt hier de hostingpartij aan, terwijl de exploitant van de website zelf de aangesprokene zou moeten zijn, het is immers ook die website beheerder die de hash checker moet gebruiken, niet de hostingpartij.

De vraag die opkomt: Is een policy waarbij een hostingpartij misbruik gevoelige websites verplicht om gebruik te maken van de hash checker voldoende? Of dient de hostingpartij afscheid te nemen van een klant als het volume aan meldingen groot blijft terwijl de website toch gebruik maakt van de hashchecker? Welk volume is dat dan (meer dan 10 meldingen per jaar)? U spreekt over maatregelen, welke andere maatregelen zijn er in uw optiek mogelijk? Als we er vanuit gaan dat de websites slachtoffer zijn, en zelf misbruikt worden voor ongewenste KP uploads, vindt u het dan redelijk om deze legale en meewerkende partijen de toegang tot Nederland te ontzeggen omdat ze een hoog volume aan KP meldingen genereren?

Artikel 9 ("Aanwijzing"):

Met aanbieder van een communicatiedienst wordt wederom niet de website die de betreffende KP afbeelding host bedoeld. Indien het een 'mere conduit' hoster is kan deze zelfs de afbeelding niet zelf weghalen, de enige mogelijkheid is het afsluiten van de verbinding.

Artikel 14 ("Behoud van materiaal"):

Zoals hierboven reeds aangegeven: 'mere conduit' hostingpartijen hebben geen toegang tot de content, zij kunnen derhalve geen materiaal bewaren.

De TU Delft cijfers:

Ten tijde van de kick-off was er een breed gedragen veronderstelling dat het KP-probleem wijd en zijd verbreid was binnen de Nederlandse hosting sector. De cijfers van het TU Delft onderzoek waren een verrassing voor iedereen. Het probleem kan gelokaliseerd worden bij 4 partijen. Deze partijen hosten (tussen januari en juni 2020) 99,45% van alle plaatjes die door het EOKM zijn gemeld.

Deze uitkomst lijkt ons, kortom, juist een reden om de 'content autoriteit' niet op te richten. Immers de #1 uit de lijst is verantwoordelijk voor 93,57% van alle meldingen gedurende bovenstaande periode. Het lijkt ons meer voor de hand te liggen om deze partij aan te sluiten op de hashchecker. Ook zou kunnen worden gekeken waarom deze partij zoveel meldingen ontvangt, specialiseert deze partij zich in legale maar vatbare sites, de zgn 'plaatjesboeren'?

Het overgrote deel van de sector voldoet aan de vrijwillige NTD regeling incluis KP addendum. De partijen die dat niet doen worden pas sinds kort publiekelijk benoemd. Dat "namen en shamen" helpt, blijkt uit de reacties van genoemde partijen en de vragen die de sectororganisaties hebben gekregen over het rapport. Zou het niet verstandig zijn om het effect van de reeds genomen maatregelen af te wachten? Het lijkt er sterk op dat een autoriteit helemaal niet nodig is.

Afsluitend, concluderen wij dat er **geen dwingende noodzaak** voor een content autoriteit bestaat. Uit de overleggen met uw ministerie is ons overigens duidelijk geworden dat de voorgestelde 'content autoriteit' zich naast KP ook bezig zal houden met Terroristische Content Online ("TCO").

Deel II : De content autoriteit

Artikel 2 ("Autoriteit aanpak online kinderpornografisch materiaal")

Indien U toch persisteert in het oprichten van een 'content autoriteit', die zich ook met KP bemoeit, dan geeft naar onze mening een ZBO constructie de juiste afstand tot de dagelijkse politiek, en is de directe politiek sturing op voldoende afstand geplaatst. Omdat regulering en verwijdering van content nauw verwant is met de grondwettelijk verankerde uitingsvrijheid en censuurverbod komt het ons verstandig over dat deze activiteit met alle waarborgen omkleed, ver van de politieke waan van de dag te houden.

