Bureau Beke

dialogic
innovatie • interactie

Mogelijkheden voor het aanpakken van kinderporno op basis van bestuursrechtelijke handhaving

Projectnummer:
2019.016

Publicatienummer
2019.016-1908

Datum:
Utrecht, 12 april 2019

Auteurs:
Jessica Steur
Tommy van der Vorst
Anton van Wijk
Menno Driesse
Wazir Sahebali

Inhoudsopgave

Managementsamenvatting

In dit rapport worden de technische en feitelijke stappen beschreven om online kinderporno te verwijderen onder de toepassing van bestuursdwang. Dit onderzoek is uitgevoerd in het kader van de 'hernieuwde aanpak online seksueel kindermisbruik'.

Om de forse stijging in het aantal meldingen van online kinderporno het hoofd te bieden, bevat de hernieuwde aanpak online seksueel kindermisbruik tevens publiek-private actiepunten. Eén van de actiepunten betreft het onderzoeken of de bestuursrechtelijke handhaving (specifiek last onder bestuursdwang) een uitkomst kan bieden. Dat is de focus van dit onderzoek.

Kinderporno moet zo snel mogelijk van internet worden verwijderd. De meeste ICT-bedrijven hebben dit materiaal ongewild en incidenteel op websites of servers staan en verwijderen dit dan ook nadat een melding daarover is gedaan door het Meldpunt Kinderporno (EOKM). Bij wijze van zelfregulering is daarvoor een gestructureerd proces ontworpen dat zoveel mogelijk aansluit bij processen van zelfregulering binnen de sector (notice-and-takedown-procedure). Zelfregulering van de sector (specifiek Internet Service Providers en Hosting Service Providers) voor het verwijderen van online kinderporno werkt goed voor het afhandelen van de meerderheid van de meldingen vanuit het EOKM. Content wordt vrijwillig en in essentie binnen 24 uur verwijderd. Een kleine groep bedrijven werkt echter niet of onvoldoende mee (zogenaamde 'bad hosters'). Binnen het ministerie van JenV wordt gekeken naar bestuursrechtelijke mogelijkheden om deze groep aan te pakken. Uit onderzoek blijkt dat het juridisch haalbaar is om met last onder bestuursdwang een ICT-bedrijf als rechtspersoon aan te pakken, waarbij rekening wordt gehouden met de mogelijkheid dat er sprake is van ongewilde medewerking door het ICT-bedrijf. In dat geval zorgt een toezichthouder er zelf voor dat de kinderporno wordt verwijderd of ontoegankelijk wordt gemaakt. In dit onderzoek wordt inzicht verkregen in de technische mogelijkheden van het toepassen van bestuursdwang.

Een instrument op basis van bestuursrecht kan worden gepositioneerd tussen de huidige notice-and-takedown-procedure vanuit de zelfregulering en het strafrecht. Het stelt een toezichthouder in staat om harder op te treden in geval er (herhaaldelijk) door eenzelfde partij niet of traag wordt meegewerkt aan een verwijderverzoek. Bestuursrecht kan louter worden toegepast op partijen die acteren op Nederlands grondgebied.

Vanwege de stapeling van diensten in de ICT-sector valt het toepassen van bestuursdwang uiteen in twee processen:

1. Het *identificeren* van de partij waarop bestuursdwang kan worden toegepast;
2. Het daadwerkelijk *toepassen* van bestuursdwang, ofwel het verwijderen van de content.

De keten in beeld

Het internet bestaat uit aan elkaar gekoppelde computernetwerken (*autonomous systems*) waaraan computers en andere netwerkapparaten zijn gekoppeld. Via het internet bieden contentleveranciers data aan gebruikers aan. Om deze content te leveren wordt er gebruik gemaakt van de diensten van derden. Zo biedt een datacenter ruimte aan een aanbieder van servers aan, die zijn servers weer aanbiedt aan een webhoster. De webhoster bedient vervolgens een aanbieder van websites of webdiensten. Content, zoals kinderporno, is dan

te vinden op een website, die fysiek staat opgeslagen op een server in een datacenter. Er zijn echter diverse variaties mogelijk, wat het zeer lastig kan maken de keten in beeld te krijgen.

Er zijn drie routes mogelijk om van website tot (fysieke) opslagplaats van de content te komen:

1. *Contactinformatie.* Op een website wordt soms de contactinformatie vermeld van de beheerder van de website of de hostingpartij. Deze partijen hebben toegang tot de content en kunnen deze verwijderen.
2. *Domeinregistratie.* Elke domeinnaam staat geregistreerd onder de naam van een persoon of bedrijf. Op deze manier kan mogelijk de hostingpartij of de website-eigenaar worden achterhaald.
3. *IP-adres.* Via het IP-adres van de website kan met behulp van de internetdienstverlener de hostingpartij of de datacenterlocatie van de server worden achterhaald. In het datacenter kan dan eventueel de server worden uitgeschakeld.

In uitzonderlijke gevallen is identificatie van de juiste partij bijna onmogelijk vanwege ingewikkelde constructies (vaak met buitenlandse partijen). In die gevallen kan niet worden vastgesteld waar de content wordt gehost, en is het niet mogelijk bestuursdwang toe te passen.

Verwijderen van de content

Afhankelijk van de positie in de keten van de geïdentificeerde partij, zijn er verschillende acties te ondernemen. Van de precieze content tot een heel datacenter kunnen de volgende elementen worden verwijderd of uitgeschakeld:

- Content
- Server proces
- Besturingssysteem
- Server en aanverwante hardware
- Rack, cage, vloer
- Connectiviteit datacenter

Er zijn twee manieren om kinderporno te verwijderen: via logische toegang tot de content (waarbij inloggegevens vereist zijn) of via fysieke toegang tot de server. Met logische toegang kan zo precies mogelijk de content worden verwijderd. Dat zorgt voor de minste nevenschade, maar is zonder medewerking van de betreffende partij haast onmogelijk. Dat betekent dat de last onder bestuursdwang eigenlijk altijd wordt opgelegd aan een partij met fysieke toegang. De toezichthouder schakelt dan zelf de hardware uit. Dan spelen ook meer praktische uitdagingen, zoals een datacenter binnentreden en de juiste server of het juiste rack vinden. Vooral de locatie van de server in een datacenter bepalen is een struikelblok. Zonder enige informatie (en dus medewerking van 'dieperliggende' partijen in de keten, zoals een datacenterexploitant) over in welk(e) rack/cage/hal de server zich bevindt, is het voor een toezichthouder bijna onmogelijk om bij de specifieke server met kinderporno te komen. Wanneer op geen enkele manier wordt meegewerkt, komt een toezichthouder al snel uit bij extreme acties, zoals het uitschakelen van de connectiviteit richting een datacenter.

In het gunstigste scenario van fysieke toegang wordt één server ontoegankelijk gemaakt of verwijderd. De precieze nevenschade hiervan is moeilijk te bepalen, omdat zonder logische toegang (of bijvoorbeeld monitoring van het verkeer) onbekend is hoeveel websites en andere diensten vanaf de betreffende server worden aangeboden. Hierbij geldt dat hoe 'dieper' men in de keten komt, hoe minder precies kan worden bepaald waar de content

staat en hoe groter de potentiële nevenschade (tot aan het uitschakelen van de connectiviteit richting een datacenter).

Implementatie

We verwachten dat er een positief effect uit zal gaan van de 'dreiging' van bestuursdwang – namelijk dat dienstverleners eerder en sneller zullen meewerken aan een verwijderverzoek. In de praktijk wordt bestuursdwang wel nadrukkelijk gezien als middel om de resterende kleine groep 'bad hosters' aan te pakken.

1 Inleiding

In dit hoofdstuk beschrijven we allereerst de aanleiding van dit onderzoek naar de (technische) mogelijkheden van overheidshandelen in de uitvoeringspraktijk bij de bestuurlijke aanpak kinderporno (paragraaf 1.1). Vervolgens worden de doelstelling en beoogde resultaten behandeld (paragraaf 1.2) en presenteren we de onderzoeksaanpak (paragraaf 1.3). Afsluitend is er een leeswijzer voor dit rapport toegevoegd (paragraaf 1.4).

1.1 Achtergrond en aanleiding voor het onderzoek

De 'hernieuwde aanpak online seksueel kindermisbruik'[1] is – naast al bestaande actiepunten voor opsporing – verbreed, en bevat nu tevens preventieve actiepunten en publiek-private actiepunten. Dit om de groei van het aantal meldingen van kinderporno bij de politie in te dammen. Het gaat namelijk om een forse stijging van ongeveer 3.000 in 2014 naar bijna 18.000 in 2017.[2]

Onder de publiek-private actiepunten wordt onder meer gekeken naar zelfregulering van de sector[3], monitoring van de beschikbaarheid van het strafbare materiaal (verspreiding en uptime)[4], de hashdatabase met codes van het bekende materiaal en de bestuursrechtelijke handhaving. Dit laatste betreft de focus van dit onderzoek.

Kinderpornografisch beeldmateriaal (hierna: kinderporno) moet zo snel mogelijk van internet worden verwijderd. De meeste ICT-bedrijven hebben dit materiaal ongewild en incidenteel op websites of servers staan en verwijderen dit dan ook nadat een melding daarover is gedaan door het Meldpunt Kinderporno (www.eokm.nl).[5] Bij wijze van zelfregulering is daarvoor een gestructureerd proces ontworpen dat zoveel mogelijk aansluit bij processen van zelfregulering binnen de sector.[6]

Een kleine groep bedrijven werkt echter niet of onvoldoende mee. Binnen het ministerie van JenV wordt gekeken naar bestuursrechtelijke mogelijkheden om deze groep aan te pakken. Uit onderzoek van AKD[7] blijkt dat het juridisch haalbaar is om met last onder bestuursdwang een ICT-bedrijf als rechtspersoon aan te pakken, waarbij rekening wordt gehouden met de mogelijkheid dat er sprake is van ongewilde medewerking door het ICT-bedrijf.

Last onder bestuursdwang is een herstellende sanctie; het oogmerk is om de overtreder te bewegen om een overtreding ongedaan te maken of om herhaling van de overtreding te voorkomen. De overtreder krijgt eerst zelf de gelegenheid om de overtreding ongedaan te maken. Doet hij dat niet (tijdig), dan beëindigt de overheid de overtreding zelf.

---

[1] Tweede Kamer (7 februari 2018). Kamerbrief over hernieuwde aanpak online seksueel kindermisbruik.

[2] Het betreft burgermeldingen, aangiftes en meldingen via NCMEC, waarbij de laatste relatief het grootst is. Voor 2018 worden 30.000 meldingen verwacht.

[3] Onder meer in de gedragscode Notice and Takedown en de gedragscode abusebestrijding.

[4] Onderzoek uitgevoerd door de TU Delft.

[5] Zij ontvangen meldingen via het online meldpunt (www.eokm.nl), maar ook via buitenlandse organisaties.

[6] Notice and Takedown en Code of Conduct, incl. addendum.

[7] AKD (27 november 2018). Haalbaarheidsstudie bestuursrechtelijke aanpak van kinderporno. Bijlage van Kamerstuk II 2018/19, 31 015, nr. 160.

Vertrekkend vanuit dit advies zijn twee trajecten gestart:

1. Welke (nieuwe) toezichthouder zou geschikt zijn voor de uitvoering van bestuursdwang? Dit onderzoek wordt uitgevoerd door het ministerie van JenV.
2. Inzicht in de (technische) mogelijkheden van de uitvoeringspraktijk. Het beeldmateriaal wordt gehost op servers die mogelijk in bezit zijn van hostingbedrijven. Op dezelfde servers kan tegelijkertijd tal van legitieme websites worden gehost. De gehele server verwijderen kan ongewenste gevolgen hebben en daarom is behoefte aan een optimaal proportioneel alternatief. Dat is de focus van dit onderzoek. Wij maken hier inzichtelijk hoe het handelen bij een last onder bestuursdwang er in de uitvoeringspraktijk (technisch en praktisch) uit kan zien.

Met de gezamenlijke adviezen kan de minister van JenV besluiten of een wetgevingstraject kan worden gestart om een bestuursrechtelijke toezichts- en sanctiebevoegdheid te regelen. Het strafrecht zal in dat geval immer als ultimum remedium dienen, voor het geval dat een bestuursrechtelijke interventie onvoldoende uitwerking op een bepaald bedrijf heeft.

1.2 Doelstelling en onderzoeksvragen

De doelstelling van dit onderzoek is na te gaan wat de mogelijkheden voor toepassing van bestuursdwang in de praktijk zijn.

De hoofdvraag van dit onderzoek luidt:

> *Welke (technische en feitelijke) stappen worden bij overheidshandelen in de uitvoeringspraktijk doorlopen, in het geval van toepassing van bestuursdwang door een toezichthouder, om kinderporno te verwijderen?*

Wij kijken daarbij nadrukkelijk naar de *keten van partijen* die betrokken zijn bij het beschikbaar maken van de content. Wie heeft welke (technische) mogelijkheden tot zijn beschikking tot blokkade/verwijdering van de content, wat zijn daarvan de kosten en hoe groot is de 'nevenschade'?

De hoofdvraag valt uiteen in de volgende deelvragen:

1. Geef een heldere beschrijving van de sector waar de bestuursdwang zich op richt. Maak daarbij onderscheid tussen de typen bedrijven waar deze content kan worden aangetroffen, type (hosting)diensten, -contracten, -relaties. Geef passende definities.

2. Geef aan welke feitelijke stappen en technische handelingen een toezichthouder moet doorlopen om kinderporno zelf, door feitelijk handelen, van een server van een (hosting)bedrijf te verwijderen. Geef opties per type bedrijf, dienst, contract en relatie.

3. Maak inzichtelijk tot welk niveau het feitelijk overheidshandelen kan strekken: bijvoorbeeld tot het niveau content, of website, of server, of bedrijf. Geef aan welke invloed encryptie op dit proces heeft.

4. Geef aan wat onbedoelde nevenschade kan zijn per niveau en hoe deze schade kan worden geminimaliseerd.

5. Geef een onderbouwde schatting van de kosten per overheidshandelen.

6. Geef een inschatting van het equipment en kennisniveau dat een professional van een toezichthouder moet hebben om deze vorm van bestuursdwang uit te oefenen.

7. Geef aan in hoeverre de uitvoering van bestuursdwang in praktische en technische zin haalbaar is.

1.3 Onderzoeksaanpak op hoofdlijnen

Voor het beantwoorden van de onderzoeksvragen hebben we een literatuurstudie uitgevoerd en interviews gehouden. De literatuurstudie had als doel het bestuderen van de (werking van de) keten, de technische mogelijkheden en de vergelijking met de werkwijze in andere landen. In de interviewronde (n=24) hebben we verschillende personen gesproken (o.a. van politie, EOKM, brancheverenigingen en hostingproviders, zie Bijlage 1 voor een overzicht van de gesprekspartners). Centraal in de interviews stonden de technische mogelijkheden en de impact en nevenschade.

