Beeldmateriaal van seksueel misbruik van minderjarigen

Tijdelijke Onderzoekscommissie Georganiseerd Sadistisch Misbruik van Minderjarigen (Commissie Hendriks)

21 december 2022

Inleiding

Wanneer een persoon aangeeft als minderjarige slachtoffer te zijn geweest van georganiseerd sadistisch seksueel misbruik (al dan niet met rituele en/of satanische aspecten) en besluit een melding of aangifte te doen, is het voor politie en het Openbaar Ministerie (OM) nodig een verdachte, getuigenissen of aanvullend bewijs – bijvoorbeeld beeldmateriaal – te hebben om tot een kansrijke aangifte en vervolging te komen van de beschuldigden. In geval van dit type misbruik is dat vaak ingewikkeld. Vermeende daders worden zelden genoemd door het slachtoffer zelf of door de omgeving omdat slachtoffers bang zijn voor repercussies van de dader(s). Volgens de slachtoffers zijn er wel getuigen die ook slachtoffers zijn; zij zouden echter dezelfde drempels ervaren om erover naar buiten te treden, zo geven zij aan in aan de Tweede Kamer toegestuurde brieven.[1] Aanvullend en belastend beeldmateriaal vergroot de kans op veroordeling van de dader(s). Slachtoffers van georganiseerd sadistisch misbruik rapporteren in interviews die de Commissie afnam regelmatig dat er beeldmateriaal is gemaakt van het misbruik dat zij hebben ondergaan. Dit zou op gegevensdragers staan of via – voor velen verborgen delen van – het internet verspreid worden. Op deze beelden zouden het seksuele misbruik, de daders en/of andere (minderjarige) slachtoffers te zien zijn.

Dit deelrapport richt zich op thema's rondom beeldmateriaal dat vervaardigd is van seksuele handelingen van misbruik van of door minderjarigen. Eerst zal de algemene context van beeldmateriaal van seksueel misbruik van minderjarigen worden beschreven, waaronder de aard en omvang, alsmede de politieke aandacht voor dit onderwerp. Vervolgens wordt dieper ingegaan op technische aspecten van opsporing en detectie van beeldmateriaal van seksueel misbruik. Waar wordt het opgeslagen of gedeeld? Hoe werkt het *Darkweb*? Over welke opsporingstechnieken beschikken opsporingsdiensten, en wat zijn de technische en juridische obstakels en beperkingen daarbij? Aanvullend wordt besproken welke Nederlandse initiatieven er zijn om beeldmateriaal van seksueel misbruik te onderscheppen, en in hoeverre (Nederlandse) organisaties die zich bezighouden met beeldmateriaal gevallen tegen zijn gekomen van georganiseerd sadistisch seksueel misbruik met rituele en/of satanische aspecten van minderjarigen.

Methode

Er is in de literatuur gezocht op de zoektermen *Child sexual abuse material* (CSAM), *Child sexual exploitation material* (CSEM)[2]*, Ritual abuse* en *Satanic abuse* in combinatie met

[1] In het deelrapport *Brieven van slachtoffers* staat de inhoud van deze brieven beschreven.

[2] *Child sexual abuse material* (CSAM) omvat materiaal dat op handelingen van seksueel misbruik en/of gericht is op de genitaliën van een minderjarige. *Child sexual exploitation material* (CSEM) omvat alle seksueel getinte beelden van minderjarigen, waaronder CSAM. Het onderscheid is vooral juridisch.

Material, indecent images of children (IIOC), en de Nederlandse equivalenten van deze zoektermen. Deze zoekopdracht gaf inzicht in de aard en omvang van beeldmateriaal, in strategieën van detectie en opsporing, en in de technische aspecten daarvan. Omdat veel literatuur over seksueel misbruik van minderjarigen in het algemeen gaat, is geen systematische review uitgevoerd, maar zijn de voor de Commisie relevante aspecten uit de literatuur samengevat. Organisaties uit Nederland die zich richten op slachtoffers van online seksueel misbruik zijn bevraagd over of zij beeldmateriaal van minderjarige slachtoffers van georganiseerd sadistisch misbruik (met rituele en/of satanische aspecten) zijn tegenkomen in de casussen die zij onder ogen hebben gekregen. Hiervoor zijn ten eerste overheidsorganisaties benaderd die advies geven over monitoring of opsporing van beeldmateriaal. Ten tweede zijn enkele particuliere organisaties benaderd die zelfstandig of in samenspraak met de overheid onderzoek verrichten naar verschillende vormen van beeldmateriaal van seksueel misbruik. Tot slot heeft de Commissie gesprekken gehouden met vertegenwoordigers van het OM en dataspecialisten van het Team Bestrijding Kinderporno en Kindersekstoerisme (TBKK) van de Landelijke Eenheid om meer kennis te verkrijgen over de juridische en technische aspecten van de opsporing van beeldmateriaal van seksuele handelingen met minderjarigen.

Wanneer er in dit rapport over beeldmateriaal gesproken wordt, dan kan dit gaan om tekeningen van slachtoffers, fysieke of digitale foto's of video- of livestreamopnamen. Het digitale materiaal kan opgeslagen zijn op gegevensdragers (diskettes, cd-roms, usb-sticks of externe harde schijven) of laptops of desktops.

Ontwikkelingen in omvang en aard van beeldmateriaal van minderjarigen

Sinds de eeuwwisseling is online seksueel misbruik wereldwijd sterk toegenomen in omvang, mede door het toegenomen gebruik van internet (Negreiro, 2020). De aard van dit online seksueel misbruik varieert van zelfgemaakte seksueel getinte foto's of video's die op het internet belanden tot sadistische verkrachting van soms zeer jonge kinderen.