In de discussies bij de 'Ronde Tafel' is zowel door J&V, het EOKM en de private partijen opgemerkt dat hier sprake moet zijn van een nauwe samenwerking, eerder een partnership dan een handhaver die vanuit een ivoren toren poogt de wereld te veranderen. De 'content autoriteit' verricht zijn taken en bevoegdheden in samenwerking met bovenstaande relevante ketenpartners. Wij pleiten dan ook voor een personele invulling die recht doet aan de uniciteit van dit project: om de samenwerking met de ketenpartners succesvol te maken is het nodig dat de autoriteit diepgaande kennis van de werking van het internet, de positie van de ketenpartners in het ecosysteem en de beperkingen van het wettelijk stelsel verkrijgt. Iemand die het verschil begrijpt tussen 'Nee (dat kan niet)' en 'Nee (dat wil ik niet). Vertrouwen speelt dan ook een grote rol, vertrouwen in de mensen geeft ook vertrouwen in de organisatie en verankert daarmee de keten. Wij geven ook mee, dat hier sprake is van een unieke manier van

aanpakken van onrechtmatige content, en dat vereist van de betrokkenen creativiteit, flexibiliteit en inzet op samenwerking met niet-overheidspartijen. De personele invulling moet dat profiel weerspiegelen.

Tijdens de 'Ronde Tafel' is gesproken over een Raad van Advies ("RvA"). Er is een briefing geweest over dit element maar we zien de RvA niet terugkomen in het Wetsvoorstel. Voor de private partijen is de RvA wel een vereiste, het is voor ons het gremium waarin de gemaakte afspraken over de manier waarop de 'content autoriteit' zijn bevoegdheden uitoefent geborgd worden. Zonder deze toegezegde RvA zal het, voor de private partijen, erg moeilijk zijn om de 'content autoriteit' een vliegende start qua vertrouwen te laten maken, en om te acteren in de geest van deze aanpak: een continue, privaat-publieke samenwerking.

Verder maken we ons zorgen over de reikwijdte van het Wetsvoorstel. Vanwege de keuze voor het bestuursrecht is deze reikwijdte beperkt tot in Nederland gevestigde dienstverleners. Dat betekent dat juist die bedrijven die zich niet aan de NTD houden én (bij monde van Arda Gerkens, directeur EOKM), niet bereidwillig zijn om de problematiek in hun netwerken aan te pakken, niet onder de wetgeving vallen. Terwijl u steeds aangeeft dat de autoriteit het vangnet is als andere maatregelen falen. Als we de top-4 van begin 2020 nemen, dan zijn 2 van de 4 bedrijven in het buitenland gevestigd (UK en Seychellen), deze bedrijven vallen derhalve buiten de reikwijdte van het gekozen instrument. Het lijkt ons dan ook om deze reden niet doelmatig om specifiek voor dit bestuursrechtelijke instrument te kiezen.

Volledigheidshalve dient opgemerkt te worden dat de Nederlandse hostingmarkt (alle vormen van hosting; shared/traditionele hosting, IaaS/'mere conduit' en CDN/caches) erg internationaal is en werkt met zgn. 'resellers'. Dit zijn vaak buitenlandse partijen die zelf resources bij een IaaS partij inkopen (voor eigen rekening en risico) en die dan doorverkopen aan een eigen (buitenlandse) achterban. De reikwijdte van het voorstel voor deze groep ondernemingen is potentieel eveneens flink beperkt.

Als laatste hebben we tevens bezwaren tegen de verplichte openbaarmaking van sommige boetebeschikkingen op een moment dat zelfs de bezwaartermijn nog niet is verstreken, laat staan de beschikking onherroepelijk is geworden. DINL meent dat een verplichting tot openbaarmaking te ver gaat, en zeker als dat gebeurt op een moment dat de juistheid van die beschikking niet onherroepelijk is komen vast te staan.