1.4 Leeswijzer

In hoofdstuk 2 beschrijven wij de problematiek en de positie die bestuursrecht zou innemen in de huidige situatie. Hoofdstuk 3 bevat een beschrijving van de sector waar bestuursdwang zich op kan richten. In hoofdstuk 4 gaan we in op de feitelijke stappen en technische handelingen die een toezichthouder zou moeten doorlopen om kinderporno te verwijderen en wat hiervan de nevenschade is, wat de kosten zijn en welke kennis en equipment nodig is. Hoofdstuk 5 plaatst enkele kanttekeningen bij de implementatie van handhaving op basis van bestuursrecht. De conclusie en aanbevelingen worden besproken in hoofdstuk 6. In bijlage 1 geven wij een overzicht van de interviewpartners.

2 Verspreiding en bestrijding van kinderporno

In dit hoofdstuk beschrijven we de criminologische achtergrond van de problematiek. Wat weten we over de wijze waarop kinderporno wordt verspreid (paragraaf 2.1) en hoe wordt dit tegengegaan (paragraaf 2.2)? Ook geven we aan welke positie het bestuursrecht zou innemen in de huidige situatie (paragraaf 2.3).

2.1 Kinderporno op internet

Het internet draagt in belangrijke mate bij aan het faciliteren en in standhouden van de vraag naar en aanbod van kinderporno. Downloaders kunnen gemakkelijk foto's en video's verzamelen, verspreiden of deel uitmaken van besloten kinderpornonetwerken. De toegankelijkheid van het materiaal en de grote mate van anonimiteit zijn hierbij belangrijke factoren. *Dé* downloader van kinderporno bestaat niet. De literatuur laat een brede variatie zien wat betreft kenmerken en achtergronden.[8]

De diversiteit geldt voor zowel hun kenmerken en achtergronden als de wijze waarop zij kinderporno verspreiden. Overigens gaat in de praktijk het verspreiden van kinderporno vaak samen met het downloaden ervan, soms ook met het vervaardigen ervan. Sommigen downloaden kinderporno om het uitsluitend te bekijken. Anderen verspreiden daarentegen wel.

Het verspreiden kan van bescheiden omvang zijn. Een voorbeeld is een man die via een datingssite in contact komt met een andere man die hem kinderporno toestuurt. Na verloop van tijd komen er nog twee personen bij, die elkaar kinderporno toesturen. Veelal betreft het geen nieuw materiaal.

Anderen verspreiden binnen besloten netwerken. Binnen die netwerken wordt wel 'nieuw' materiaal uitgewisseld. Nieuw wil in dit verband zeggen dat het niet bij de politie bekend materiaal is. In bepaalde gevallen maken de verspreiders eigen opnamen van het misbruik om die vervolgens te delen. De druk op het aanleveren van nieuw materiaal kan groot zijn vanwege de sociale druk binnen de netwerken. Het verspreiden kan op verschillende manieren gebeuren, zoals via e-mail, nieuwsgroepen, WhatsApp of Skype. Er is – voor zover bekend - geen wetenschappelijke literatuur voorhanden waaruit blijkt op welke wijzen zij het materiaal verspreiden en welke ontwikkelingen zij daarin doormaken. Wel is duidelijk dat een bepaald deel – verondersteld wordt degenen die in de besloten netwerken zitten – over goede technische kennis beschikken, elkaar daarvan op de hoogte brengen en daardoor uit handen van politie en justitie blijven.

Kinderpornografie draait veelal niet om het geld, omdat het voor de afnemers een intrinsieke behoefte vervult. Imagehostingspartijen – veel afbeeldingen worden geüpload via imagehosters[9] – zien er echter wél geld in en zetten constructies op met premium (afgeschermde) accounts. Hierdoor wordt opsporing van de afbeeldingen bemoeilijkt.

---

[8] Zie Van Wijk et al. (2019) voor meer informatie over downloaders.

[9] 87% van de illegale content staat op image hosting services. Bron: Jaarverslag EOKM 2018.

2.2 Bestrijding van kinderporno

Een niet-geaccepteerde seksuele geaardheid is niet strafbaar en vooral een maatschappelijk probleem. Het bekijken of verspreiden van kinderporno is wel strafbaar. Binnen de politie houdt het Team ter bestrijding van Kinderpornografie en Kindersekstoerisme (TBKK) van de Landelijke Eenheid zich bezig met deze problematiek. Zij krijgen meldingen binnen over personen die strafbare feiten plegen. Het TBKK heeft te weinig capaciteit om alle meldingen af te handelen. De focus ligt op misbruikers, producten en sleutelfiguren op het darkweb[10] die fora in de lucht brengen of een trekkende rol vervullen op een omgeving. De TBKK-organisatie pakt thans de 500 grootste verdachten op. De restgroep blijft gestaag groeien. Over deze groep heeft de politie relevante informatie, maar dat mag vooralsnog niet gedeeld worden buiten het strafrechtelijk traject.[11]

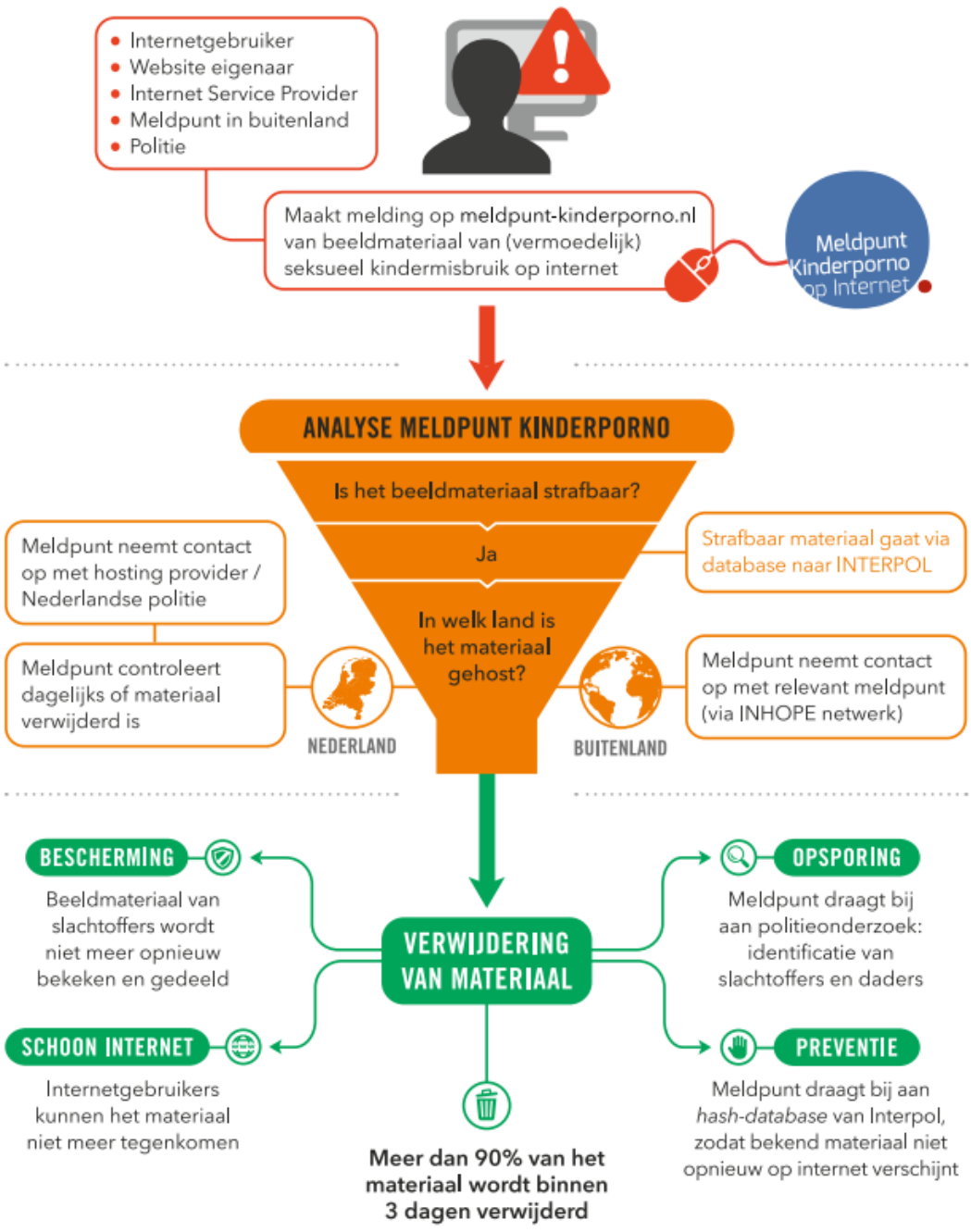
Bij het offline halen van content neemt de politie contact op met de supportafdeling van het betreffende bedrijf. Grotere bedrijven hebben hier een speciaal abuse-loket voor ingericht. Deze loketten gaan over het offline halen van content, ongeacht de materie (dus dit betreft ook illegale films, malware, etc.). Bij kleinere bedrijven wordt er meestal contact opgenomen met de eigenaar, die het zelf afhandelt. Hierdoor gaat het materiaal er via deze weg soms zelfs sneller af. In het geval van filesharingdiensten als Dropbox wordt er een aanvraag ingediend om het account offline te halen en alle data van het account over te dragen. In Nederland wordt volgens de gesproken respondenten op eerste vordering van de politie eigenlijk altijd meegewerkt als de politie vraagt om het aanleveren van informatie of het verwijderen van content. Na een melding bij het bedrijf wordt online de bereikbaarheid van de website gecontroleerd. Indien nodig gaat de politie naar een datacenter toe om de servers op locatie uit te lezen of in beslag te nemen.

Waar de politie meldingen ontvangt over personen, ontvangt het EOKM (Expertisecentrum Online Kindermisbruik) meldingen over websites met illegale content. Het doen van takedownverzoeken van webpagina's is uitbesteed aan deze stichting. Het EOKM[12] is voortgekomen uit het in 1995 opgerichte Meldpunt Kinderporno. Dit Meldpunt was een initiatief van de Nederlandse internet service providers (ISP's), die kinderporno op hun netwerken niet accepteerden, maar zich niet wilden (of konden) bezighouden met de inhoud. Het doel van het Meldpunt is het verwijderen van content in Nederland op basis van meldingen in een notice-and-takedown-procedure (NTD). In Figuur 1 wordt de werkwijze van het EOKM weergegeven.

[10] De politie kijkt beperkt naar het open internet. Hier richt het EOKM zich op.

[11] Op internationaal niveau is er bij Interpol wel een zogenaamde "Worst of"-list, met verdachte webpagina's en domeinen. Na onderzoek door WODC is er vanuit JenV besloten hier niets mee te doen.

[12] Naast het Meldpunt ontplooit het EOKM ook andere activiteiten, zoals 'Stop it now' (een hulplijn voor personen met gevoelens voor kinderen) en 'Help wanted' (voor slachtoffers van kindermisbruik).



Figuur 1. Werkwijze EOKM. Bron: Jaarverslag EOKM 2016.

In 2018 verwerkte het EOKM 224.173 meldingen.[13] Een 'melding' is een specifieke URL, waarop zich één of meerdere afbeeldingen kunnen bevinden. Wanneer het EOKM een melding ontvangt wordt deze beoordeeld en, indien het om kinderporno gaat, getraceerd waar de URL wordt gehost (hierbij wordt gewerkt met tussenliggende Content Delivery Network (CDN)-partijen, zoals CloudFlare). Wanneer een melding 'uitkomt' in een ander land, zal dit via het INHOPE-netwerk worden doorgegeven aan de aangesloten organisatie

[13] Volgens INHOPE is Nederland hostingland nr. 1 op het gebied van kinderporno binnen Europa (met een aandeel van 51% in 2017) en nr. 2 wereldwijd (met een aandeel van 19% in 2017). Bron: www.inhope.org

in het betreffende land. Het overgrote deel van de Nederlandse hosters haalt kinderporno op verzoek direct weg – sommige van hen varen blindelings op de verzoeken van het EOKM. Een deel van de hosters moet herhaaldelijk worden herinnerd, maar verwijdert uiteindelijk wel. De redenen hiervoor lopen uiteen; mogelijk is het eigen proces niet goed ingericht, is er weinig capaciteit op de abusedesk, of (in extreme gevallen) een belang om te vertragen. Het gedrag van de partijen over tijd is redelijk constant: het EOKM kan 'goede' en 'slechte' hosters onderscheiden. Er zijn momenteel geen cijfers bekend – de monitor die wordt gebouwd door de TU Delft zal hier binnenkort duidelijkheid over kunnen geven[14] – maar een grove schatting is dat er in Nederland een tiental bad hosters zijn die ófwel volledig weigeren te handelen naar een verwijderverzoek, ófwel vertragen en in discussie gaan voor zij het materiaal uiteindelijk offline halen.

Er kan discussie ontstaan over wat kinderporno is en wat niet. Een hoster kan dit als argument gebruiken om niet aan een verwijderverzoek te voldoen. Aangezien het om een verwijderverzoek gaat is de discussie over (bijvoorbeeld) leeftijden daardoor minder relevant (vergeleken met de bewijslast die nodig is in een strafzaak). Daar het EOKM als separate stichting geen juridische dwang kan uitoefenen, geven sommige hostingpartijen pas gehoor aan een verwijderverzoek van de officier van Justitie. Het EOKM markeert daarnaast niet alleen evident 'fout' materiaal, maar ook materiaal dat niet direct kinderporno is (maar bijvoorbeeld onwenselijke foto's binnen eenzelfde serie waar ook kinderporno in te vinden is).

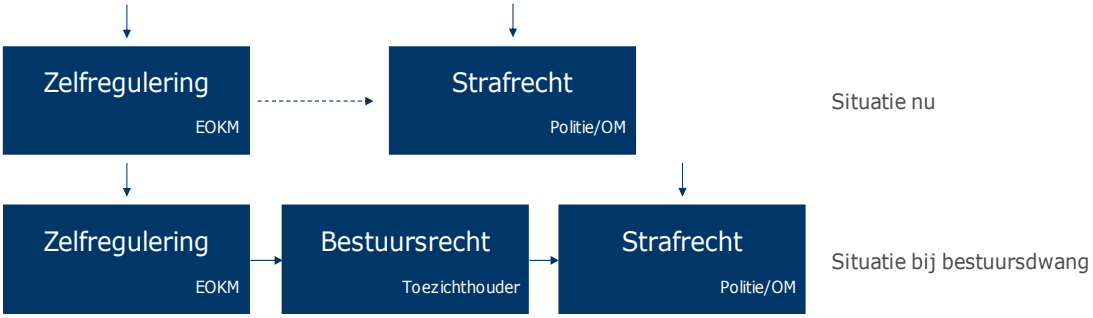
Het EOKM wordt vanuit verschillende hoeken gefinancierd. Naast een structurele bijdrage vanuit het ministerie van JenV (115k€ in 2016 en 215k€ in 2018) komen de middelen met name vanuit Europese subsidies, SIDN en enkele marktpartijen (KPN, Ziggo, LeaseWeb).