Voor wat betreft de omvang van beeldmateriaal van seksuele handelingen bij minderjarigen is het een onmogelijke taak om in kaart te brengen om hoeveel beeldmateriaal het gaat en wat het aandeel van (zeer) ernstig misbruik is. Slechts een deel van het materiaal staat online, en verder wordt het via verschillende routes verspreid en op meerdere plekken opgeslagen. Wijdverspreid opererende organisaties geven in hun jaarlijkse rapportages enig zicht op de ontwikkelingen in de omvang. De *Internet Watch Foundation* (IWF)[3]

[3] De IWF is een onafhankelijke organisatie in het Verenigd Koninkrijk die sinds 1996 inhoud bestrijdt die seksueel misbruik van kinderen op internet laat zien. Via hotlines is het mogelijk om meldingen te doen van

rapporteerde over seksueel misbruik bij minderjarigen in 2010 rond de 1 miljoen meldingen om verder te onderzoeken; in 2019 waren dit 19 miljoen meldingen over misbruik bij minderjarigen van álle 70 miljoen plaatjes en video's van algemeen seksueel misbruik die bij de IWF zijn gemeld. In 2021 was het aantal te analyseren meldingen van beeldmateriaal van minderjarigen bijna 30 miljoen. Voor de Europese Unie gaat het om een toename van 23.000 meldingen in 2010 naar 725.000 meldingen in 2019. In 2019 ging het in totaal om drie miljoen plaatjes en video's van seksuele handelingen bij minderjarigen om te onderzoeken volgens het *National Centre of Missing and Expoited Children* (NCMEC).[4] Zowel de totale omvang van het online beeldmateriaal als het aantal jaarlijkse meldingen nemen dus toe.

In de laatste vijf jaar is de Europese Unie het continent geworden waar het meeste aanbod van online beeldmateriaal te vinden is. In 2019 was 90% van de URL's (*uniform resource locator* oftewel website-adressen) waarvan bekend is dat ze online beeldmateriaal bevatten gehost in Europa.[5] Binnen Europa staat Nederland bovenaan als het land met de meeste hostingruimte voor URL's met beeldmateriaal van seksueel misbruik van minderjarigen; in 2019 iets meer dan 71% van het totaal (European Commission, 2020).[6] In gesprek met dataspecialisten van het TBKK geven zij aan dat dit voornamelijk komt doordat Nederland een 'goede technische infrastructuur' heeft, wat het aantrekkelijk maakt om hier serverruimte te kopen. Ter nuancering merken zij op dat dit niet betekent dat het materiaal hier gemaakt wordt (TBKK, persoonlijke communicatie, 20 juni 2022). In 2019 zijn Nederlandse hostingbedrijven door de IWF gevraagd om 94.000 webpagina's met daarop elk honderden of duizenden plaatjes en video's te verwijderen (European Commission, 2020). Opsporingsinstanties en onafhankelijke partijen, zoals het Meldpunt Kinderporno van het Expertisebureau Online Kindermisbruik (EOKM), verzenden meldingen naar hostingbedrijven, waarin zij hen verzoeken om beeldmateriaal van seksueel kindermisbruik binnen 24 uur offline te halen. Nederlandse en Europese hostingbedrijven zijn niet wettelijk verplicht om proactief actie te ondernemen tot het opsporen van beeldmateriaal, maar zijn wel verantwoordelijk voor het verwijderen ervan nadat zij officieel genotificeerd zijn (EOKM,

---

foto's of video's van seksueel misbruik van kinderen. De stichting ziet in samenwerking met andere justitiële partijen toe op de verwijdering ervan. Er is een wettelijke basis om proactief op het internet naar materiaal te zoeken om het te verwijderen. Bron cijfers: *EU Strategy for a more effective fight against child sexual abuse. (z.d.). Migration and Home Affairs.* Geraadpleegd op 6 juli 2022, van https://home-affairs.ec.europa.eu/policies/internal-security/child-sexual-abuse/eu-strategy-more-effective-fight-against-child-sexual-abuse_en

[4] Het NCMEC is een particuliere non-profitorganisatie die zich sinds 1984 inzet voor vermiste en uitgebuite kinderen. Wetgeving verplicht internetserviceproviders (ISP's) melding te maken van de aanwezigheid van (potentieel) kinderpornografisch materiaal op hun servers. Het NCMEC sorteert die meldingen per land en stuur ze door naar de nationale opsporingsdiensten.

[5] Bron cijfers over 2020: *CyberTipline Data.* (z.d.). *National Center for Missing & Exploited Children.* Geraadpleegd op 19 juli 2022, van https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata

[6] Hierover is begin mei 2020 een Kamervraag gesteld door Van Wijngaarden (VVD) aan de toenmalige minister van Justitie en Veiligheid Grapperhaus (Tweede Kamer, vergaderjaar 2019-2020, Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden, nr. 3147).

persoonlijke communicatie, 27 juli 2022). Onderzoekers van de Technische Universiteit Delft werken sinds 2018 aan een 'CSAM-hostingmonitor' die aangeeft door welk Nederlands bedrijf dit materiaal wordt gehost en hoe lang de bedrijven doen over het verwijderen na verzoek daartoe (Lone *et al.*, 2020, Lone *et al.*, 2022). Onder de toenmalige minister Grapperhaus is ingezet op het versterken van bestuursrechtelijke maatregelen om bedrijven ertoe aan te zetten het beeldmateriaal van hun server binnen korte tijd te verwijderen (waarover later meer in dit deelrapport). De analisten van het TBKK merken de laatste jaren meer bereidheid van bedrijven om in het kader van maatschappelijk verantwoord ondernemen (MVO) hier een plan van aanpak voor te maken. Wel geven ze aan dat een obstakel is dat eigenaren uit binnen- en buitenland de digitale ruimte verder onderverhuren aan derden. Het is hierdoor voor het hostingbedrijf en voor de primaire koper niet na te gaan wat de onderhuurders met deze ruimte doen (TBKK, persoonlijke communicatie, 20 juni 2022).

De omvang van beeldmateriaal is dus verveelvoudigd. De IWF en het NCMEC rapporteren over (de ontwikkelingen in) de aard van de inhoud van het beeldmateriaal. Het gaat om een grote variëteit in de ernst van het misbruik dat te zien is. Beeldmateriaal geeft logischerwijs alleen zicht op wat gefotografeerd of gefilmd is. Of en hoe ernstig het misbruik is voor en na het creëren van het beeldmateriaal is niet te achterhalen. Een klein aandeel van het beeldmateriaal is extreem gewelddadig en sadistisch, zoals *hurtcore*. Uit de gegevens van de IWF en het NCMEC blijkt dat in 2019 bijna de helft (46%) van het materiaal van kinderen van 10 jaar of jonger was. Uit een analyse van beeldmateriaal blijkt dat het misbruik in deze leeftijdscategorie voor bijna eenderde van de hoogste ernstcategorie A[7] is.