Deel III : De additionele relevante zaken en randvoorwaarden

De TU Delft methodiek:

Het percentage niet tijdig verwijderd materiaal zoals het in het TU Delft rapport en in de MvT vermeld staat is te hoog. De oorzaak is dat de methodiek en het proces van versturen en informatie over afhandeling van meldingen nog gebreken en tekortkomingen heeft, die verbetering behoeven. Het probleem is (daardoor) in werkelijkheid iets kleiner dan in de cijfers tot uiting komt. Het zou u sieren als in de memorie van toelichting alsnog het juiste percentage wordt benoemd. Wel vinden we dat de TU Delft studie moet worden voortgezet, de meetmethode moet worden verbeterd, waarbij het uiteraard vanzelfsprekend is dat steeds ook met input en werkwijze van de sector rekening wordt gehouden - om zo de cijfers beter, betrouwbaarder te maken. En daarmee ook acceptabel te maken voor degenen die zich daadwerkelijk stevig inspannen en nu vanwege de gebreken, ondanks hun inzet alsnog worden aangemerkt als nalatig.

Technische bezwaren:

De autoriteit mag zelf gaan crawlen. Maar in onze optiek zou dit beter passen bij het EOKM. Zij staat dichter bij de sector, de meldingen vanuit EOKM worden door de sector goed opgevolgd. In de huidige systematiek doet het EOKM de initiële melding, pas indien er geen of een te late reactie komt, is de 'content autoriteit' aan zet. Het lijkt niet logisch om de 'content autoriteit' een duale functie te geven: als meldingen via het EOKM binnenkomen speelt ze achtervang; als meldingen, zelf via de 'crawler' worden gevonden, handelt ze ze zelf af, of meldt ze via het EOKM door. We hebben een sterke voorkeur voor een standaard meldingen proces, en een beperkte rol als "achtervang" voor de content autoriteit.

Een ander bezwaar tegen crawlen is dat je alleen daar materiaal vindt, waar je gaat zoeken. Dat kan leiden tot algoritme bias of zelfs rechtsongelijkheid. Transparantie over de plaatsen waar de crawler zoekt en het gebruikte algoritme moet derhalve goed geregeld zijn.

In de MvT wordt benoemd dat de 'content autoriteit' mogelijk geautomatiseerd materiaal als KP bestempeld bijvoorbeeld omdat er een hit is op de hashcheckservice. Die service werkt (nu) met algoritmes waar het risico op zgn. "collisions" aanwezig is. Een collision is een plaatje dat dezelfde hash oplevert zonder dat het dezelfde 'afbeelding' is. Het opzettelijk plaatsen van niet-KP plaatje dat dezelfde MD5 of SHA-1 hash geeft dan KP plaatje is een risico op een zgn. 'denial of service' aanval. Een voorwaarde automatische detectie is dat onomstotelijk vastgesteld kan worden dat iets KP is, want verifiëren van beelden door medewerkers is volstrekt onwenselijk, en feitelijk zelfs verboden. Eventueel zou je naast de MD5/SHA-1 hash ook de bestandsgrootte kunnen meenemen. Ook dit geeft aan, dat continue (door)ontwikkeling van de gebruikte methoden noodzakelijk is.

EOKM:

De belangrijke positie van het EOKM is hierboven vaak ter sprake gekomen, helaas hebben we in het Wetsvoorstel geen enkele aanwijzing gevonden over de financiering van dit cruciale instituut. Dat is buitengewoon zorgwekkend. De 'content autoriteit' is het sluitstuk in een keten waar het EOKM de meeste meldingen verwerkt, de nauwste contacten met de sector heeft, een track record

heeft als betrouwbare partner, en in de code of conduct NTD, één van de pijlers van de aanpak, wordt benoemd en aangewezen als "trusted flagger". Het is volstrekt onduidelijk hoe de 'content autoriteit', en het hele systeem van melden en verwijderen, überhaupt kan functioneren zonder het EOKM. Het is voor ons dan ook ongepast om dit Wetsvoorstel te doen en daarbij de financiële positie - en daarmee de continuïteit van het EOKM niet mee te nemen.