2.3 Positionering van het instrument bestuursrecht

In de huidige situatie wordt ca. 90% van de meldingen over websites met illegale content via de zelfregulering door het EOKM en de sector succesvol[15] afgehandeld. Via het strafrecht behandelt de politie meldingen over personen, waarbij zij zich hoofdzakelijk richt op de grootste verdachten. In het geval van introductie van bestuursrecht blijven de zelfregulering en het strafrecht onveranderd bestaan. Bestuursrecht biedt in die zin een derde handelingsoptie en is specifiek voor de groep bad hosters die niet (adequaat) reageert op de verwijderverzoeken van het EOKM. Die ca. 10% - die in de huidige situatie tussen wal en schip valt - kan dan worden aangepakt door een toezichthouder. Dat is de groep waar dit onderzoek op gericht is.

[14] Dit betreft een van de andere actielijnen (transparantie).

[15] Er is een norm van 24 uur afgesproken. In hoeverre die wordt behaald is onduidelijk. In 2016 werd meer dan 90% van het materiaal binnen drie dagen verwijderd (bron: jaarverslag EOKM 2016).



Figuur 2. Positionering bestuursrecht

Het AKD concludeerde dat bestuursrecht een haalbare optie is. Daarbinnen achtten zij bestuursdwang als het beste middel t.o.v. een dwangsom of bestuurlijke boete (die ook bij bestuursdwang kan worden opgelegd). Het inzetten van een dwangsom of combinatie zou ook een mogelijkheid zijn en daarmee is ook binnen het bestuursrecht enige escalatie mogelijk (bijv. waarschuwen, boete 1, boete 2, dwangsom, zelf handelen onder bestuursdwang).[16] In dit onderzoek kijken wij nadrukkelijk naar de toepassing van bestuursdwang.

Mogelijk blijven er alsnog partijen over die enkel of beter door het strafrecht kunnen worden aangepakt (zie ook paragraaf 5.4). Het gaat dan niet meer om meldingen, maar om rechtspersonen.

[16] De dreiging van bestuursdwang kan op zichzelf ook al waardevol zijn, maar kent mogelijk juridisch enkele haken en ogen.

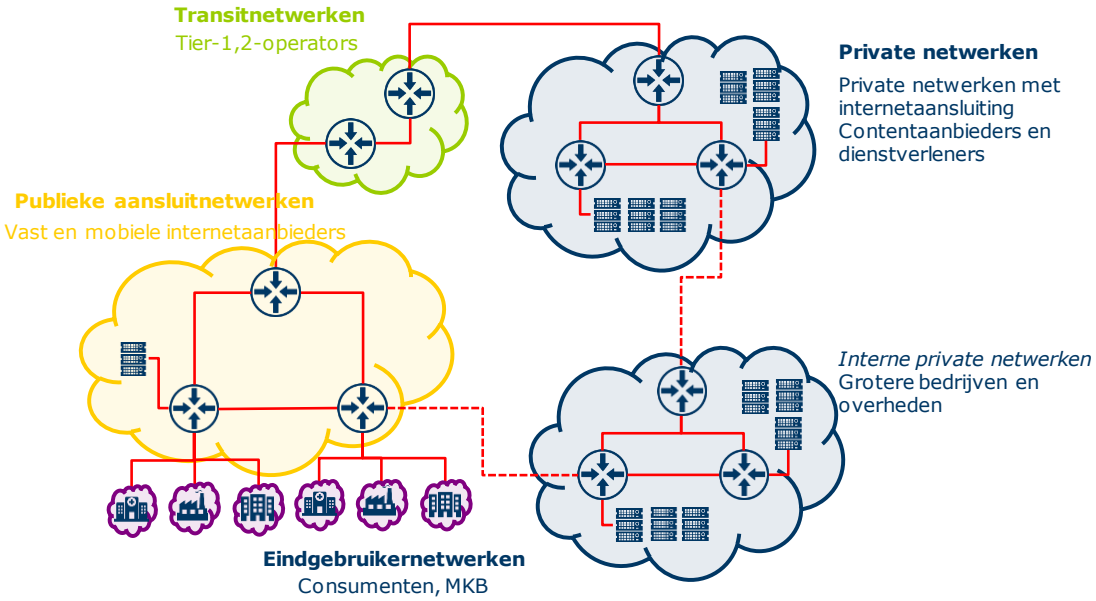
3 Verspreiding van kinderporno op het internet

In dit hoofdstuk geven wij een beschrijving van de sector waar de bestuursdwang zich op kan richten. We beschrijven de technische achtergrond, waarbij we stilstaan bij de verschillende type bedrijven, diensten, contracten en onderlinge relaties.

3.1 Werking van het (open) internet

Om tot een goede afweging te kunnen komen ten aanzien van methoden om ongewenste inhoud van het internet te verwijderen, is een goed begrip nodig van de verschillende manieren waarop dergelijke inhoud op het internet kan worden aangeboden.

In de basis bestaat het internet uit aan elkaar gekoppelde computernetwerken (*autonomous systems*) waaraan computers en andere netwerkapparaten zijn gekoppeld. De netwerken zijn aan elkaar verbonden via één-op-één verbindingen of via een internetknooppunt, zoals de AMS-IX in Amsterdam. Op dergelijke knooppunten komen verbindingen van en naar een veelheid aan netwerken bij elkaar, en kan eenvoudig worden gekoppeld. Ten tijde van schrijven zijn er circa 1200 van dergelijke netwerken met een Nederlandse registratie (RIPE, 2018).



Figuur 3. Schematisch overzicht van verschillende netwerktypen op het internet en koppelingen daartussen. Bron: Dialogic

Er zijn verschillende soorten netwerken te onderscheiden. Geteld naar het aantal aangesloten apparaten zijn de aansluitnetwerken van internetproviders, waarop consumenten zijn aangesloten, het grootst. Daarbinnen is onderscheid te maken naar mobiele en vaste netwerken. De tweede belangrijke categorie netwerken betreft die van 'contentleveranciers' (waarover verderop meer). Daarnaast zijn er diverse private netwerken (van grotere bedrijven en overheden). Als deze aparte netwerken niet direct op elkaar

aangesloten zijn, wordt er gebruik gemaakt van transitnetwerken om ervoor te zorgen dat de verschillende netwerken elkaar kunnen bereiken.

Om informatie, zoals een webpagina, van het internet op te halen maakt een computer (de 'client') verbinding met een andere computer (een 'server'). Eens verbonden geeft de client door waar deze naar op zoek is (de link van de bedoelde webpagina), waarna de server de webpagina terugstuurt. Voor een reguliere webpagina verloopt deze uitwisseling volgens de http-standaard; er zijn echter legio andere standaarden:

- Bij BitTorrent wisselen grote groepen computers ('zwermen') stukjes van een groter bestand met elkaar uit. BitTorrent wordt veel gebruikt voor uitwisseling van grote bestanden, waaronder veel illegale films en muziek.

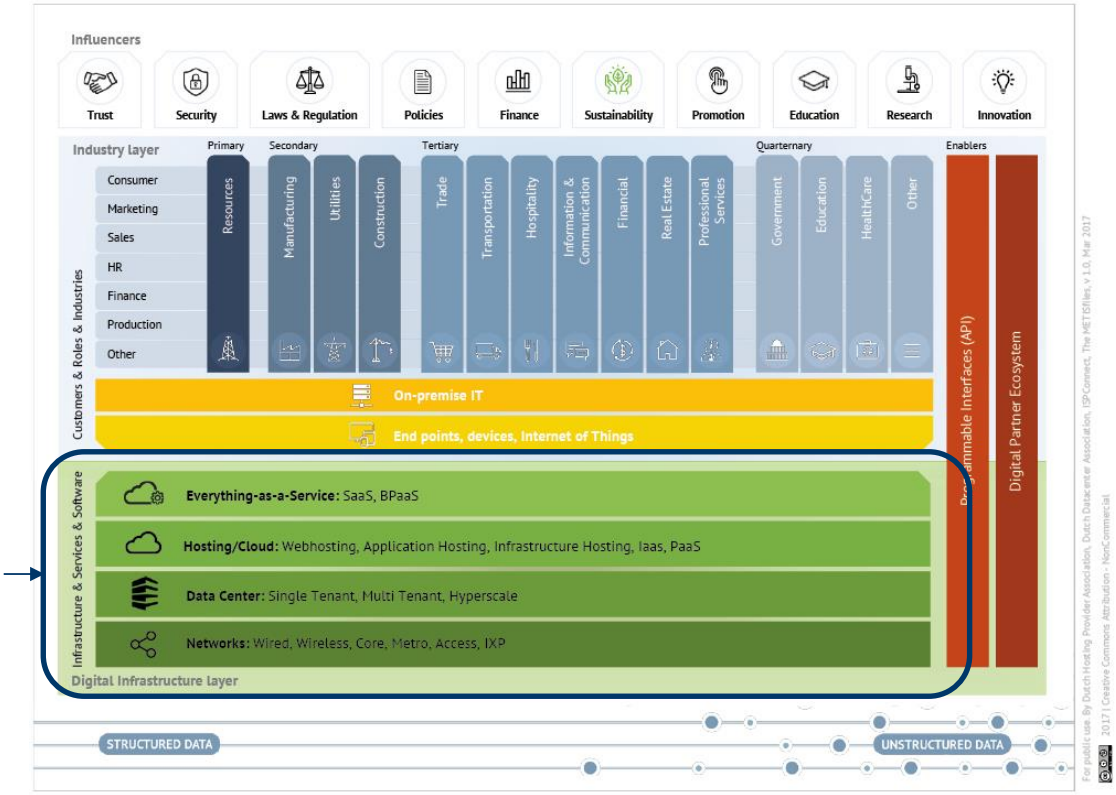
- Bij FTP kan met een gebruikersnaam en wachtwoord verbinding worden gemaakt met een afgesloten stuk opslagruimte, waar bestanden kunnen worden geüpload en gedownload.

- Bij Tor wordt een verbinding tussen client en server via een groot aantal tussengelegen computers geleid, waardoor de herkomst en in sommige gevallen ook de bestemmingsserver van een verbinding niet meer te traceren is.

Merk op dat uitwisseling van informatie ook kan gebeuren via een tussenpartij, ook wel 'platform' genoemd. Zo kunnen gebruikers bestanden (via de website) uploaden naar diensten als Dropbox, OneDrive of Box, waarna een andere gebruiker deze weer van de betreffende dienst kan downloaden. Daarnaast zijn er diverse (instant) messaging-platforms (zoals Facebook Messenger, WhatsApp en Skype) en diensten zoals WeTransfer waarover gebruikers rechtstreeks bestanden naar elkaar kunnen sturen.

3.2 Contentleveranciers en faciliterende partijen

De ICT-sector heeft een bepaalde gelaagdheid (zie Figuur 4). Onderin de keten bevinden zich partijen die zorgen voor de infrastructuur. Dit zijn ***netwerken*** die de elementen in Figuur 3 met elkaar verbinden. Een stap hoger zijn de ***datacenters***, dit zijn fysieke locaties waar de hardware voor de servers geplaatst wordt. Deze servers zijn fysieke computers die op de locatie in het datacenter voorzien worden van elektriciteit en eventueel gekoppeld worden aan andere netwerken. Vanaf die servers worden specifieke diensten geleverd via de ***hosting***laag. Dit kan gaan om bepaalde applicaties en platformen, maar ook om het leveren van een bepaalde infrastructuur. Partijen op de ***everything-as-a-service***laag nemen deze diensten af om zelf weer nieuwe online diensten aan te leveren die gericht zijn op de eindgebruiker. Dit gaat om websites maar ook om andere webdiensten, zoals FTP file shares en fora.



Figuur 4. Schematische weergave van de sector. De groene lagen zijn met name relevant voor dit onderzoek. Bron: DINL

Grote contentleveranciers als Facebook, Google en NPO hebben hun eigen datacenters, met daarin eigen servers, en eigen verbindingen naar andere netwerken. De meeste contentleveranciers zijn echter een stuk kleiner, en maken gebruik van diensten van derden om hun diensten te leveren:

- **Datacenterruimte.** Diverse partijen (zoals LeaseWeb, Colt en Interconnect) verhuren ruimte in datacenters. Daarbij kan er gekozen worden uit een bepaalde hoeveelheid ruimte in een 'rack' tot aan een verzameling racks (al dan niet fysiek afgesloten in een eigen 'cage'). De datacenteraanbieder verzorgt daarnaast de (nood)stroomvoorziening, koeling en fysieke beveiliging. Daarnaast zijn er veelal een groot aantal verbindingen naar diverse andere netwerken en aanbieders beschikbaar. In de datacenterbranche zijn diverse partijen actief, in verschillende 'segmenten'; te denken valt aan Interxion, KPN (NLDC), Alticom, Colt en Equinix.

- **Colocatie**. Hierbij biedt de aanbieder naast datacenterruimte ook connectiviteit naar het internet, en mogelijk enkele andere diensten (zoals 'remote hands', e-mailservers, remote back-upfaciliteiten, et cetera). Colocatieruimte wordt in Nederland (grotendeels in en rond Amsterdam) aangeboden door partijen als LeaseWeb, True, TransIP en PCextreme.

- **Dedicated server**. Hierbij biedt de aanbieder niet alleen colocatie, maar levert deze ook de hardware. Vaak betreft het een leaseconstructie, waarbij de aanbieder verantwoordelijk is voor het vervangen van de hardware bij defecten. De afnemer heeft een grote keuze uit servers en is volledig vrij de server naar eigen inzicht in te richten. Onder andere LeaseWeb, Strato en Hostnet bieden in Nederland dedicated serverdiensten aan.

- **Managed server**. Hierbij biedt de aanbieder een server waarop een besturingssysteem (Windows of Linux) geïnstalleerd is. De klant heeft volledige toegang tot de server en kan deze naar eigen inzicht inrichten. De aanbieder zorgt voor basaal onderhoud. Daarnaast kunnen aanvullende diensten worden geboden (zoals back-ups). Aanbieders van managed servers zijn onder andere Prolocation, LeaseWeb en de grotere IT-dienstverleners zoals Ordina.

- **Virtual private server.** Hierbij biedt de aanbieder een virtuele server aan. Er worden op dezelfde fysieke server meerdere besturingssystemen geïnstalleerd. De gebruikers van de verschillende installaties kunnen elkaar niet 'zien', en het lijkt voor de afnemer alsof deze een volledige server ter beschikking heeft. In werkelijkheid wordt de onderliggende capaciteit (processor, opslag en connectiviteit) gedeeld met andere gebruikers. Virtuele servers zijn om deze reden vaak efficiënter wanneer een dienst niet altijd volledig belast is. Daarnaast biedt virtualisering een hoge mate van flexibiliteit (er kunnen eenvoudig virtuele servers worden verplaatst tussen fysieke servers, en daardoor kan er makkelijk worden opgeschaald).