Ook de wijze waarop daders hun nieuwe slachtoffers online vinden, is in de afgelopen decennia veranderd. Als gevolg van de uitbraak van de coronapandemie hebben de lidstaten van de Europese Unie ingrijpende quarantainemaatregelen aan hun burgers opgelegd, waaronder beperkingen in het reizen en bij het uitgaan en lockdowns. De ontmoetingskansen in het echte leven namen hierdoor af. Criminelen hebben van deze omstandigheden gebruikgemaakt door hun werkwijzen aan te passen of door andere criminele activiteiten te ontplooien (Europol, 2020; Negreiro, 2020). Vooral beelden gerelateerd aan *sextortion* (afpersing met zelfgemaakte en aan de afperser opgestuurde foto's) en online *grooming* komen vaak voor (Negreiro, 2020). Ook het aandeel van cybersekstrafficking is relatief groot. Cybersekshandelaren brengen hiervoor minderjarigen onder in *cybersex dens* (locaties waar het misbruik dat wordt opgenomen plaatsvindt). Via webcams kan het seksueel misbruik in *realtime* gestreamd worden aan een koper. Onderzoek uit 2020 van de *National Crime Agency* in het Verenigd Koninkrijk liet zien dat

[7] IWF-categorie A is het meest ernstig, waarbij er sprake is van seksueel binnendringen, beelden waarop seksuele activiteit met dieren te zien is, of sadisme. Categorie B zijn andere handelingen zonder binnendringen, en categorie C zijn de relatief minder ernstige situaties die niet vallen onder A of B (IWF-jaarverslag 2021).

beelden van uitbuiting van minderjarigen binnen ‘drie keer klikken’ ook via een reguliere zoekmachine te vinden zijn.[8]

Politieke aandacht voor beeldmateriaal

Zowel op mondiaal niveau als op nationaal niveau staat het onderwerp beeldmateriaal van seksueel misbruik van minderjarigen hoog op de politieke agenda, mede door de toename van de hoeveelheden beeldmateriaal op internet. In de jaren van de coronacrisis zijn de modus operandi en het online aanwezig zijn van minderjarigen op internet, socialemediaplatformen of online videogames veranderd (Europol, 2020). De kwetsbaarheden hiervan worden als blijvende dreiging gezien volgens de rapportage van de *Internet Organised Crime Threat Assessment 2020* door Europol (2020). Ook in Nederland is het bestrijden van online kindermisbruik een belangrijk speerpunt voor politiek en voor uitvoeringsinstanties die belast zijn met opsporing (zie hierover volgende paragraaf). Periodiek rapporteert de minister over de initiatieven die ondernomen zijn of zullen worden in de *Aanpak online seksueel kindermisbruik en zeden* (Tweede Kamer, 2021-2022, 34843, nr. 52). De toenmalige minister Grapperhaus heeft enkele wetsvoorstellen en wetten gemaakt die relevant zijn om te noemen in de context van seksueel misbruik van minderjarigen.

Medio 2020 is een wetvoorstel gedaan dat voorbereidingshandelingen met het oog op het plegen van seksueel misbruik van een kind zelfstandig strafbaar wil stellen (toevoeging 240c WvSr). Dit betreft een uitwerking van de aangenomen motie van Van Wijngaarden over het strafbaar stellen van het ‘pedohandboek’[9] en vraagt om het strafbaar stellen van gedragingen als het (online) verspreiden, verwerven of in bezit hebben van *“instructief materiaal tot het plegen van kindermisbruik”*. Medio september 2022 is dit wetsvoorstel aangenomen.[10]

In november 2020 is wetgeving aangekondigd die de vorming van de Autoriteit kinderpornografische en terroristische content mogelijk maakt (Tweede Kamer, 31 015 en 29 754, nr. 208). Dit wordt een zelfstandig bestuursorgaan dat bedrijven kan verplichten om beeldmateriaal te verwijderen op straffe van bestuurlijke boetes. Hiermee heeft Nederland

[8] National Crime Agency (Red.). (2020, 14 februari). European police chiefs back NCA demands for tech companies to do more to prevent child sex abuse. *National Crime Agency*. Geraadpleegd op 30 juni 2022, van https://www.nationalcrimeagency.gov.uk/news/european-police-chiefs-back-nca-demands-for-tech-companies-to-do-more-to-prevent-child-sex-abuse

[9] Meer informatie over dit handboek: https://www.rtlnieuws.nl/nieuws/nederland/artikel/4052086/gevaarlijk-pedohandboek-ongestoord-verspreid-internet-politiek-wil

[10] Ministerie van Justitie en Veiligheid. (2022, 13 september). *Tweede Kamer stemt in met maximale gevangenisstraf van 4 jaar voor bezit pedohandboek*. Nieuwsbericht | Rijksoverheid.nl. Geraadpleegd op 19 september 2022, van https://www.rijksoverheid.nl/actueel/nieuws/2022/09/13/tweede-kamer-stemt-in-met-maximale-gevangenisstraf-van-vier-jaar-voor-bezit-pedohandboek

meer zicht op de aanwezigheid van dergelijk materiaal op Nederlandse servers en is men niet afhankelijk van meldingen uit het buitenland. Het EOKM stuurt verwijderverzoeken van onlinemateriaal uit naar bedrijven (waarover later meer in het deelrapport). De Autoriteit richt zich dan ook op verwijderverzoeken waaraan geen gehoor wordt gegeven door aanbieders van communicatiediensten die beeldmateriaal van seksueel kindermisbruik hebben opgeslagen. Medio 2022 is deze wet in consultatie.

In mei 2022 kondigde de Europese Commissie een wetsvoorstel aan om strengere maatregelen mogelijk te maken, zoals het actief scannen van beeldmateriaal op bekend en geregistreerd materiaal van seksueel misbruik, waaronder dat van minderjarigen. Ze stelt voor daartoe te verplichten in chatberichten van apps als WhatsApp en Signal. Tot op heden zijn berichten versleuteld, zodat behalve zender en ontvanger niemand op de hoogte is van de inhoud. Autoriteiten zien dit als een obstakel in de opsporing van beeldmateriaal van minderjarigen en willen *client-side device scanning* toepassen. Hiermee kan data van bekende beelden van misbruik volledig geautomatiseerd vergeleken worden met gedeelde beelden in (versleutelde) chatgesprekken. In Nederland is er kritiek uit de hoek van privacy-experts.[11] Op het moment van schrijven is nog niet duidelijk hoe Nederland hierover stemt, en hoe dit uitgewerkt en geïncorporeerd zal worden in nationale wetgeving.