Het EOKM faciliteert bovendien twee van de drie overige actielijnen die we hebben ontwikkeld binnen onze samenwerking, te weten de hashcheckservice en (de input/cijfers voor) de TU Delft monitor. Gezien de workload en de financieringsbehoefte van de 'content autoriteit' zou een 'matching funding' voor het EOKM voldoen aan een reële behoefte, maar dit lijkt politiek nu steeds niet haalbaar. EOKM heeft jaar-op-jaar moeite om haar financiering rond te krijgen. We vragen dan ook om een structurele oplossing, waarbij het EOKM kan beschikken over een budget van minimaal 1 miljoen euro per jaar, voor een langere termijn (minimaal 5 jaar) zodat de essentiële rol van het EOKM als ketenpartner geborgd is. Dit is dan exclusief een IT refresh (voor eenzelfde bedrag) waarbij de systemen van het EOKM en de 'content autoriteit' aan elkaar worden geknoopt en deze systemen, **inclusief databases**, ook Europees/wereldwijd beschikbaar worden gemaakt. Zodat elk land de technische mogelijkheid heeft om een hash checker aan te bieden aan daar gehoste websites.

Conclusie:

Als sector, zijn we gemotiveerd in deze samenwerking gestapt. We hebben steeds de *mogelijke* noodzaak voor een toezichthouder open gehouden, als eventuele stok achter de deur, indien dat noodzakelijk zou blijken. We hebben steeds het belang van – en inzet op alle pijlers gesteund, de integrale aanpak.

Maar, nu blijkt dat meer dan 93% van de meldingen bij **1 hoster** vandaan komen, moet e conclusie zijn dat er geen toezichthouder nodig is. Een NS retourtje Den Haag - Roosendaal volstaat. Verder, wilt u een bestuurlijk handhavingsinstrument om dat strafrechtelijke handhaving te veel tijd kost, echter 50% van de top 4 valt buiten de reikwijdte van dit instrument. U adresseert hosting partijen, maar de meldingen genererende websites staan bij 'mere conduit' partijen, die u specifiek uitsluit. U sluit ook caching services uit en opent daarmee de deur voor een legale u-bocht om de content toch in Nederland te hosten.
Het geheel wekt de indruk, dat beleidsdoelen voorop staan, en niet de realiteit en effectiviteit. Zo span je eigenlijk het paard achter de wagen.

Riskant en zelf contra-productief is dat u met dit wetsvoorstel niet de pijlers van de aanpak: het EOKM, hashcheck en de meetmethodes; en de continuiteit van die instrumenten. Zonder die randvoorwaarden kan onze gezamenlijke aanpak niet functioneren.

Hostingbedrijven zijn voor meldingen immers volledig afhankelijk van de continuïteit van het EOKM, en van een goed werkende hash-database. Er zijn voor deze bedrijven geen andere mogelijkheden, omdat ze hun personeel niet mogen en niet kunnen vragen om deze beelden te inspecteren en te beoordelen. Daarnaast is het gehele stelsel afhankelijk van de kwaliteit en continuïteit van de metingen: waar zijn er eventuele (nieuwe) hotspots, en hoe meet de toezichthouder anders de snelheid waarmee bedrijven reageren op de meldingen

van het EOKM. Ook valt of staat werking van het stelsel met de continue verbetering van functies, die in dit vroege stadium van ontwikkelingen nog tekortkomingen hebben. De continuïteit van deze gedeelde, gezamenlijke faciliteiten, alsmede de continue verbetering ervan - is een harde randvoorwaarde voor succesvolle bestrijding van KP. Daarom dient een nieuw voorstel de continuïteit daarvan te adresseren, en te borgen.

Als sector willen we ons blijvend inzetten om samen met de U dit schadelijke beeldmateriaal uit Nederland te weren. We rekenen daarom op een zodanige verbetering van eventuele juridische instrumenten, dat deze gezamenlijke doelen blijvend worden gediend.

Vanzelfsprekend zijn wij bereid tot - en beschikbaar voor een nadere toelichting,

Namens DINL en haar deelnemers,

Michiel Steltman
Directeur