  Virtuele servers worden vaak aangeboden in combinatie met back-up en 'snapshot'-faciliteiten. Daarnaast hebben de aanbieders vaak 'fail over' ingericht: wanneer een fysieke server defect raakt worden alle getroffen virtuele servers verplaatst of opnieuw gestart op een andere server (al dan niet op een andere locatie, bijvoorbeeld een ander datacenter).

  Aanbieders van virtuele servers zijn onder andere Google (Cloud Platform), Amazon (AWS) en Microsoft (Azure) – allen hebben (ook) datacenters in Nederland. In Nederland zijn partijen als LeaseWeb, Prolocation en TransIP actief.

- **Containers**. Hierbij verzorgt de aanbieder het uitvoeren van een applicatie (naar specificatie van de afnemer) via containertechnologie. In tegenstelling tot virtuele private servers is het voor een afnemer niet meer te 'zien' op welke servers een applicatie wordt gedraaid. Containergebaseerde diensten kunnen transparant opschalen en vereisen minder beheer (door de afnemer) dan virtuele servers. Aanbieders van containerdiensten zijn onder andere Microsoft (Azure), Google (Cloud Platform) en Amazon (AWS).

- **Webhosting**. Hierbij gaat het om gestandaardiseerde dienstverlening, primair gericht op het aanbieden van een website. De afnemer uploadt zijn website of webapplicatie (denk aan een webwinkel) en bijbehorende databases naar de webhoster. De webhoster zorgt ervoor dat de site beschikbaar komt via een bepaalde domeinnaam, en handelt daarbij alle randzaken (zoals beveiliging met certificaten, e-mailadressen en virusscans) af. Er zijn diverse vormen van gespecialiseerde webhosting, bijvoorbeeld specifiek gericht op webwinkels (waarbij de aanbieder bijvoorbeeld ook de webwinkelsoftware onderhoudt). Aanbieders van webhostingdiensten zijn onder andere TransIP, Antagonist, LeaseWeb en MijnDomein.

Merk op dat het technisch gezien geen probleem is om een website (of andere internetdienst) aan te bieden vanaf een internetaansluiting buiten een datacenter (bijvoorbeeld een kantoor- of consumentenaansluiting). Zo werd begin deze eeuw veel illegale content aangeboden vanuit studentenkamers, aangezien er daar vaak snelle internetaansluitingen beschikbaar waren (Leenders, 2004). Dergelijke hosting kan ook onvrijwillig plaatsvinden – computers

van consumenten en bedrijfsservers kunnen worden gehackt en worden ingezet voor distributie van illegale inhoud.

3.3 Alternatieven voor uitwisseling via het open internet

Voor uitwisseling van niet-legitieme inhoud kan, naast het open internet, gebruik worden gemaakt van verschillende alternatieve technieken:

- Via het *dark web* kunnen websites worden aangeboden op internet zonder dat precies is te achterhalen wie deze beheert en waar deze (fysiek) gehost wordt. Het 'dark web' maakt gebruik van de Tor-software, welke verbindingen op het internet via een groot aantal computers 'omleidt'. Dark websites hebben vaak een cryptisch webadres en zijn niet in reguliere zoekmachines te vinden.

- Netwerken kunnen direct aan elkaar worden gekoppeld via eigen verbindingen (fysieke kabels of draadloze verbindingen, of virtueel via een 'virtual private network').

- Een *sneakernet* is een netwerk waarbinnen gegevens worden uitgewisseld door het fysiek uitwisselen van datadragers, zoals harde schijven. Hoewel dit erg ouderwets lijkt, is de bandbreedte hiervan zeer hoog in vergelijking met reguliere consumentenaansluitingen, en dient daarom niet te worden onderschat (ter vergelijking: met de post kan een harde schijf ter grootte van 4TB in 24 uur worden bezorgd, wat netto neerkomt op een overdrachtssnelheid van gemiddeld 407 Mbit/s).

4 Werkwijze bij het verwijderen van kinderporno

In dit hoofdstuk beschrijven we de feitelijke stappen en technische handelingen die een toezichthouder zou moeten doorlopen bij het uitoefenen van bestuursdwang. Twee duidelijke processen worden hierbij onderscheiden:

1. *Identificatie van de partij die onderwerp is van bestuursdwang*
2. *De content bij de betreffende partij daadwerkelijk verwijderen of ontoegankelijk maken*

We staan in dit hoofdstuk eerst stil bij wat we onder verwijderen verstaan (paragraaf 4.1). Vervolgens brengen we de keten in beeld (paragraaf 4.2 – ten behoeve van het eerste proces) en gaan we per partij in de keten na wat voor technische handelingen er bij toepassing van bestuursdwang nodig zijn (paragraaf 4.3 – ten behoeve van het tweede proces). Verder staan we stil bij de nevenschade (paragraaf 4.4), de kosten (paragraaf 4.5) en de benodigde equipment en kennis (paragraaf 4.6).

4.1 Wat verstaan we onder verwijderen?

In het AKD-advies werd al kort ingegaan op de technische mogelijkheden van verwijderen, namelijk:

1. Het fysiek verwijderen van de (virtuele) server uit het pand van een ICT-bedrijf of door kinderporno op die server te wissen. Dit kan - vanuit het bestuursrecht - bij in Nederland gevestigde servers of in Nederlandse bedrijven.

2. Toegang tot kinderporno blokkeren, bijvoorbeeld door het blokkeren van een IP-adres. Een dergelijke blokkade is technisch in veel gevallen te omzeilen.

3. Bepaalde content door een ISP te laten filteren die voorkomt in een bepaalde database (‘dynamic filtering’), bijvoorbeeld met de hashcodedatabase waarin inmiddels bekende kinderpornoafbeeldingen zijn opgenomen. Ook een filter is te omzeilen op het internet.

Er wordt terecht opgemerkt dat een aantal vormen van blokkades te omzeilen is - een Domain Name Server (DNS)-blokkade voorkomt in principe alleen dat een bezoeker het IP-adres van een domeinnaam niet meer kan vinden; alsof je een naam uit het telefoonboek wist. Het IP-adres is echter nog wel benaderbaar. Daarnaast kan een bezoeker een ándere DNS-server gebruiken. Er zijn echter ook blokkades die niet te omzeilen zijn. Zo kan bijvoorbeeld de hele hostingpartij worden afgesloten van het internet. Ook kan de routering worden aangepast. Vaak is dit echter te rigoureus en echt een noodoplossing, omdat hierbij meerdere partijen geraakt kunnen worden.

Het omzeilen van hashcodering (filteren) kan ook relatief gemakkelijk plaatsvinden. Hashcodering veronderstelt dat de content steeds hetzelfde is. Als een server bepaalde content aanbiedt en daarin steeds iets wijzigt (bijvoorbeeld een tijdstempel opneemt op een afbeelding, of iets anders willekeurigs) dan werkt een hash niet meer. Uitzondering is het gebruik van een soort ‘fuzzy’ hash of ‘fingerprint’. Naast hashcodering zouden ook beeldherkenningsalgoritmes kunnen worden gebruikt. Het voordeel is dat die ook niet eerder

geziene content blokkeert, maar het nadeel is dat die modellen type-1 en type-2 fouten maken én voor de gek te houden zijn.

Hoe werkt hashfiltering van afbeeldingen?

Om het voor platformhouders mogelijk te maken om bestanden met kinderporno te kunnen herkennen en op te ruimen, moeten deze houders op een of andere manier bestanden kunnen vergelijken met bekende bestanden met kinderporno. Een platformhouder mag dergelijke bestanden echter niet in bezit hebben. Met hashfiltering kan, zonder te beschikken over een bestand, toch worden vastgesteld of een ander bestand dezelfde inhoud bevat.

Een hash is een wiskundig 'controlegetal' dat kan worden afgeleid van data, zoals een afbeelding. De hash van een afbeelding bevat veel minder informatie dan de volledige afbeelding. De hash wordt echter wel zodanig berekend dat wanneer deze voor twee verschillende bestanden gelijk is, de kans zeer groot is dat de twee bestanden ook exact gelijk aan elkaar zijn.

Door deze eigenschap kunnen hashes worden gebruikt om bestanden met daarin kinderporno te herkennen: het uitrekenen van de hash en het controleren of deze hash eerder is gemarkeerd als zijnde een hash van een bestand waarin kinderporno is aangetroffen, is voldoende. De controleur hoeft daarbij niet te beschikken over het eerder gevonden bestand met kinderporno, maar slechts over de hash.

Veelal zijn de gebruikte hashingalgoritmes zodanig opgezet dat het praktisch gezien onmogelijk is om een bestand te maken dat precies dezelfde hash heeft als een ander bestand. Als dat wel eenvoudig zou zijn, dan zou het feit dat twee hashes gelijk zijn aan elkaar nauwelijks meer iets zeggen over de gelijkheid van de onderliggende bestanden. Een nadeel is dat de hashcode van een bestand radicaal verandert wanneer er ook maar één bit wordt gewijzigd. In de context van filtering van afbeeldingen betekent dit dat een kwaadwillende slechts één kleine aanpassing hoeft te doen om te zorgen dat de afbeelding niet meer wordt herkend. Het vergroten of verkleinen van de afbeelding in een fotobewerkingsprogramma of het aanpassen van een enkele pixel is al voldoende. Geavanceerdere algoritmes, die bijvoorbeeld worden gebruikt voor hashing van biometrische gegevens, kunnen mogelijk uitkomst bieden.[17]

Het filteren door ISP's is daarnaast ondoenlijk wanneer er end-to-end gecodeerde verbindingen worden gebruikt ("https" in plaats van "http" in de URL). Dit is voor vrijwel alle websites tegenwoordig het geval. Een eindgebruiker zou wel vrijwillig een certificaat of stuk software kunnen installeren zodat de ISP het verkeer kan onderscheppen en controleren, maar ook dit werkt niet met alle diensten. Ook zou er aan de aanbodkant bij hostingpartijen gebruik gemaakt kunnen worden van een hashdatabase (van het EOKM) om te zien of er bestanden met kinderporno op de server opgeslagen staan. Het staat hosters vrij om dit al dan niet te implementeren; wat een kwaadwillende partij niet snel zal doen. Algemene filtering en inspectie van alle content heeft geen wettelijke basis en wordt in bestaande EU-wetgeving uitgesloten.

Het ligt dus voor de hand om als uitgangspunt het daadwerkelijk fysiek verwijderen van de server of het wissen van de content op de server te nemen. In het geval van bestuursdwang kan de partij aan wie de bestuursdwang is opgelegd bezwaar maken. De termijn voor bezwaar is zes weken. Vervolgens moet er besloten worden over dat bezwaar (een

[17] Voor een overzicht van de uitdagingen bij het hashen van biometrische data, zie de Groot (2014), *Biometric security on body sensor networks* (pure.tue.nl). Microsoft biedt de dienst PhotoDNA aan, waarmee foto's op basis van een hashalgoritme kunnen worden gecontroleerd. Daarbij wordt een techniek gebruikt waarbij afbeeldingen worden gestandaardiseerd (onder andere door ze naar grijswaarden te converteren) en vervolgens meerdere hashes worden berekend over verschillende segmenten van een afbeelding. Zie news.microsoft.com.

zogenaamd 'besluit op bezwaar'). Hoofdregel is dat een bestuursorgaan binnen zes weken beslist (twaalf weken als het bestuursorgaan extern advies inwint). Tegen dit besluit op bezwaar kan dan weer binnen 6 weken beroep worden ingesteld en dan komt de zaak voor de rechter (een procedure die ook lang kan duren). De verwijdering van content is (mits deze goed is uitgevoerd) een onomkeerbare actie. Dit houdt in dat de content voor het verlopen van de bezwaartermijn van minstens zes weken (en nog veel langer als er bezwaar wordt gemaakt) niet verwijderd kan worden, zodat de verweerder van de beroepsprocedure deze content nog als bewijs kan opvoeren. Om deze reden ligt het voor de hand om de content in eerste instantie ontoegankelijk te maken en pas na het verlopen van de bezwaartermijn definitief te verwijderen. Het komt echter wel vaker voor dat de uitvoering van een besluit (in dit geval de uitvoering van de bestuursdwang) onomkeerbare gevolgen heeft. Het is in zulke gevallen aan de partij zelf om niet alleen bezwaar te maken maar ook de rechter te vragen om een 'voorlopige voorziening' te treffen. In dit geval zou de rechter dan bijvoorbeeld kunnen beslissen dat het materiaal niet verwijderd mag worden maar slechts geëncryptet, totdat het besluit op bezwaar is genomen of op het beroep is beslist. Enkel justitie zou dan kunnen decrypten wanneer de content gecontroleerd moet worden. Hetzelfde geldt voor de beroepsprocedure.

Wanneer er sprake is van een virtuele server kunnen er meerdere webdiensten draaien op één fysieke server. Dit maakt de situatie ingewikkelder. Het maakt het namelijk moeilijker aan te wijzen waar op de server de content precies staat. Het virtuele karakter van de server maakt het daarnaast mogelijk om de server snel te verplaatsen naar een andere server. Ook is het mogelijk dat er (veel) meer andere webdiensten geraakt worden bij verwijdering, vanwege de gedeelde capaciteit.

Ook bij het fysiek verwijderen van een server zijn er uitdagingen. Van veel data op servers bestaat een back-up die vaak ergens anders wordt opgeslagen (bijvoorbeeld in het geval van brand). Dit is wellicht minder aan de orde voor criminelen die zélf hardware in een datacenter ophangen (zgn. "colocated" of "dedicated" servers), maar niettemin relevant. Zoals eerder is opgemerkt wordt een server vaak gedeeld met andere klanten. Bij het verwijderen wordt dus in theorie een grotere groep klanten getroffen dan wenselijk. Aangezien een server ook spontaan kan uitvallen kan de infrastructuur van een cloudaanbieder dat doorgaans opvangen. Een andere server neemt de data dan over. Hiervoor wordt vaak (zeker bij de cloud- en virtuele aanbieders) gebruik gemaakt van separate opslagsystemen (SAN's; Storage Area Networks), en moet de data dus eigenlijk dáár gewist worden. Dat is echter niet eenvoudig, want een SAN wordt ook weer gedeeld door meerdere klanten.

4.2 Identificatie: de keten in beeld

Voor de toepassing van bestuursdwang zal er al een heel traject aan meldingen voorafgaan. Zonder een melding is het namelijk niet duidelijk dat er ergens content staat. Deze meldingen komen via verschillende bronnen bij de politie en het EOKM binnen. Dit betreft een URL naar de content zelf of naar een website of platform waar meer content op staat. Als dit naar een partij buiten Nederland wijst, dan zal het via de koepelorganisatie INHOPE worden doorgezet naar een meldpunt van het land in kwestie.

Er zijn verschillende aanknopingspunten om dichter bij de (fysieke) opslagplaats van de content te komen. In Figuur 5 wordt dit schematisch weergegeven. Websites, webpagina's en webdiensten zijn over het algemeen benaderbaar via een URL. Met die URL kan er op verschillende manieren worden nagegaan aan welke partij de melding geadresseerd kan worden.