Opsporing en detectie van beeldmateriaal

Opslagplaatsen van beeldmateriaal

Er zijn grofweg vier verschillende manieren waarop beeldmateriaal wordt opgeslagen dan wel gedeeld. Ten eerste wordt beeldmateriaal opgeslagen op de lokale schijf van een desktop en op draagbare gegevensdragers zoals USB-sticks, cd's, dvd's en externe harde schijven. Indien pedoseksuelen elkaar fysiek ontmoeten of een netwerk vormen om beeldmateriaal te delen, worden vaak draagbare gegevensdragers uitgewisseld. De overige manieren van het opslaan en delen van beeldmateriaal vinden online plaats (Lee *et al.*, 2020; Steel *et al.*, 2022) (TBKK, persoonlijke communicatie, 20 juni 2022). Daarbij kan onderscheid gemaakt worden tussen het plaatsen op het 'normale internet' (*Clearweb*, zie volgende alinea), op afgeschermde delen van het *Clearweb*, en op het *Darkweb*. Als beeldmateriaal op het *Clearweb* wordt geplaatst, dan wordt dit ofwel op een zelfgemaakte website gedaan, ofwel op de pagina's van dienstverleners (*electronic serviceproviders* (ESPs)) zoals Youtube (Google), Facebook (Meta), of file-hosting- en cloud-ervicebedrijven. Grote *Internet Service Providers* (ISPs) hebben medewerkers in dienst om geplaatst beeldmateriaal te beoordelen en ontwikkelen automatische detectiemechanismen om illegaal beeldmateriaal makkelijker

[11] Verhagen, L. (2022, 11 mei). Diensten als WhatsApp en Gmail moeten van de EU actief jagen op kinderporno, privacy-experts vrezen gevolgen. *De Volkskrant*.

op te sporen (Edwards *et al.*, 2021; Lee *et al.*, 2020). Ook beeldmateriaal op privéwebsites kan gedetecteerd worden met zogeheten *webcrawlers*[12] (Lee *et al.*, 2020). Bij plaatsing op het *Clearweb* wordt bovendien een digitaal spoor achtergelaten van IP-adressen en inloglocaties, waardoor opsporingsdiensten de plaatsers hiervan relatief makkelijk kunnen identificeren. Opsporing wordt moeilijker zodra het plaatsen van beeldmateriaal op afgesloten delen van het internet gebeurt. Hierbij gaat het veelal om het plaatsen van beeldmateriaal op cloudservices, waarop data vaak versleuteld (*encrypted*) is, en waarbij vanwege privacywetgeving ook de hostingbedrijven niet zomaar de inhoud van de privé-accounts van hun klanten mogen bekijken of scannen op illegaal materiaal (Teunissen & Napier, 2022). Cloudservices hebben een bijkomend voordeel dat data die daarop staat niet verzonden hoeft te worden (wat de kans op detectie vergroot), maar dat slechts een uniek webadres met eventuele inloggegevens tussen mensen gedeeld hoeft te worden. Naast cloudservices vallen ook berichtenservice-apps als WhatsApp en Telegram hieronder. Daarbij vindt veelal *end-to-end (E2E) encryption* plaats, waarbij de data die tussen verschillende gebruikers wordt gedeeld alleen door die gebruikers gezien kan worden, waardoor er dus geen beoordeling op illegaal beeldmateriaal gemaakt kan worden (Teunissen & Napier, 2022). Ook livestreamdiensten, waarbij misbruik van minderjarigen live wordt uitgezonden, vallen onder deze categorie. Tenslotte vindt een groot deel van het plaatsen en delen van beeldmateriaal op het *Darkweb* plaats. Dit wordt in de volgende paragraaf in meer detail besproken.

Surface Web en *Deep Web*

Het meeste bekende deel van het internet is wat ook wel het *Clearweb*, *Clearnet* of *Surface Web* genoemd wordt. Deze laatste term verwijst naar het deel van een ijsberg waarvan alleen de top aan de oppervlakte zichtbaar is. Bij gebruik van het *Surface Web* gaat het om het bezoeken van vrij toegankelijke, geïndexeerde websites die via zoekmachines vindbaar zijn. Naar schatting vindt slechts vijf tot tien procent van het internetgebruik op het *Surface Web* plaats. Het *Deep Web,* waarvan het *Darkweb* weer een onderdeel is, omvat ongeveer 90 tot 95 procent van het internetgebruik. Het *Deep Web* bestaat uit niet vrij toegankelijke websites, waar bijvoorbeeld een wachtwoord voor nodig is of die alleen gevonden kunnen worden met een specifieke URL[13] (Janssen, 2022; NPOKennis, n.d.; Zieniūtė, 2022).

[12] Een *webcrawler* is een algoritme of 'bot' dat ingezet wordt om aangewezen internetomgevingen te doorzoeken naar specifieke informatie (bijvoorbeeld beeldmateriaal) of dat de inhoud van een webomgeving analyseert en categoriseert.

[13] Daarbij gaat het bijvoorbeeld om e-mails, bankgegevens, privédata van personen, bedrijven en instanties, academische en medische gegevens, beveiligde databases etc.

Darkweb

Het *Darkweb* is een onderdeel van het *Deep Web*, waarbij privacy en anonimiteit centraal staan. Het *Darkweb* bestaat uit een gedecentraliseerd netwerk van computers, waarbij het versleutelde (*encrypted*) internetverkeer wordt geleid via talloze IP-adressen en hosts. Webadressen zijn niet zomaar te vinden op het *Darkweb*, maar bestaan vaak uit een reeks willekeurige cijfers en letters, eindigend op *.onion*. De webadressen van websites veranderen daarbij ook regelmatig. Voor het bezoeken van het *Darkweb* is een speciale browser nodig, wat meestal de *Tor*-browser (*The Onion Router*) is. Andere *Darkweb*-browsers zijn *I2P* of *Freenet*. Met deze browsers kan men overigens ook het *Surface Web* bezoeken (Janssen, 2022; NPOKennis, n.d.; Zieniūtė, 2022).

Hoewel het *Darkweb* veelal geassocieerd wordt met criminele activiteiten, is dit zeker niet altijd het geval. *The Onion Router* is oorspronkelijk ontwikkeld door de Amerikaanse overheid met als doel anonieme en beveiligde communicatie tussen veiligheidsdiensten mogelijk te maken. Het *Tor*-project is vervolgens *open source* gemaakt, onder andere omdat een groter aantal gebruikers en een groter volume aan internetverkeer op het *Tor*-netwerk het volgen van activiteiten op dit netwerk moeilijker maken en daarmee de anonimiteit vergroten. Tegenwoordig is het anoniem zoeken naar informatie de belangrijkste reden dat mensen het *Darkweb* gebruiken. Er zijn dan ook relatief veel gebruikers in landen met dictatoriale regimes, waar normale websites gecensureerd worden. Verscheidene nieuws- en technologiewebsites hebben dan ook een *Darkweb*-variant. *ProRepublica* is een bekend voorbeeld van een journalistenplatform op het *Darkweb*. Daarnaast is het *Darkweb* nuttig voor de bescherming van de anonimiteit van klokkenluiders, waarvan *WikiLeaks* of de *SecureDrop* van de *Freedom of the Press Foundation* voorbeelden zijn. Toch is het *Darkweb* vooral bekend, of berucht, vanwege de illegale activiteiten die zich erop afspelen. Marktplaatsen waarop zaken als wapens en drugs worden verhandeld, en websites met illegaal pornografisch materiaal, waaronder ook strafbaar materiaal van minderjarigen, zijn daarbij de meest bekende problemen. Door de verscheidene legitieme en nuttige toepassingen van het *Darkweb*, en door het gedecentraliseerde en uitgebreide karakter ervan, is een algehele sluiting van het *Darkweb* geen realistische en wenselijke oplossing om criminele activiteiten daarop tegen te gaan. Bestrijding en opsporing zal dan ook moeten plaatsvinden tegen individuele URL's en fora (Janssen, 2022; NPOKennis, n.d.; Zieniūtė, 2022).

Zoeken en vinden op het *Darkweb*

Omdat websites op het *Darkweb* niet geïndexeerd zijn, en omdat de URL's willekeurig zijn, is traditioneel doorzoeken zoals op het *Surface Web* niet mogelijk. Toch zijn er websites die als 'zoekmachines' fungeren, waarop een grote verzameling van populaire *dark websites* met bijbehorende links staat. Het bekendste voorbeeld hiervan is *The Hidden Wiki*. Dit maakt het

navigeren een stuk makkelijker. Daarnaast maakt de populaire internetbrowser *DuckDuckGo* gebruik van het *Darkweb* om anonieme navigatie van het *Surface Web* mogelijk te maken. Tenslotte worden op de vele discussiefora op zowel het *Clearweb* als het *Darkweb* weblinks uitgewisseld (Janssen, 2022; Leclerc *et al.*, 2021; van der Bruggen & Blokland, 2021a).

Kinderpornografisch materiaal op het *Surface Web* en het *Darkweb*

Verschillende (internationale) opsporingsinstanties alsmede de grote internetbedrijven zoals Microsoft, Google en Meta (Facebook) houden zich actief bezig met de detectie van kinderpornografisch beeldmateriaal en het verwijderen daarvan (Edwards *et al.*, 2021; Lee *et al.*, 2020; Teunissen & Napier, 2022). Als het om al bekend beeldmateriaal gaat, zijn hier tegenwoordig effectieve geautomatiseerde detectiemethoden voor (zie het deel over *PhotoDNA* hieronder). Bij origineel (nieuw) beeldmateriaal is de detectie echter een stuk moeilijker. Het traceren van plaatsers en kijkers van illegaal beeldmateriaal op het *Clearweb* is technisch mogelijk indien de URL's van de betreffende websites bekend zijn en de IP-adressen van bezoekers geregistreerd worden. Om deze reden speelt de uitwisseling van kinderpornografisch beeldmateriaal zich voor een groot deel op het *Darkweb* af.

Uitwisseling van kinderpornografisch beeldmateriaal vindt voornamelijk op fora op het *Darkweb* (Leclerc *et al.*, 2021; van der Bruggen & Blokland, 2021c, 2021a; TBKK, persoonlijke communicatie, 20 juni 2022). Deze fora worden opgezet door forummanagers die de technische kennis hebben een hostinglocatie te organiseren en een *Tor*-webadres te genereren. Individuele forumleden of -bezoekers moeten ook over basiskennis van het *Darkweb* beschikken en weten hoe zij bij de juiste URL van het forum terechtkomen. Dit laatste blijkt vooral via algemene *Tor*-pagina's te lopen, waarop meerdere *Darkweb*-fora gericht op seksueel kindermisbruik vermeld staan. Deze algemene *Tor*-pagina's worden op hun beurt vermeld op het *Clearweb* of gedeeld door mededaders. Op de fora zijn vaak verschillende subfora te vinden voor specifieke subcategorieën van beeldmateriaal, bijvoorbeeld misbruik van jongens en meisjes. Daarnaast hebben de leden uitgebreide gesprekken en discussies met elkaar en wordt er informatie uitgewisseld. Naast beeldmateriaal gaat dit om het bespreken van seksuele fantasieën, maar ook algemene zaken, alsmede hoe zo voorzichtig (anoniem) mogelijk te zijn en hoe opsporingsinstanties te ontlopen. Door de hoge mate van anonimiteit en ontraceerbaarheid van het *Darkweb* wanen forumleden zich ongrijpbaar en straffeloos en worden gevoelens, fantasieën en strafbare feiten openhartig besproken (Leclerc *et al.*, 2021; van der Bruggen & Blokland, 2021a).

Op veel fora zijn beeldmateriaal en discussies niet vrij toegankelijk, maar moeten leden zich eerst bewijzen en een hogere status verwerven door zelf materiaal te delen (Kloess & van der Bruggen, 2021). Daarmee wordt ook vertrouwen gewonnen en 'bewezen' dat een nieuw lid geen politiemedewerker of hacker is. Met een hogere status hebben leden vaak ook

toegang tot bijzonderder (vaak extremer) beeldmateriaal (van der Bruggen & Blokland, 2021b; TBKK, persoonlijke communicatie, 20 juni 2022).

Voor forummanagers is het van belang dat de privacy en anonimiteit beschermd wordt, en bovendien dat het forum zich ontwikkelt en er nieuwe leden en nieuw beeldmateriaal bij blijven komen. Fora werken hiervoor vaak samen en de sfeer tussen fora onderling is dan ook samenwerkend in plaats van concurrerend. Bij veel onderzochte fora is vrijwel geen sprake van een commercieel of geldelijk motief. Contact met eensgezinden en het verwerven van (sociale) status zijn daarentegen vaak de belangrijkste motieven (Kloess & van der Bruggen, 2021; Leclerc *et al.*, 2021; van der Bruggen & Blokland, 2021b, 2021c, 2021a).