Ten *eerste* kan er **contactinformatie** op de website staan van de website-eigenaar of de webhoster. Bij websites van grotere organisaties is er vaak een abuse-afdeling. Deze afdeling houdt zich bezig met het offline halen van illegale content op hun eigen website. In veel gevallen is er echter geen contactinformatie bekend, omdat de website-eigenaar zelf bepaalt dit wel of niet te vermelden.

Ten *tweede* kan er aan de hand van de URL worden opgezocht waar de **domeinnaam** geregistreerd is. Domeinnamen kunnen worden aangekocht bij domeinnaam registrars. Voor Nederlandse websites (.nl) kan dit bijvoorbeeld bij Stichting Internet Domeinregistratie Nederland (SIDN). Dergelijke organisaties houden vaak bij op welke naam een domeinnaam geregistreerd is ('whois-informatie'). Deze informatie verwijst dan naar de persoons-, bedrijfs- of contactgegevens van de domeinnaamhouder. Dit hoeft niet direct de eigenaar van een website te zijn. Het kan ook verwijzen naar een aanbieder van webhosting. Deze zou in principe moeten weten wie de website-eigenaar is, tenzij het een reseller van domeinnamen betreft.

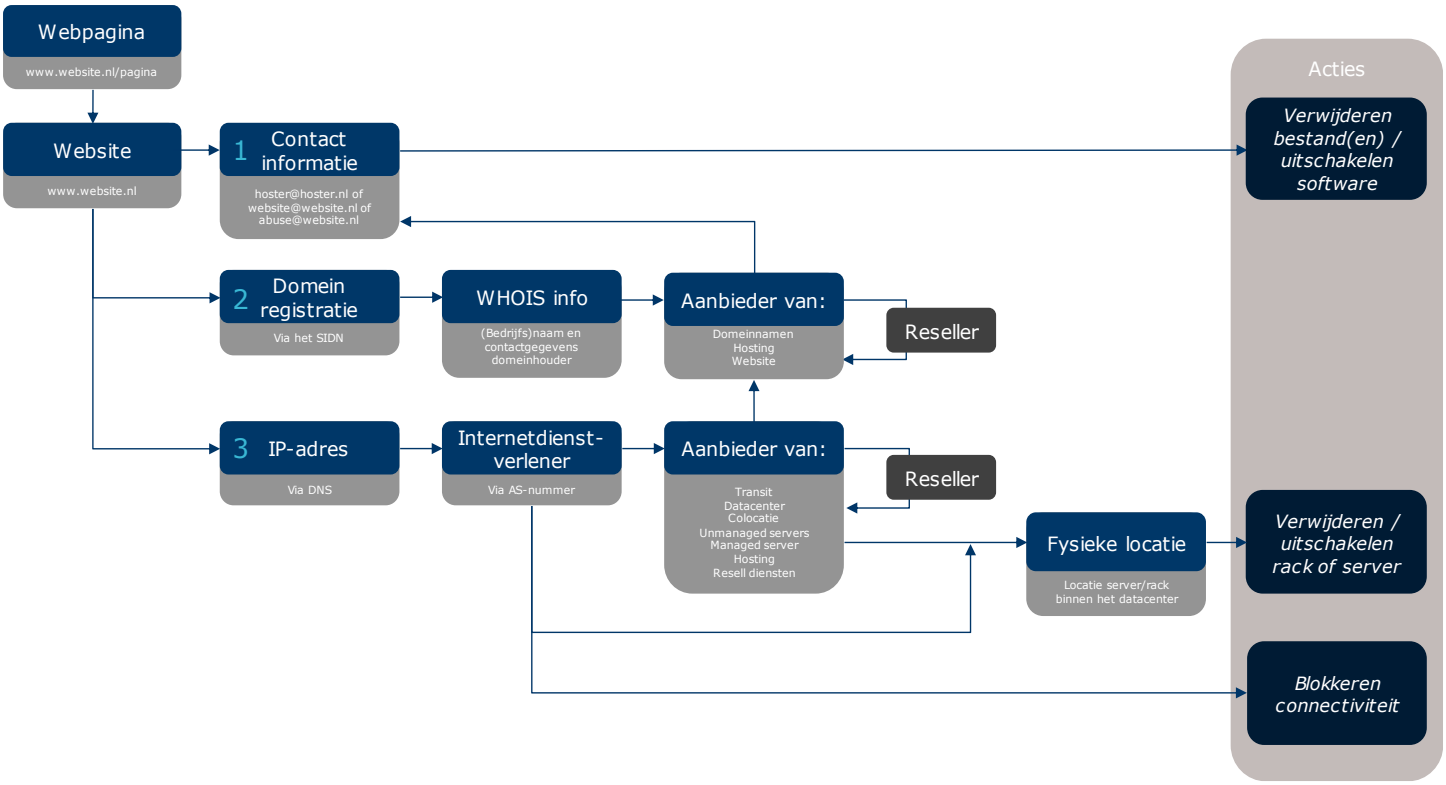
Een *derde* route gaat via het **IP-adres**. Domeinnamen verwijzen naar een IP-adres – dit adres is nodig om contact te kunnen leggen met de server waarop de website of webdienst draait. Via een Domain Name Server (DNS) worden domeinnamen omgezet tot IP-adressen. Op basis van een IP-adres kan worden bepaald welke internetaanbieder de internetverbinding verzorgt richting de server. De organisaties die IP-adressen verdelen houden namelijk bij welk bereik van IP-adressen bij welk netwerk (*autonomous system* of AS) hoort, en welke organisatie voor dat netwerk verantwoordelijk is.

Grotere bedrijven en internetdienstverleners hebben vaak een eigen AS-nummer en bijbehorend IP-bereik. Deze partijen beschikken vaak ook over een eigen abuse-afdeling.

Kleinere bedrijven en particulieren hebben meestal geen eigen AS, maar maken typisch gebruik van diensten van grotere dienstverleners. Deze dienstverleners kennen de identiteit van de klant die gebruik maakt van een specifiek IP-adres binnen hun netwerk. Dergelijke gegevens kunnen dus worden opgevraagd bij de dienstverlener. Merk op dat er sprake kan zijn van verschillende 'lagen' van dienstverleners (deze zitten ook de infrastructuurlagen van Figuur 4):

- Een *datacenteraanbieder* biedt fysieke locaties waar servers kunnen worden geplaatst. In de regel is deze partij niet verantwoordelijk voor het leveren van de connectiviteit naar het internet. Deze wordt typisch ingekocht bij een *transit*aanbieder en/of gerealiseerd door 'peering' op een internetknooppunt.
- Een *colocatie-aanbieder* biedt rackruimte en connectiviteit in een datacenter, waarbij gebruik wordt gemaakt van de diensten van een *datacenteraanbieder*.
- Een aanbieder van *unmanaged servers* (vaak ook 'dedicated servers' genoemd) biedt servers te huur aan die worden geplaatst in ruimte die de *colocatie-aanbieder* voorziet.
- Een aanbieder van *managed services* biedt diensten aan op basis van servercapaciteit (die het inkoopt bij aanbieders van unmanaged servers, of realiseert door servers te plaatsen bij een colocatie-aanbieder; de allergrootste partijen hebben eigen datacenters).
- Een *hostingaanbieder* maakt veelal gebruik van de diensten van een (un)managed dienstenaanbieder, en biedt webruimte aan consumenten of (kleine tot middelgrote) bedrijven.

- Een *reseller* koopt grote hoeveelheden 'white label' capaciteit in bij een van bovenstaande aanbieders en biedt ze op de markt aan met bepaalde toegevoegde diensten. Er kunnen meerdere niveaus van resellers te vinden zijn in de waardeketen.



Figuur 5. Pad van website tot andere aanknopingspunten. Bron: Dialogic

Bovenstaand schema geeft de route van webpagina tot de verschillende soorten aanbieders weer. Deze route achterhalen is niet altijd eenvoudig en zal in uitzonderlijke gevallen bijna onmogelijk zijn (zie paragraaf 5.4). Vooral de route via een IP-adres (waar men bij bad hosters toch vaak op uitkomt) kan ingewikkeld worden. Dit is onder andere afhankelijk van de partij die de internetdienst afneemt bij het bedrijf dat IP-adreshouder is.

Om als website benaderbaar te zijn via een IP-adres op het internet, moet er een internetdienst worden afgenomen. Via de internetdienstverlener (zakelijke ISP) is de server aangesloten op het internet en benaderbaar met een IP-adres. In principe weet de internetdienstverlener dus bij welke klant een IP-adres hoort en op welke fysieke locatie het IP-adres uitkomt. Er is dan in ieder geval bekend in welk datacenter de server staat waar dit adres binnenkomt op een modem. De moeilijkheid ontstaat vooral op de weg van modem tot server, want:

1. Het datacenter weet over het algemeen hoe de verbinding van modem naar de servers loopt, maar de internetdienstverlener weet dit niet.
2. De internetdienstverlener weet welke van hun eigen IP-adressen er bij het datacenter binnenkomen, maar een datacenter weet dit niet.

De exacte locatie van de server binnen het datacenter is dan alleen te achterhalen als de internetdienstverlener en het datacenter samenwerken, of als deze diensten door hetzelfde bedrijf worden afgenomen. Door te koppelen op bedrijfsnaam zou het dan in theorie mogelijk zijn om ongeveer te bepalen in welk rack de server zou moeten staan. Dit zijn echter niet altijd het geval. Daarnaast is het mogelijk dat een IP-adres uitkomt bij een server waar de

content niet staat. Deze server dient dan alleen als proxy, wat betekent dat deze server enkel verkeer van andere servers over de wereld doorsluist. De weg van een IP-adres naar een fysieke server is dus enkel te achterhalen met de medewerking van (meerdere) partijen.

Merk op dat het proces van identificatie iteratief kan plaatsvinden. Wanneer een hoster geïdentificeerd wordt - maar niet reageert op eerdere verwijderverzoeken – kan de toezichthouder dieper in de keten het datacenter identificeren. Wanneer deze wel reageert en zelf de content verwijdert, is verdere toepassing van bestuursdwang niet meer nodig.

4.3 Feitelijke handelingen toepassing bestuursdwang

De meeste ISP's en HSP's hebben zich gecommitteerd aan de "Gedragscode Notice-and-Take-Down" (NTD) waarin een algemene procedure voor het verwijderen van onrechtmatige content is opgenomen. Kinderporno wordt dan in beginsel vrijwillig verwijderd na een melding - in essentie binnen 24 uur.[18,19] Voor de groep bad hosters die niet (adequaat) reageert op meldingen wordt toepassing van bestuursdwang voorgesteld.

Het advies uit de reactie van DHPA en ISPConnect op het AKD-advies[20] zegt dat de maatregel van bestuursdwang moet worden opgelegd bij het bedrijf dat zo dicht mogelijk op de strafbare content zit. Dit om de nevenschade te beperken, m.a.w. te voorkomen dat vele websites en webservices onnodig worden afgesloten. Wij beschrijven hier een dergelijke 'koninklijke route' waarbij we het dichtst bij de content beginnen om zo precies mogelijk te verwijderen. Naarmate we dieper in de keten komen wordt de bijl 'botter' en de schade groter. Het is echter denkbaar dat er in de praktijk een kantelpunt komt (bijvoorbeeld vanwege tijdsinspanning) waarop de toezichthouder toch bij een partij dieper in de keten inschiet en daar handhaaft.

Momenteel is de situatie bij de zelfregulering (NTD) als volgt: een melding van het EOKM gaat naar de eigenaar van een IP-blok (abuse contact van een hoster). Deze speelt de melding door naar de partij in de keten die bij de content kan (klant van de hoster). Deze klant is dan verantwoordelijk voor het verwijderen van de content. Wanneer bestuursdwang nodig is, houdt dit in dat ergens in de keten een partij weigert te handelen naar de melding. De benodigde actie hangt af van de plaats van deze partij in de keten, maar dit kan reiken tot aan het binnentreden van een datacenter.[21]

In de volgende sectie lichten we eerst toe wat er qua verwijdering mogelijk is voor een marktpartij in de keten als de aanbieder die diensten van die partij (dus de volgende partij in de keten) afneemt niet mee wil werken. Hiermee wordt er eerst een duidelijk beeld gegeven van wat er binnen de technische mogelijkheden ligt van de partijen op de verschillende lagen. Daarna gaan we over op welke feitelijke handelingen er uitgevoerd

---

[18] AbuseIO is momenteel aan het verkennen of het werk dat bij het EOKM wordt uitgevoerd niet verder geautomatiseerd kan worden. Een groot deel van de detectie en het versturen van meldingen zou geautomatiseerd kunnen worden.

[19] Door een grens van 24 uur op te nemen in het addendum van de zelfregulering geeft de sector feitelijk aan dat het verwijderen van de content binnen die tijd zou moeten kunnen. Dit kan dus tevens de norm zijn voor de route die de toezichthouder volgt bij bad hosters.

[20] DHPA en ISPConnect (11 december 2018). Commentaar op haalbaarheidsstudie bestuursrechtelijke aanpak van kinderporno.

[21] Volgens *Artikel 5:27 Algemene wet bestuursrecht* zou een bestuursrechtelijke toezichthouder bevoegd zijn om een datacenter te betreden voor zover dat voor de uitvoering van de taak nodig is. Bron: wetten.overheid.nl

moeten worden door een mogelijke toezichthouder als er bestuursdwang moet worden toegepast op één van de partijen in de keten.

4.3.1 Manieren van ingrijpen

In Tabel 1 wordt er per aanbieder van een bepaalde dienst aangegeven welke optie tot verwijdering technisch mogelijk is. De aanbieders zijn hier opgedeeld aan de hand van de lagen in Figuur 4. Hierbij is alleen de minst schadelijke optie opgenomen, omdat het onwaarschijnlijk is dat een partij kiest voor een optie die onnodig meer schade oplevert. Zoals in paragraaf 4.2 wordt beschreven is het niet altijd duidelijk waar de content precies staat. Zonder identificatie van de partij waarop bestuursdwang zou moeten worden toegepast is er ook geen actie mogelijk. In deze paragraaf gaan we er dus vanuit dat er in ieder geval één Nederlandse partij in de keten bekend is.

We maken een onderscheid tussen het fysiek en logisch niveau. Het fysieke niveau vertegenwoordigd de opties die een fysieke handeling vereisen. Het logische niveau betreft een digitale handeling. Een digitale handeling houdt hier in dat er op een computer bepaalde commando's uitgevoerd moeten worden, zoals het opgeven van een gebruikersnaam en wachtwoord of het digitaal verwijderen van een bestand.