Detectie van kinderpornografisch beeldmateriaal door middel van *hashing*

PhotoDNA is de meest gebruikte technologie om al bekend beeldmateriaal op het internet (*Clearweb* en *Darkweb*) te detecteren (Edwards *et al.*, 2021; Lee *et al.*, 2020; Microsoft, n.d.). Hierbij wordt beeldmateriaal omgezet tot zwart/wit beeld, geformatteerd en in kleine stukjes opgebroken, waarvan vervolgens de intensiteitsgradiënten worden bepaald. Dit vormt de basis van een unieke digitale handtekening van een foto, ook wel een *hash* genoemd. Voor videos gebeurt dit op een overeenkomstige manier, maar de software daarvoor heet *PhotoDNA for video*. De *hashes* van bekende beelden van kinderporno en van ander illegaal beeldmateriaal worden opgeslagen in het *Hash Value Sharing platform*[14], waarin verschillende internationale databases verenigd zijn. Beelden die op vele websites worden geplaatst, worden met deze databases vergeleken. *PhotoDNA* is ontwikkeld door Microsoft en wordt dan ook voor hun eigen diensten als Outlook, OneDrive en Bing gebruikt, maar wordt daarnaast door grote internetbedrijven als Google, Meta, Twitter en Reddit ingezet. Zodra op één van deze diensten een foto of video wordt geplaatst, wordt dit vergeleken met de beelden in de database, en bij een match wordt het beeldmateriaal verwijderd en worden de autoriteiten ingelicht. Er zijn echter verschillende limitaties aan het gebruik van *PhotoDNA* of soortgelijke technieken. Ten eerste kan het niet toegepast worden op materiaal waarvan de ESP geen toegang heeft tot de ruwe data, bijvoorbeeld omdat het *end-to-end* versleuteld is. Ook verandert de *hash* bij elke (kleine) aanpassing van het beeldmateriaal, zoals bijvoorbeeld het kleiner snijden van de frame van de foto of video, het toevoegen van een logo of het spiegelen van een beeld. Tenslotte werkt *PhotoDNA* alleen bij materiaal dat al bij de instanties bekend is en al in de hash- databases is opgenomen. Nieuw vervaardigd of nog niet bekend materiaal moet op andere manieren gedetecteerd worden.

[14] Thorn (2017, 15 november). *Industry Hash Sharing - Reporting Child Sexual Abuse Content.* Geraadpleegd op 19 september 2022, van https://www.thorn.org/reporting-child-sexual-abuse-content-shared-hash/

Databases van beeldmateriaal

Er zijn verscheidene nationale en internationale databases waarin beeldmateriaal en/of *hashes* van beeldmateriaal worden opgeslagen. De belangrijkste zijn de *International Child Sexual Exploitation*[15] (ICSE) database van Interpol, de database van het NCMEC[16] uit de VS en de ICCAM[17]-database van de *International Association of Internet Hotlines en van Internet Hotline Providers in Europe* (INHOPE), een samenwerkingsverband tussen verschillende internationale hotlines voor (online) kindermisbruik. Deze databases zijn verenigd in het *Hash Value Sharing platform THORN*.

Digitale opsporingstechnieken

Automatisering en artificiële Intelligentie

Door de sterke toename van de hoeveelheid online kinderpornografisch beeldmateriaal in de laatste jaren en een gebrek aan mankracht is het in toenemende mate onmogelijk voor zowel ISP's als zedenrechercheurs om al het beeldmateriaal te beoordelen op illegaliteit. Zeker als het gaat om materiaal dat nog niet in de internationale databases geregistreerd staat. Als oplossing hiervoor wordt vaak gewezen in de richting van automatisering en vormen van cognitieve programmering, waarvan artificiële intelligentie (AI) een voorbeeld is (zie kader).[18] Daarvoor is het van belang de mogelijkheden en limitaties daarvan te begrijpen.

Artificiële intelligentie

Een definitie van artificiële of kunstmatige intelligentie is de theorie en ontwikkeling van computersystemen die taken kunnen uitvoeren waarvoor normaal gesproken menselijke intelligentie vereist is. Daarbij zijn processen als visuele perceptie, spraakherkenning, vertalen, het nemen van beslissingen, redeneren en plannen betrokken. Strikt genomen gaat het bij AI om zowel analyse van vergaarde informatie als 'besluitvorming' over het uitvoeren van (een) specifieke ta(a)k(en). Vaak wordt de term AI echter ruimer gebruikt, bijvoorbeeld als een algoritme patronen in data kan herkennen zonder op basis daarvan een beslissing te nemen.

[15] https://www.interpol.int/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database
[16] https://www.missingkids.org/home
[17] https://www.inhope.org/EN
[18] Voor het maken van dit kader zijn de volgende bronnen geraadpleegd:
https://www.sas.com/en_us/insights/articles/big-data/artificial-intelligence-machine-learning-deep-learning-and-beyond.html
https://www.encora.com/insights/natural-language-processing-and-machine-learning
https://monkeylearn.com/blog/nlp-ai/

Machine learning

Machine learning (ML) is een vorm van cognitieve programmering waarbij een algoritme getraind wordt patronen in data te herkennen. Machine learning is een van de meest gebruikte vormen van automatisering. Voorbeelden zijn software in zelfrijdende auto's die verkeerslichten detecteren, of medische software waarin een algoritme naar afwijkingen in een weefselpreparaat speurt. Voor ML zijn meerdere *training datasets* nodig waarmee het algoritme leert de gewenste patronen te herkennen.

Natural language processing

Natural language processing (NLP) is een vorm van cognitieve programmering waarbij taal wordt verwerkt en geanalyseerd. Dit is van nut als een tekst bijvoorbeeld op bepaalde zoektermen wordt doorzocht of in het geval van vertalingen.