Tabel 1. Niveau van overheidshandelen per ketenpartij

Laag	**Aanbieder van:**	**Uitschakelen/verwijderen van (cq. blokkeren connectiviteit naar):**					
		Fysiek niveau			**Logisch niveau**		
		Datacenter	*Rack, cage, vloer*	*Server en aanverwante hardware*	*Besturingssysteem*	*Server proces*	*Content*
Everything-as-a-service	*Webdienst*						X
Hosting/cloud	*Webhosting*					X	Soms
	Container					X	
	Virtual private server				X	X	
	Managed server				X	X	
	Dedicated server			X			
Datacenter	*Colocatie*		X				
	Datacenterruimte		X				
Netwerken	*Backbone*	X					

We beschrijven hier welke handelingen per niveau zouden kunnen worden uitgevoerd om de content ontoegankelijk te (laten) maken of te verwijderen (de *escalatieladder*). Zoals eerder aangegeven behandelen we hier de 'koninklijke route'. In veel gevallen moet hiervan worden afgeweken, omdat bijvoorbeeld de keten niet volledig bekend is, de tijdsinspanning te groot wordt of de toezichthouder een actie niet (zelf) kan uitvoeren (hier komen we later op terug).

- **Webdienst:** Aanbieders van webdiensten hebben toegang tot de bestanden (*content*). De toegang hiervan is beperkt omdat er inloggegevens nodig zijn om deze bestanden te verwijderen.
- **Webhosting/Container:** Een aanbieder van webhosting heeft soms toegang tot de bestanden en anders toegang tot het *server proces*. Dit server proces is software dat ervoor zorgt dat de bestanden of webdiensten online beschikbaar zijn. De aanbieders van containers hebben enkel toegang tot dit server proces. Hier gaat het ook om logische toegang, m.a.w. er zijn inloggegevens vereist om toegang te krijgen.
- **Managed server/VPS:** De aanbieder van een managed server of VPS heeft toegang tot het besturingssysteem waar de website en het serverproces op draait. Ook hier is een wachtwoord nodig voor toegang tot het beheer van het besturingssysteem. De volgende partij op de escalatieladder kan een aanbieder van de dedicated server zijn of – wanneer er sprake is van een resellerconstructie – een andere aanbieder van managed servers of VPS.
- **Dedicated server:** Een aanbieder van dedicated servers heeft geen logische toegang tot een server. Hier gaat het namelijk om hardware dat in een rack binnen een datacenter hangt. Op deze hardware draait een besturingssysteem. De aanbieder van de dedicated server zou dit kunnen uitschakelen. Als deze partij niet mee werkt, dan neemt de toezichthouder contact op met de aanbieder van datacenterruimte om toegang te krijgen tot de fysieke locatie. In dit geval kan het zijn dat het serverrack waar de hardware in hangt afgesloten is met een (geavanceerd) slot. Dit slot zal dan moeten worden opengebroken.
- **Datacenterruimte/Colocatie:** Een aanbieder van datacenterruimte en colocatie biedt een stuk grond en toegang tot internet aan. Deze aanbieders kunnen daarom bij het betreffende rack. Soms moet dit worden opengebroken, maar veel datacenters hebben een masterkey voor alle racks. Met deze sleutel kunnen ze elk rack openen (als veiligheidsmaatregel in geval van kapotte onderdelen of brand). Ook kunnen zij de internet- en stroomvoorzieningen van de servers afschakelen. Als deze partij weigert mee te werken zal de toezichthouder de locatie moeten binnenvallen. Datacenters zijn over het algemeen goed beveiligd met hekken om het pand, grote deuren met geavanceerde beveiliging en dikke muren. Om een dergelijke ruimte geforceerd binnen te treden, zullen er veel fysieke beveiligingen opengebroken moeten worden. In de box hieronder wordt kort beschreven hoe men normaal gesproken een datacenter binnen gaat. Daaruit blijkt dat het naast de verschillende fysieke barrières ook moeilijk kan zijn om de weg te vinden binnen een datacenter vanwege het grote aantal verschillende (afgesloten) ruimtes. In veel gevallen zal enige medewerking van ófwel het datacenter ófwel de huurder van het rack nodig zijn om de goede server te vinden.
- **Netwerken:** Tot slot zou de aanbieder van de connectiviteit naar het internet aangesproken kunnen worden. In het uiterste geval kan de toezichthouder de internetverbinding afsluiten.

Zoals uit de omschrijving hierboven blijkt is fysieke toegang vaak wel te forceren, maar is voor logische toegang een wachtwoord vereist. Een wachtwoord is in een klein aantal gevallen te omzeilen, maar de mogelijkheid om dat hier toe te passen schatten wij heel gering in.[22] Last onder bestuursdwang kan enkel worden opgelegd als zeker is dat die last (na niet meewerken) feitelijk kan worden uitgevoerd. Een bestuursorgaan zou waarschijnlijk dus geen last onder bestuursdwang kunnen opleggen als logische toegang vereist is, omdat vooraf duidelijk is dat de last niet uitvoerbaar is. Dat betekent dat een bestuursorgaan bij

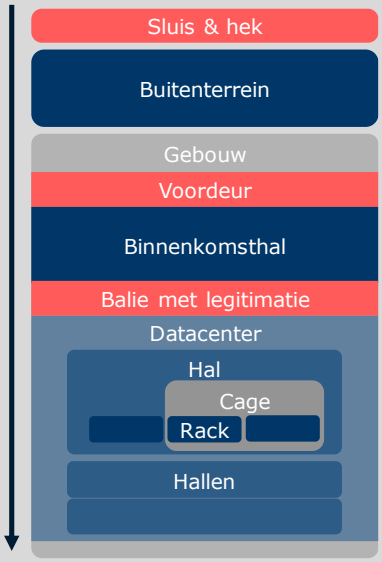
[22] Tenzij er excellente hackers worden ingezet. Mogelijk kan een dwangsom er wel toe leiden dat inloggegevens worden verstrekt.

bestuursdwang eigenlijk al laag op de escalatieladder moet beginnen en de last onder bestuursdwang eigenlijk altijd wordt opgelegd aan één van de partijen die fysieke toegang hebben.

Een datacenter binnentreden: van hek tot serverrack

De hoeveelheid beveiliging verschilt per datacenter. Hieronder wordt een algemene beschrijving gegeven.

Veel datacenters zijn gevestigd in een loods. Dit *gebouw* staat op een terrein met een *hek onder spanning* en *camerabewaking*. Middels een *sluis* is toegang te verkrijgen tot het *buitenterrein.* Vanaf het buitenterrein kan het *gebouw* worden betreden door een *deur*. Vaak is er eerst sprake van een *binnenkomsthal* met een *balie* waar een bezoeker zich moet *legitimeren*. Bij bepaalde datacenters moet er zelfs een intakeprocedure worden doorlopen om toegang te krijgen tot een bepaald deel van het datacenter. Middels een pas die bij elke deur gescand moet worden, kan de bezoeker toegang krijgen tot verschillende ruimtes. In grotere datacenters is er sprake van meerdere *hallen* en wordt er alleen toegang verleent tot de hal waar het systeem staat waarvoor de bezoeker is aangemeld. In de hal is er soms sprake van meerdere *kamers* waarin de verschillende *racks* staan. Om deze racks zit een *behuizing* heen welke is afgesloten met een *slot*. Deze racks bevatten meerdere servers. Om een groep racks kan zelfs nog een *cage* zitten.



In onderstaande box geven wij een voorbeeld van een case waarbij bestuursdwang concreet kan worden toegepast.

Voorbeeld toepassing bestuursdwang

Via een bepaald IP-adres of bepaalde link wordt aantoonbaar kinderporno aangeboden. Allereerst vindt identificatie plaats – in dit geval kan zowel via de domeinnaam, eventuele (contact)informatie op de website zelf, als via het IP-adres worden gezocht naar de identiteit van de aanbieder.

Noch de aanbieder, noch zijn leveranciers met logische toegang weigeren mee te werken. De 'eerstvolgende' dienstverlener met fysieke toegang in de keten wordt geïdentificeerd, en ook deze weigert medewerking. Deze dienstverlener bevindt zich in Nederland en er wordt overgegaan tot dwang.

Wanneer de dienstverlener op geen enkele manier meewerkt, komt een toezichthouder al snel uit bij de meest extreme acties met de grootste nevenschade (zoals het uitschakelen van een heel datacenter). Medewerking is bijvoorbeeld nodig om toegang te kunnen krijgen tot het datacenter en tot de administratie, om de juiste server (dan wel het juiste rack, et cetera) te kunnen identificeren.

Wanneer we uitgaan van een situatie waarbij er op de één of andere manier wel informatie wordt verkregen over de locatie van de server, wordt toepassing van bestuursdwang realistischer. Hiervoor is enige dus medewerking van de internetaanbieder, datacenterexploitant of (onder)huurder(s) van het rack nodig.[23] In dit voorbeeld gaan we ervan uit dat de partij die onderwerp is van bestuursdwang niet meewerkt, maar de 'dieperliggende' dienstenaanbieder wel informatie levert over de locatie van de server. De dieperliggende partij handelt dan dus niet zelf (bijvoorbeeld omdat zij niet de verantwoordelijkheid van de nevenschade op zich willen nemen).

Via het IP-adres is bepaald in welk datacenter de server staat. Met behulp van de verkregen informatie van bijvoorbeeld het datacenter en de internetaanbieder is de server van de hostingpartij die kinderporno host gevonden. De toezichthouder treedt het datacenter binnen en lokaliseert de juiste server. De server wordt uitgeschakeld en eventueel meegenomen.

4.3.2 Invloed van encryptie

Encryptie betekent dat data tijdens opslag en/of tijdens transmissie wordt versleuteld, zodat alleen de eigenaar (c.q. de partij betrokken in de transmissie) de inhoud kan ontsleutelen. In dit onderzoek kijken we naar het verwijderen van kinderporno en niet naar het blokkeren ervan (bijvoorbeeld door het toepassen van filtering); het gaat hier dus vooral om encryptie van data in opslag.

Encryptie maakt het verwijderen van data niet per definitie lastiger; versleutelde data kan net zo goed worden verwijderd als onversleutelde data. Wel kan het vele malen lastiger zijn om de content te *vinden*. Dit heeft een aantal consequenties:

- Het is moeilijker om aan te tonen dat bepaalde content daadwerkelijk op een bepaalde locatie staat opgeslagen. Zonder te beschikken over de decryptiesleutel ziet gecodeerde inhoud er (op een opslagmedium) uit als willekeurige data. De enige manier om vast te stellen dat een bepaald opslagmedium ongewenste inhoud bevat, is door vast te stellen dat de inhoud op een bepaalde manier toegankelijk is, en vervolgens te 'traceren' waar deze inhoud vandaan komt (een bepaalde server, een bepaalde schijf, et cetera).

- Het is lastig om te verifiëren dat content daadwerkelijk is verwijderd; alleen de toegankelijkheid van de content kan nog worden gecontroleerd (en daar is

[23] Of de informatie moet uit de administratie van een datacenter worden verkregen, bijvoorbeeld door vordering.

manipulatie mogelijk – bijvoorbeeld door de server zo in te stellen dat alleen de toezichthouder een 'niet gevonden'-melding krijgt te zien).

- Het verwijderen van content zonder daarbij nevenschade aan te richten wordt lastiger. Wanneer de harde schijf van een server is gecodeerd, kan een derde partij niet zien welke bestanden er op de schijf staan, noch wáár op de schijf deze zich bevinden. Als één bestand kinderporno bevat, zal de hele schijf moeten worden gewist (c.q. de hele server ontoegankelijk moeten worden gemaakt) om zeker te zijn dat het ongewenste materiaal is verwijderd.

Het automatisch vinden en wissen van ongewenste inhoud op basis van (bijvoorbeeld) hashes is eveneens onmogelijk wanneer encryptie op de opslag van servers wordt toegepast en de 'scanner' niet beschikt over de decryptiesleutel.

Merk op dat er mogelijkheden zijn om decryptiesleutels te achterhalen. Een server waarvan opslagmedia zijn versleuteld zal de inhoud immers op enig punt moeten kunnen ontsleutelen. Vaak staat de sleutel daarvoor in het geheugen van de server. Wanneer het geheugen van de server kan worden uitgelezen (bijvoorbeeld door deze te hacken, of door het geheugen letterlijk te bevriezen en over te zetten in een andere server) zou de sleutel mogelijk kunnen worden achterhaald. Dergelijke technieken worden in opsporing reeds ingezet.

4.4 Nevenschade

De onbedoelde nevenschade verschilt per niveau van ingrijpen (zie Tabel 1). Wanneer de content zeer specifiek kan worden verwijderd (in geval van websitebeheerders), is de nevenschade praktisch nul. Wanneer alles wordt verwijderd/offline wordt gehaald van een intermediaire webhoster (reseller) die meerdere servers huurt bij een datacenter en deze zelf weer gebruikt voor verschillende websites (klanten), dan is de nevenschade groter. Veel legitieme websites gaan dan ook offline. De nevenschade kan verder reiken dan enkel het offline zijn van een legitieme website. In theorie zouden zo kleine bedrijven failliet kunnen gaan, omdat ze hun dienst niet kunnen leveren. Daarnaast raakt het datacenter of de webhoster mogelijk klanten kwijt.

In paragraaf 4.3 constateren we al dat bestuursdwang eigenlijk pas uitvoerbaar wordt op het niveau van fysieke toegang. De relevante acties uit paragraaf 4.3 worden hieronder opnieuw behandeld vanuit het oogpunt van nevenschade. Per actie wordt er hier aangegeven wat het te verwachten niveau van nevenschade gaat zijn en door welke omstandigheden de mate van nevenschade kan afwijken bij de specifieke ingreep.

- **Server en aanverwante hardware**: Het uitschakelen of verwijderen van servers (fysieke hardware) heeft als gevolg dat alle websites en andere webdiensten die vanaf deze server worden aangeboden onbereikbaar worden. Het maximale aantal webdiensten dat hierdoor getroffen wordt is afhankelijk van de schijfruimte en het werkgeheugen van de hardware. Virtueel gezien bestaat er hier namelijk geen limiet. Theoretisch kunnen het dus enkele websites zijn, maar ook honderden tot duizenden. Daarnaast levert het offline zijn van sommige websites meer schade op dan andere websites. Een grote online webshop heeft hier bijvoorbeeld meer onder te lijden dan een simpele blog. Al is het wel zo dat grotere websites vaak redelijk geïsoleerd worden in datacenters.

  Een ander gevolg van het uitschakelen van de servers is dat de bestanden, de opslag en de uitvoering van programma's niet meer beschikbaar is voor de gebruikers van de server. Deze gebruikers kunnen huurders van een managed server zijn, maar ook

onderhuurders die via een resellerconstructie gebruik maken van de opslag of rekenkracht van de server.

- **Rack, cage, vloer**: Het uitschakelen of verwijderen van één of meerdere racks heeft dezelfde gevolgen als het loskoppelen van de hardware. De omvang van de gevolgen worden hier enkel velen malen groter. In één standaard rack passen namelijk ca. 42 servers.

- **Connectiviteit**: De nevenschade is het grootst als een datacenter weigert mee te werken en het AS-nummer wordt geblokkeerd. Al het verkeer is dan (tijdelijk) uitgeschakeld. Dit tast uiteraard ook de reputatie van het datacenter aan. Veel klanten willen het risico niet lopen dat hun website onbereikbaar is en zullen overstappen naar een ander datacenter.