Gezichts- en leeftijdsherkenning

Bij de opsporing en analyse van beeldmateriaal worden automatisering en AI op verschillende vlakken ontwikkeld (Edwards *et al.*, 2021; Lee *et al.*, 2020; Negreiro, 2020). Een belangrijk onderzoeksveld is dat van gezichtsherkenning, wat zou kunnen helpen bij het identificeren van zowel slachtoffers als daders. Een bedrijf dat zich hier bijvoorbeeld mee bezighoudt is *Clearview AI*, dat gebruik maakt van een database van drie miljard foto's. Het bedrijf beweert daarmee de opsporingsinstanties geholpen te hebben bij het identificeren van slachtoffers en daders, maar tegelijkertijd is de werkwijze van het bedrijf controversieel omdat het naar alle waarschijnlijkheid niet aan de privacywetgeving van de EU voldoet (Negreiro, 2020). Binnen opsporingsinstanties wordt gezichtsherkenning alleen af en toe ingezet binnen een onderzoek, maar niet standaard uitgevoerd op gevonden beeldmateriaal. Dit is complex omdat vanwege privacyregelgeving niet zomaar databases van gezichten van slachtoffers of daders mogen worden bijgehouden of gebruikt. Daarnaast zijn er verschillen in internationale wetgeving over of beeldmateriaal, of *hashes* daarvan, door instanties opgeslagen mogen worden (TBKK, persoonlijke communicatie, 20 juni 2022). Vanuit slachtoffers wordt wel met enige regelmaat gevraagd naar zulke mogelijkheden omdat verdere verspreiding met beeldmateriaal van bepaalde personen op die manier beperkt zou kunnen worden. Meta (Facebook) werkt hier samen met het NCMEC bijvoorbeeld ook aan (EOKM, persoonlijke communicatie, 27 juli 2022).

Een ander aspect waarvoor automatisering wordt ingezet is het herkennen van leeftijd (Negreiro, 2020). Algoritmes kunnen getraind worden om in ieder geval een globale inschatting te maken van de leeftijd van personen die op beeldmateriaal te zien zijn. Dit kan het automatisch detecteren van seksueel beeldmateriaal met minderjarigen vereenvoudigen, zeker als het algoritme ook getraind is om naaktheid te herkennen. Voor

het uiteindelijke oordeel is natuurlijk nog wel een menselijk oordeel nodig. Daarnaast hebben verschillende ISP's interesse in leeftijdsherkennende algoritmes. Op die manier zou op een meer betrouwbare manier kunnen worden vastgesteld of een persoon oud genoeg is om aan de gebruikersvoorwaarden van bijvoorbeeld een socialmedia-app te voldoen. Daarmee zou dus kunnen worden voorkomen dat minderjarigen gebruik maken van een app die voor volwassenen bedoeld is. In Nederland voert het NFI (Nationaal Forensisch Instituut) momenteel een pilotstudie uit met leeftijdsherkenningssoftware, en internationaal zijn meerdere opsporingsinstanties hiermee bezig.

Tekstherkenning

Beeldmateriaal wordt veelal geplaatst met een titel en soms ook met een beschrijving. *Natural language processing*-algoritmes kunnen op internet zoeken naar trefwoorden en termen in deze teksten en zo beeldmateriaal van misbruik van minderjarigen detecteren. Deze techniek kan ook op de discussiefora op het *Darkweb* en *Clearweb* worden gebruikt om potentiele daders te vinden (Edwards *et al.*, 2021; Lee *et al.*, 2020). Voorbeelden van termen zijn *teenager* of *pre-teen*. Voor misbruik met sadistisch en ritueel satanische aspecten zouden ook een aantal voor de hand liggende zoektermen gebruikt kunnen worden, maar bij weten van de Commissie is dit tot op heden nooit uitgevoerd.

Automatische herkenning van andere aspecten

Theoretisch kan een machinelearningalgoritme getraind worden om van alles te herkennen. Voor kinderpornografisch beeldmateriaal zouden bijvoorbeeld aspecten als naaktheid, geslacht van de slachtoffers en daders, het aantal personen op beeld, etniciteit en de aard van het misbruik (bijvoorbeeld met of zonder penetratie) interessant zijn om betere inzichten te vergaren en om aanknopingspunten voor opsporing te vinden. In Nederland wordt vooralsnog alleen ingezet op leeftijds- en gezichtsherkenning (TBKK, persoonlijke communicatie, 20 juni 2022).

Met betrekking tot beeldmateriaal van sadistisch misbruik met rituele of satanische aspecten zou voor een automatische detectie een trainingsdataset benodigd zijn. Hoewel er geen beeldmateriaal van zulk misbruik zelf voorhanden is, kan een algoritme wel getraind worden om voorwerpen als kruizen, gewaden of kaarsen te herkennen. Zulk soort automatische opsporing zou daarmee nooit een alomvattend resultaat met al het geplaatste beeldmateriaal van ritueel satanisch misbruik opleveren, maar in het geval dat er iets aangetroffen zou worden, zou dit wel tot aanknopingspunten voor opsporingsonderzoek kunnen leiden. In Nederland is er ook een (anonieme) commerciële partij die zulk soort onderzoek technisch gezien zegt uit te kunnen voeren (anonieme communicatie).

Opsporingsinstanties en vindplaatsen van beeldmateriaal in Nederland

De Commissie heeft diverse gesprekken gevoerd met overheidsorganisaties en particuliere organisaties om na te gaan of zij in hun werk gevallen tegenkomen van georganiseerd seksueel misbruik van minderjarigen, en specifiek met rituele en/of satanische kenmerken. Ook is hen gevraagd naar beeldmateriaal van dit type misbruik.

Het Team Bestrijding Kinderporno en Kindersekstoerisme (TBKK) van de Landelijke Eenheid

Het TBKK is in Nederland een centraal punt waar opsporing naar beeldmateriaal wordt gedaan op het *Clearweb* en *Darkweb* en op in beslag genomen gegevensdragers. Het team houdt zich onder andere bezig met zicht houden op de verschillende fora en lijsten met weblinks op het *Darkweb* en is hier vaak undercover op aanwezig. Daarnaast werken zij met internationale opsporingsinstanties samen om informatie over nieuwe webpagina's, nieuw beeldmateriaal en *hashes* daarvan, informatie over daders en dergelijke uit te wisselen. Ook hebben zij verschillende activiteiten gericht op het *Clearweb*, met name file-hostingbedrijven en berichtendiensten. Als beeldmateriaal in een onderzoek aangetroffen wordt, worden *hashes* hiervan in de internationale databases gedeeld. De collectie beeldmateriaal van het onderzoek wordt gecategoriseerd, maar niet elk individueel beeld wordt beschreven. Er bestaat dus ook geen database waarin gezocht kan worden naar beschrijvingen van al het bekende beeldmateriaal. Op die manier zou dus ook niet naar eventueel beeldmateriaal met ritueel satanische aspecten gezocht kunnen worden. Bij navraag geeft het team aan een klein percentage beeldmateriaal van ernstig sadistisch misbruik en georganiseerd misbruik tegen te komen (*hurtcore*), maar niet van misbruik met satanische en/of rituele aspecten (TBKK, persoonlijke communicatie, 20 juni 2022).