Nevenschade kan over het algemeen geminimaliseerd worden door zo hoog mogelijk in de keten in te grijpen (zo dicht mogelijk bij de content). Aangezien bestuursdwang pas uitvoerbaar wordt op het niveau van fysieke toegang, zal dit minimaal het uitschakelen van een server betreffen. Omdat onbekend is hoeveel websites en webdiensten vanaf een server worden aangeboden, is de precieze nevenschade doorgaans niet te bepalen.

4.4.1 Blokkeren als alternatief

Wanneer partijen op hogere dienstenniveaus niet meewerken zal de verwijdering op een 'lager' niveau (dichter bij de infrastructuur) moeten worden uitgevoerd. Zoals hierboven beschreven is de nevenschade groter naarmate er op een lager niveau wordt ingegrepen. De toegang blokkeren tot specifieke inhoud is echter wél mogelijk op de hogere lagen, zonder medewerking van de betreffende partijen, en met de gewenste precisie. Een ander argument om in eerste instantie te blokkeren in plaats van te verwijderen is de eerdergenoemde bezwaartermijn in het bestuursrecht.

Hoewel een blokkade er niet voor zorgt dat het materiaal definitief verwijderd is, wordt deze ontoegankelijk via de tot dan toe gebruikte route. In de context van webhosting op het publieke internet betekent blokkeren het ontoegankelijk maken van een specifieke URL. Technisch gezien zou dit op verschillende manieren kunnen worden gerealiseerd:

- Het blokkeren van de toegang tot het IP-adres (of de IP-adressen) waar de betreffende domeinnaam naar verwijst. Dit is relatief eenvoudig te doen (het kan worden doorgevoerd in de routers van de hoster of zelfs door ISP's). In dit geval kan er nevenschade zijn doordat andere op de server gehoste websites of diensten eveneens onbereikbaar worden. Via de hoster kunnen de getroffen afnemers (inclusief de aanbieder van kinderporno) eventueel hun website of virtuele server verplaatsen naar een ander IP-adres. Het is dus essentieel dat de hoster in dit geval niet meewerkt aan het verplaatsen op verzoek van de aanbieder van kinderporno.

- Het 'overnemen' van een domeinnaam, en de verwijzing naar de server verwijderen. Hierbij vraagt de toezichthouder aan de instantie die het domeinnamenregister bijhoudt (zoals SIDN voor het .nl-domein) de domeinnaam in quarantaine te plaatsen (de domeinnaam wordt inactief *en* kan niet opnieuw worden geregistreerd). Alternatief kan de instantie waar de aanbieder van kinderporno de domeinnaam heeft geregistreerd (vaak dezelfde partij als de hostingpartij) een vergelijkbare actie uitvoeren. Deze methode wordt onder andere gehanteerd door Nederlandse ISP's voor het blokkeren van torrentwebsite The Pirate Bay. Hoewel eenvoudig te omzeilen door technisch onderlegde gebruikers is de maatregel waarschijnlijk effectief om de

meerderheid van de bezoekers tegen te houden. Daarnaast kan de domeinnaam eventueel worden gekoppeld aan een waarschuwingspagina.

- Het filteren van verkeer op applicatieniveau. Hierbij installeert het hostingbedrijf of de ISP een filter in het netwerk dat http-verzoeken inspecteert, en blokkeert indien deze bepaalde inhoud heeft. Een dergelijk filter is kostbaar (zeker voor ISP's en hosters met een groot klantenbestand), leidt mogelijk tot een trager werkende internetverbinding (alle verkeer moet immers worden geïnspecteerd) en wordt in het publieke debat gezien als onwenselijk (zie de discussies rondom netneutraliteit). Daarnaast is het filter niet effectief in te zetten bij beveiligde verbindingen, wat vandaag de dag de standaard is geworden voor het hosten van websites (https) en filesharing (FTPS/SFTP).

Merk op dat wanneer gebruik wordt gemaakt van een *Content Delivery Network* (CDN) het verkeer via een tussenpartij loopt, waardoor bovenstaande handelingen in de praktijk moeilijker uit te voeren zijn. Voor een dergelijke CDN-partij is een blokkade evenwel eenvoudig zelf te realiseren.

4.5 Kosten per overheidshandelen

De bestuursrechtelijke aanpak van kinderporno zit qua complexiteit en hoeveelheid werk/bewijslast vermoedelijk tussen de NTD-procedure en het strafrecht in. Hoewel beide geen voorbeelden zijn van bestuursdwang, en bestuursdwang vermoedelijk duurder zal zijn omdat het een laatste optie van zélf handelen betreft, helpt een indicatie van de kosten om een beeld te krijgen van de grootte van beide aanpakken:

- In 2017 behandelde het EOKM 154.897 verzoeken met gemiddeld 11 medewerkers die tezamen 7,29 fte bezetten met een budget van ca. 8 ton.[24] Dit betreft 'eenvoudige' meldingen. Kosten per melding zijn dan circa 5,17 euro.
- De politie krijgt meer dan 30.000 meldingen per jaar binnen die allemaal digitaal en deels handmatig ter selectie worden bekeken. Voor het behandelen van de meldingen, het darkweb, kindersekstoerisme en slachtofferidentificatie heeft het TBKK een bezetting van 20 fte.[25]

Er is een hoge mate van variatie in bestuursrechtzaken. De kosten van een handeling onder bestuursdwang zijn daarmee zeer lastig te bepalen. Aangezien het uitgangspunt is dat er geen medewerking is en een toezichthouder moet ingrijpen op het niveau van fysieke toegang, is het meest waarschijnlijke scenario als volgt: een medewerker reist naar een datacenter toe, breekt fysieke beveiligingen (hekken, deuren, sloten op racks) open of laat deze openbreken, vindt de juiste server, schroeft die los en neemt die mee om vervolgens de content te verwijderen. Deze handeling kan lang duren. Daarnaast moet waarschijnlijk hulp van de politie worden ingeschakeld om het datacenter binnen te komen en is enige informatie nodig over de locatie van de server (in de regel 'weet' een datacenterexploitant welke klant welke ruimte inneemt). Er zijn echter talloze variaties mogelijk, allen met een eigen kostenplaatje. Zelfs de fysieke opstelling kan per server erg verschillen, afhankelijk van de hoeveelheid en type beveiliging die een datacenter heeft. De kosten zullen vooral uitgedrukt zijn in tijd die de medewerkers kwijt zullen zijn aan een actie. Alle (redelijke)

[24] EOKM Jaarrekening 2017.

[25] Bron: interview.

kosten van overheidshandelen kunnen namelijk verhaald worden op het bedrijf dat onderwerp is van bestuursdwang.

Verder is er een hogere (vaste) hoeveelheid werk aan juridische afhandeling. Denk aan rechtszaken aangespannen door benadeelde partijen of schadevergoedingen wanneer een deur onterecht is ingetrapt.

Hoeveel personeel nodig is, is afhankelijk van het aantal keren dat bestuursdwang moet worden ingezet. Maar wanneer de bestuursrechtelijke verwijdering wordt belegd bij een organisatie zal deze waarschijnlijk niet alle zaken kunnen afhandelen en (net als de politie) moeten prioriteren. De kosten zijn daarmee een functie van de hoeveelheid budget die aan de uitvoerende instantie wordt toegekend en daarmee de ambitie. Kosten per geval zijn nauwelijks te geven vanwege dit gegeven en de variatie. Een richtlijn zou gekozen kunnen worden tussen de toepassing van NTD en strafrecht. In een verdere fase zou bijvoorbeeld een lijst met taken kunnen worden opgesteld die er moeten worden verricht in 'worst case' en 'best case'.

Denk daarnaast ook aan de kosten voor de opstart van een toezichthouder of het uitbreiden van de taken van een bestaande toezichthouder en kosten van het opleiden van medewerkers. In de tussentijd verbetert er weinig. In die zin zijn de maatschappelijke kosten nog lange tijd hoog.

4.6 Benodigde equipment en kennisniveau van een professional

De toezichthouder zal professionals nodig hebben op meerdere gebieden. Enerzijds zal er juridische expertise nodig zijn om te bepalen wat er juridisch mogelijk is in een bepaalde situatie. Anderzijds heeft een toezichthouder expertise nodig op het gebied van systeembeheer en techniek. Allereerst om de juiste partij te vinden en vervolgens om de content te vinden. Het fysiek verwijderen van content of, indien nodig, het geforceerd binnen treden van een locatie zal een taak zijn die de toezichthouder kan uitbesteden. Een goede partij hiervoor kan de politie zijn, aangezien de kennis en bevoegdheden hier toch al aanwezig zijn.

Het benodigde equipment is sterk afhankelijk van de situatie. Voor het losschroeven van een server uit een rack zal een normale gereedschapskist volstaan. Echt specifieke equipment zal enkel benodigd zijn bij het binnentreden van een datacenter in het geval dat geen enkele partij meewerkt. Dan zal de organisatie die het binnentreden ondersteunt, zoals een politieteam, het benodigde equipment wel voorhanden hebben.

5 Implementatie van handhaving op basis van bestuursrecht

In dit hoofdstuk zullen we stil staan bij de belangrijkste overwegingen bij het implementeren van een maatregel op basis van bestuursdwang ten behoeve van de bestrijding van kinderporno.

5.1 Invloed op het open karakter van het internet

Inherent aan de kwestie van overheidshandelen speelt de discussie over open internet versus de verantwoordelijkheid voor schadelijke content. De ICT-branche heeft van oorsprong een open karakter en houdt daar sterk aan vast. Internet wordt vergeleken met een tolweg, waarbij de partij die de tolweg exploiteert geen verantwoordelijkheid heeft voor wat er op zijn weg gebeurt. Het open internet kan ook zeker mooi zijn – denk aan landen waarin overheidscensuur de norm is. Diverse respondenten zijn echter van mening dat het beschermen van het internet als 'vrijplaats' een gepasseerd station is: de (commerciële en maatschappelijke) belangen zijn te groot.

Naast de zorgen rondom proportionaliteit van de maatregel, speelt ook de kwestie van scope creep. Een bestuursrechtelijk instrument moet strak gedefinieerd zijn, met name als het gaat om de doelgroep (om welke partijen gaat het?) en afbakening van het onderwerp. Hoewel het onderwerp kinderporno relatief goed is af te bakenen (zodanig dat "onmiskenbare onrechtmatigheid" evident is), is er mogelijk precedentwerking: vanuit bestrijding van andere maatschappelijke onwenselijke zaken (zoals pro-ana-forums[26], online kansspelen, en online haatzaaien[27]) zal mogelijk worden gewezen op het voor kinderporno ingerichte instrument. Dat kan leiden tot een 'glijdende schaal' (of scope creep), waarbij steeds meer content op internet 'gecensureerd' kan worden. Zelfs met een goede afbakening van het instrument is het mogelijk dat het instrument later toch nog wordt verbreed (want het instrument bestaat toch al), zodat het ook op andere content kan worden toegepast.

Daarnaast moet niet alleen de doelgroep strak gedefinieerd zijn, maar ook de drempel waarna het instrument kan worden toegepast. Het zou een hinder kunnen zijn voor het open internet als het instrument te makkelijk wordt ingezet. Als het instrument enkel wordt ingezet als ultimum remedium, om het structureel plaatsen van de content aan te pakken, dan blijft die hinder beperkt. Met andere woorden, het moet duidelijk zijn dat de introductie van deze maatregel geen invloed gaat hebben op de bestaande zelfregulering en alleen wordt toegepast wanneer deze faalt (dus in geval van bad hosters).

Dat moet duidelijk gecommuniceerd worden naar de sector. Zoals eerder beschreven is er in theorie namelijk sprake van enige wisselwerking met de zelfregulering wanneer bestuursdwang (te) gemakkelijk wordt ingezet. In een situatie waarin de hoster weigert mee te werken maar de aanbieder van de datacenterruimte de content wel wil verwijderen/ontoegankelijk maken, zou toepassing van bestuursdwang op de hoster minder nevenschade met zich meebrengen dan uitoefening van de zelfregulering waarbij de aanbieder van de datacenterruimte vrijwillig een rack offline haalt. In extreme gevallen kan

[26] Forums van mensen die eetstoornissen als levensstijl beschouwen.

[27] In deze gevallen is de inhoud van het plaatje echter niet strafbaar, maar de toepassing ervan wel. Dat kan een belangrijk onderscheid zijn.

deze realisatie ervoor zorgen dat bedrijven eerder achteroverleunen en acties liever aan de toezichthouder laten.

5.2 Bestuursdwang vs. andere oplossingen

Het vertrekpunt van dit onderzoek was het AKD-advies, ofwel toepassing van bestuursdwang. Dat is dan ook de scope van dit onderzoek. Bestuursdwang kent vele voordelen, zoals een mogelijk snellere rechtsgang en meer handelingsmogelijkheden. Toch plaatsten veel respondenten vraagtekens bij de keuze voor bestuursdwang en daarom willen we hier kort ingaan op andere geopperde oplossingsrichtingen.

Een voorwaarde voor de toepassing van bestuursdwang is dat de betreffende bad hoster geïdentificeerd kan worden. In interviews is gepleit voor een systeem waar het verplicht wordt voor iedereen om zich kenbaar te maken, bijvoorbeeld aan de hand van ***legal entity identifiers***. Idealiter weten we namelijk van iedere website/IP wie de 'bovenste' klant is, hoewel dit ook nadelen heeft in het kader van privacy.

ACM heeft andere, niet-bestuursrechtelijke routes verkend om de bad hosters aan te pakken. Zo is gekeken naar de peeringovereenkomsten die de hosters hebben met andere partijen; deze partijen kunnen attent worden gemaakt op het feit dat zij zakendoen met een partij die voornamelijk slechte content host, in de hoop dat zij hier consequenties aan verbinden. Een vorm van ***'naming and shaming'*** zou effectief kunnen zijn.[28] We merken overigens op dat het onbekend is in hoeverre bad hosters geschaad zouden worden door het verlies van bonafide klanten.

Een andere optie zou zijn om het ***wetboek van strafvordering*** aan te passen, zodat ook onder dit instrument efficiënter kan worden gehandeld. Rechtstreeks vorderen (toepassing strafrecht, artikel 54a procedure) is in essentie een daadkrachtige maatregel. Dit kan wellicht efficiënter door het introduceren van spoedprocedures via rechters of in bijzondere (nood)situaties kan rechtelijke toestemming achteraf geoorloofd zijn.[29] Deze optie raakt aan organisatorische problemen. Er is momenteel te weinig capaciteit bij de partij die het meest kundig is in het oppakken van de moeilijkere zaken (justitie/rechtbanken).

5.3 Werkwijze in andere landen

INHOPE is een samenwerkend wereldwijd netwerk van hotlines en coördineert internationaal het doorspelen en afhandelen van meldingen van online kinderporno. Via het INHOPE netwerk belandt een melding bij het meldpunt van het land waar het materiaal wordt gehost.

In de meeste landen is de werkwijze vergelijkbaar met de Nederlandse situatie: de sector wordt veelal vrijgelaten om zelf te reguleren en er is een meldpunt van waaruit NTD-meldingen worden doorgestuurd naar website hosters.

Er zijn echter ook landen waar vooral wordt ingezet op het filteren van verkeer en blokkeren van content aan de kant van de ISP's. In het Verenigd Koninkrijk geeft de Internet Watch Foundation een lijst met te blokkeren websites aan hun leden. Een groot deel van de ISP's gebruikt deze lijst ook daadwerkelijk.[30] De ISP British Telecom (BT) heeft hier een eigen

[28] Zie ook de motie van de leden Van Oosten en Buitenweg (6 juni 2018). 29 270 nr. 128.

[29] Vergelijk ook met het wetsvoorstel computercriminaliteit iii (www.rijksoverheid.nl).

[30] Publications.parliament.uk

filter systeem voor opgezet onder de naam Cleanfeed. Dit systeem van BT wordt ook door andere ISP's in het Verenigd Koninkrijk gebruikt.

Een soortgelijk Cleanfeed systeem is eveneens in gebruik in Canada, maar de deelname van ISP's is ook daar vrijwillig.[31] Dit in tegenstelling tot Italië waar sinds 2007 voor ISP's het blokkeren van dergelijke content juist wettelijk verplicht is gesteld.[32]

In Frankrijk wordt de problematiek aangepakt middels de LOPPSI2 wet.[33] Deze wet kan ISP's opleggen de toegang tot gehoste kinderporno te blokkeren aan de hand van een lijst met te verbieden sites. De manier waarop ISP's deze inhoud blokkeren is aan de ISP zelf. Voor content gehost vanuit Frankrijk kan een rechter door deze wet de hoster opleggen de content te verwijderen of de website offline te halen.

De Nederlandse ICT-sector staat bekend om zijn openheid, dus waarschijnlijk is het verplichten tot filteren of blokkeren niet gewenst. Wel zou het delen van lijsten met sites of het aanbieden van een filtersysteem aan ISP's kunnen bijdragen aan de aanpak. Feitelijk wordt dit al gedaan door de hashdatabase die het EOKM sinds kort aanbiedt aan ISP's. Op deze wijze kunnen zij zelf de (geüploade) content controleren.

5.4 Een uitzonderlijke case

In interviews werden wij meermaals gewezen op een specifieke case waarop toepassing van bestuursdwang erg moeilijk zou zijn. De partijen in kwestie baseren hun bedrijfsmodel (deels) op het feit dát ze uitzondering zijn ("bulletproof hosting"). Hun bedrijfsmodel - waarin gebruik wordt gemaakt van katvangers - maakt het lastig te achterhalen welke Nederlandse partij onderwerp van bestuursdwang moet worden en dus strandt de actie al bij het eerste proces, namelijk het identificeren.

Figuur 6 geeft de case schematisch weer. In deze case heeft webhoster Z content staan op één van de servers van hostingprovider Y. Hostingprovider Y huurt dit rack aan servers in bij hostingprovider X. De racks van hostingprovider X staan in datacenter W. Van deze partijen zijn X, Y en Z alle drie in het buitenland gevestigd en is alleen datacenter W in Nederland gevestigd.

Bestuursdwang zou hier inhouden dat – wanneer niemand meewerkt – een toezichthouder naar datacenter W zou reizen om handmatig servers of racks (afhankelijk van in hoeverre kan worden vastgesteld waar de kinderporno-content staat) te verwijderen. Het probleem is echter dat een toezichthouder niet bij datacenter W uitkomt.

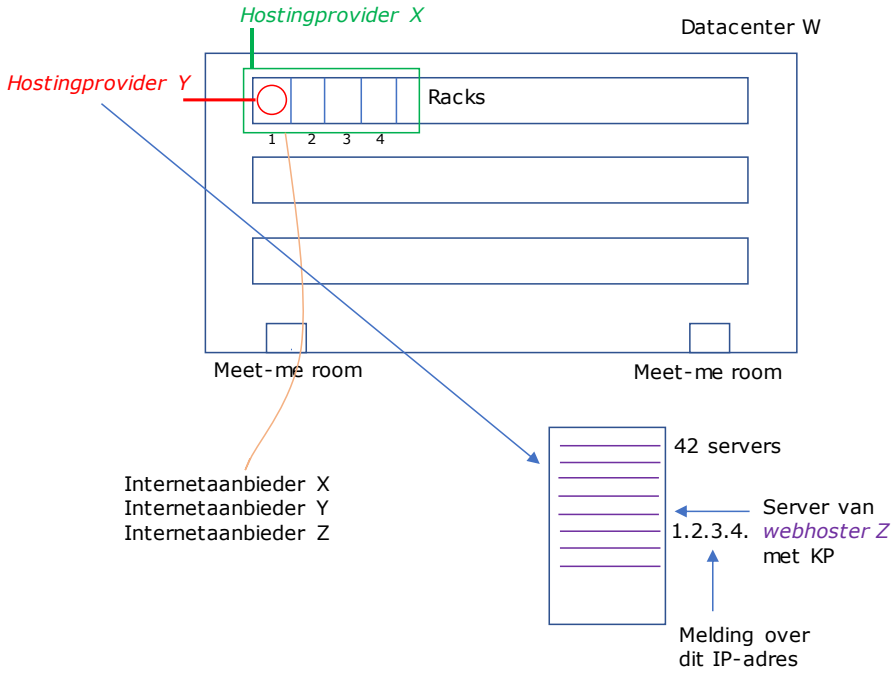
De melding komt namelijk binnen over het IP-adres van partij Z. Dit IP-adres staat geregistreerd onder het AS-nummer van Y. Dit is echter een buitenlandse partij die weigert mee te werken en niet in Nederland geregistreerd staat. Indien een toezichthouder al uitkomt bij hostingprovider Y (buitenlandse partij die niet meewerkt), dan valt dus niet te achterhalen in welk datacenter de content van Z staat. In deze constructie komt naar voren dat het lastiger wordt te achterhalen waar de content staat, omdat partijen in het buitenland gevestigd zijn en hostingprovider X gebruik maakt van een resellerconstructie.

[31] www.cybertip.ca

[32] www.reuters.com

[33] www.assemblee-nationale.fr

Bestuursdwang is niet toe te passen op buitenlandse partijen en medeplichtigheid/medeverantwoordelijkheid is lastig aan te tonen, want partijen beroepen zich op het argument dat ze niet (kunnen/willen) weten wat er op hun infrastructuur gebeurt.



Figuur 6. Voorbeeld van een uitzonderlijke case.

Als er gebruik wordt gemaakt van VPS kan het zelfs nog ingewikkelder worden. Zoals de case nu in Figuur 6 staat uitgetekend, zouden er namelijk maar 42 servers vanuit het rack van hostingprovider Y worden gedraaid. Als één van die servers wordt gehuurd aan een partij die er een VPS op draait, dan kunnen er op virtueel niveau nog veel meer servers worden gedraaid welke elk weer aan een andere partij kunnen worden verhuurd.

Toepassingsmogelijkheden vanuit het bestuursrecht lijken hier dus beperkt, wat dit één van de cases maakt die uiteindelijk toch echt door het strafrecht opgepakt zal moeten worden.

6 Conclusie en aanbevelingen

In dit laatste hoofdstuk vatten we tot slot de belangrijkste conclusies samen (paragraaf 6.1) en formuleren we enkele aanbevelingen voor de overheid (paragraaf 6.2).

6.1 Conclusies

- Zelfregulering van de sector (ISP's en HSP's) voor het verwijderen van online kinderporno werkt goed[34] voor het afhandelen van de meerderheid van de meldingen vanuit het EOKM. Content wordt vrijwillig en in essentie binnen 24 uur verwijderd. Er wordt echter niet altijd adequaat gereageerd op deze meldingen, wat aanleiding is voor de overheid om op zoek te gaan naar aanvullende instrumenten om de partijen die niet meewerken aan te pakken. Het gaat hier zowel om partijen die niet mee (denken te) kunnen werken en partijen die niet mee willen werken, de zogenaamde 'bad hosters'.

- Een instrument op basis van bestuursrecht kan worden gepositioneerd tussen de huidige notice-and-takedown-procedure vanuit de zelfregulering en het strafrecht. Het stelt een toezichthouder in staat om harder op te treden in geval er (herhaaldelijk) door eenzelfde partij niet of traag wordt meegewerkt aan een verwijderverzoek. Bestuursrecht kan worden toegepast op partijen die acteren op Nederlands grondgebied.

- Bestuursdwang is de uiterste actie die een toezichthouder binnen dit kader van bestuursrecht kan toepassen, waarbij de toezichthouder zélf acties onderneemt om inhoud te (laten) verwijderen. Als gevolg van de bezwaartermijn die er bestaat betekent verwijdering in de praktijk het ontoegankelijk maken van materiaal en het (na minimaal zes weken) daadwerkelijk verwijderen ervan.

- Vanwege de stapeling van diensten in de ICT-sector (een hoster neemt een server af van een partij die weer datacenterruimte afneemt van een andere partij) valt het toepassen van bestuursdwang uiteen in twee processen:

    1. Het *identificeren* van de partij waarop bestuursdwang kan worden toegepast;
    2. Het daadwerkelijk *toepassen* van bestuursdwang.

- Binnen de groep bad hosters zullen er vermoedelijk ook partijen zijn voor wie bestuursrecht geen oplossing zal bieden. Dit omdat de juiste (Nederlandse) partij niet kan worden geïdentificeerd, bijvoorbeeld vanwege het gebruik van (buitenlandse) katvangers. Deze partijen kunnen beter via het strafrecht worden aangepakt.

- In beginsel zou bestuursdwang moeten worden toegepast op de partij die daadwerkelijk verantwoordelijk is voor het aanbieden van het strafbare materiaal. Meestal gaat dit om een partij waarbij logische toegang (inloggegevens) nodig is om bij de content te komen. Een toezichthouder zou waarschijnlijk echter geen last onder bestuursdwang kunnen opleggen als logische toegang vereist is, omdat vooraf

[34] Hoewel er altijd verbetering mogelijk is.

duidelijk is dat de last niet uitvoerbaar is (zonder medewerking kan de toezichthouder niet bij de content komen). Dat betekent dat de last onder bestuursdwang eigenlijk altijd wordt opgelegd aan één van de partijen die fysieke toegang hebben. Het zelf uitvoeren van een verwijdering door een toezichthouder is wel (praktisch) uitvoerbaar wanneer het gaat om fysieke infrastructuur (het fysiek uitschakelen van servers).

- Daarbij geldt dat het zonder enige informatie (en dus medewerking van 'dieperliggende' partijen in de keten, zoals een datacenterexploitant) over de locatie van de server met kinderporno, bijna onmogelijk is om als toezichthouder bij de specifieke server te komen. Wanneer op geen enkele manier wordt meegewerkt, komt een toezichthouder al snel uit bij extreme acties, zoals het uitschakelen van de connectiviteit richting een datacenter.

- Nevenschade kan over het algemeen geminimaliseerd worden door zo hoog mogelijk in de keten in te grijpen (zo dicht mogelijk bij de content). Aangezien bestuursdwang pas uitvoerbaar wordt op het niveau van fysieke toegang, zal dit minimaal het uitschakelen van een server betreffen (hierbij moet dan wel informatie worden vrijgegeven over waar de server is opgehangen). Omdat onbekend is hoeveel websites en webdiensten vanaf een server worden aangeboden, is de precieze nevenschade onbekend. Hoe dieper in de keten wordt ingegrepen, hoe groter de potentiële nevenschade (tot aan het uitschakelen van de connectiviteit richting een datacenter).

6.2 Aanbevelingen

- We verwachten dat er een positief effect uit zal gaan van de 'dreiging' van bestuursdwang – namelijk dat dienstverleners eerder en sneller zullen meewerken aan een verwijderverzoek. Juridisch gezien is het echter mogelijk lastig om een instrument te definiëren waarvan wordt voorzien dat het slechts beperkt wordt ingezet (als 'laatste redmiddel'). We bevelen aan deze implicaties te onderzoeken.

- In de praktijk wordt bestuursdwang gezien als een middel om de resterende kleine groep 'bad hosters' aan te pakken. Dienstverleners die nu meewerken in de zelfregulering geven aan dat invoering van bestuursdwang voor deze groep weinig verandert, maar wel aanvullend 'juridisch risico' met zich meebrengt. We bevelen aan om in de formulering van het instrument duidelijk op te nemen dat bestuursdwang enkel kan worden ingezet als de zelfregulering faalt.

- Overweeg een 0- en 1-meting om de effectiviteit van het instrument te bepalen, mocht bestuursdwang worden ingevoerd.

- Gezien de bezwaartermijn die geldt voor bestuursdwang zal rekening moeten worden gehouden met tijdelijke opslag (een soort 'escrow') van de verwijderde dan wel ontoegankelijk gemaakte inhoud.

- Er bestaat bij de diverse betrokken partijen scepsis over de vraag of bestuursdwang het middel is om specifieke bad hosters aan te pakken. Technisch gezien verwachten we vooral beperkte inzetbaarheid bij bulletproof hosters die gebruik maken van ingewikkelde constructies (bijv. katvangers) om onder de radar te blijven. Het alternatief voor aanpak van deze partijen is het strafrecht. Overweeg in dit kader of last onder bestuursdwang de juiste aanpak van bad hosters is.

Bijlage 1. Overzicht gesprekspartners

Naam	Functie/organisatie
Alex de Joode	Public policy manager Nederland ICT
Arda Gerkens	Directeur EOKM
Arie van Bellen	Directeur ECP
Dave Jansen	Teamleider TBKK Nationale Recherche Landelijke Eenheid
Egon Berghout	Hoogleraar informatiesystemen RuG
Eldert van Wijngaarden	Directeur Web-IQ
Elmar Krack	Public/regulatory affairs manager VodafoneZiggo
Erik Jan Hofstede	CTO Antagonist
Evert Jan Hummelen	Teammanager, Directie Consumenten ACM
Gert Wabeke	Manager Lawful Intercept KPN
Lesley Koomen	Team Manager Compliance Leaseweb
Maarten Simon	Jurist SIDN
Michiel Steltman	Directeur DINL
Nico van Eijk	Hoogleraar informatierecht UvA
Paul Knol	Senior Regulatory Officer KPN
Rejo Zenger	Beleidsadviseur Bits of Freedom
René Blankestein	Government security affairs manager VodafoneZiggo
Richard Vroegop (per e-mail)	Lead engineer NForce
Roelof Meijer	Algemeen directeur SIDN
Rory Breuk	Security officer TransIP
Stijn Grove	Directeur Dutch Datacenter Association
Sven Visser	Voorzitter DINL, oprichter CYSO en voorzitter DHPA
Thijs Eleveld	Case Officer Abuse WorldStream
Wido Potters	Voorzitter ISPConnect en manager BIT

Contact:
Dialogic innovatie & interactie
Hooghiemstraplein 33-36
3514 AX Utrecht
Tel. +31 (0)30 215 05 80
www.dialogic.nl