Als motief lijkt er geen sprake van winstbejag, maar meer van onderlinge ruil van materiaal van minderjarigen (B. van Mierlo, coördinator TBKK, persoonlijke communicatie, 23 september 2021; medewerkers OM, persoonlijke communicatie, 17 mei 2022; dataspecialisten TBKK, persoonlijke communicatie, 20 juni 2022). *"Met extremer beeldmateriaal krijgt men als maker/verspreider een hogere status in een netwerk en daarmee weer toegang tot ander extremer materiaal"*, aldus de coördinator. Georganiseerd misbruik waarvan ook beeldmateriaal is geeft in principe veel aanknopingspunten voor politieonderzoek, wat de kans op een succesvolle opsporing vergroot, aldus de coördinator van het TBKK. Afbeeldingen van georganiseerd ritueel satanisch misbruik bieden nog meer aanknopingspunten voor verder onderzoek (vanwege specifieke rituele objecten, omgevingskenmerken en meerdere daders) en zijn dus relatief makkelijker dan 'gewoon' beeldmateriaal van individuele daders te onderzoeken. Zijns inziens is het feit dat de

(internationale) politie dan ook niet of nauwelijks stuit op kinderpornografisch beeldmateriaal met rituele en/of satanische kenmerken een aanwijzing voor het ontbreken van beeldmateriaal hiervan.

De Nationaal Rapporteur Mensenhandel en Seksueel Geweld tegen Kinderen

De Nationaal Rapporteur Mensenhandel en Seksueel Geweld tegen Kinderen heeft de wettelijke taak om over de aard en omvang van mensenhandel en seksueel geweld tegen kinderen in Nederland te rapporteren aan de overheid. Met (voormalige) medewerkers zoals onderzoekers of leidinggevenden is gesproken over onderwerpen rondom seksueel misbruik van minderjarigen. Zij geven aan dat ze geen gevallen van ritueel satanisch misbruik tegengekomen te zijn in de casuïstiek die zij onder ogen krijgen. Ook zien zij geen (digitaal) beeldmateriaal van dit type misbruik. Het bestaan van georganiseerd misbruik van minderjarigen, onder andere met vermiste migrantenkinderen, wordt wel bevestigd (Nationaal Rapporteur Mensenhandel en Seksueel Geweld tegen Kinderen, persoonlijke communicatie, 27 januari 2022). Ook is er beeldmateriaal waarop kinderen gedood (lijken te) worden (M. van der Bruggen, persoonlijke communicatie, 9 december 2021).

Het Openbaar Ministerie (OM)

Vertegenwoordigers van het OM geven aan dat ze geen beeldmateriaal van ritueel (satanisch) misbruik van minderjarigen zijn tegengekomen in de zaken over kinderpornografie of kindersekstoerisme waarin zij een beslissing tot al dan niet vervolgen hebben genomen. Beeldmateriaal van seksueel misbruik van minderjarigen van sadistische aard komt wél voor (vertegenwoordigers OM, persoonlijke communicatie, 3 juni 2022).

Het Expertisebureau Online Kindermisbruik (EOKM)

Het EOKM is een organisatie die zich inzet voor het voorkomen en bestrijden van online kindermisbruik. Het is in 1995 voortgekomen uit het Meldpunt Kinderporno op Internet. Dit Meldpunt, tegenwoordig onderdeel van het EOKM, bestaat sinds 1985 en heeft als doel het voorkomen en bestrijden van online seksueel kindermisbruik en seksuele uitbuiting van kinderen. Via de website van het Meldpunt Kinderporno kunnen beelden op internet van seksueel misbruik van minderjarigen (anoniem) worden gemeld. Daarnaast kunnen meldingen van doorgestuurd beeldmateriaal van seksueel misbruik van minderjarigen via chatapplicaties zoals WhatsApp, Telegram, Signal, Viber of Facebook Messenger worden gemeld bij het Meldpunt Kinderporno via de betreffende chatgroepen. Het Meldpunt Kinderporno is onderdeel van INHOPE, het internationale netwerk van meldpunten.

Het EOKM doet zelf niet aan actieve opsporing van beeldmateriaal van seksueel misbruik van minderjarigen en is hier ook niet toe bevoegd volgens de juridische afspraken met het OM (A. Gerkens, persoonlijke communicatie, 27 juli 2022). Het EOKM krijgt vooral foto's binnen en minder video's, omdat deze vaker op file hosting- of cloudservices staan, waar het EOKM op juridische gronden geen toegang tot heeft. Het EOKM werkt nauw samen met het TBKK en vervult een complementaire functie omdat beeldmateriaal bij hen actief gemeld wordt, terwijl een soortgelijk meldpunt van de politie geen succes bleek te zijn. Dit laatste kan komen doordat het EOKM de anonimiteit van melders waarborgt en als doelstelling heeft om beeldmateriaal te laten verwijderen en niet om eventuele strafbare feiten van melders te onderzoeken. Ook het EOKM geeft aan wel af en toe sadistisch beeldmateriaal tegen te komen, waarvan de mate van organisatie van de daders niet te achterhalen valt omdat alleen het slachtoffer te zien is. Materiaal met ritueel satanische aspecten heeft men nooit gezien (EOKM, persoonlijke communicatie, 27 juli 2022).

Het *Child Protection Research Centre* (CPRC)

Het CPRC is een in 2020 opgerichte Nederlandse stichting die zich op het voorkomen van seksuele uitbuiting van minderjarigen richt.[19] De belangrijkste werkzaamheden van het CPRC zijn het reageren op meldingen van casussen en het doorverwijzen naar de juiste instanties op internationaal niveau. Momenteel houdt de particuliere stichting zich, net als de professionals met wie er een samenwerking is, bezig met meldingen van (seksuele) uitbuiting. Aanvullend voeren zij OSINT-onderzoek[20] uit. Door praktische omstandigheden is het niet mogelijk geweest om ook hun ambities ten aanzien van het pro-actief naar beeldmateriaal zoeken op het *Darkweb* te realiseren. In alle jaren dat de oprichter van het CPRC bij *Terre de Hommes/Watch!* en bij het CPRC heeft gewerkt, is hij geen ritueel satanische kenmerken tegengekomen in casussen of in beeldmateriaal van minderjarigen. Wel geeft ook hij aan dat er materiaal van ernstig sadistische *hurtcore* voorkomt (G. van Aartsen, persoonlijke communicatie, 15 juni 2022). Behalve praktische obstakels is oprichter Van Aartsen van mening dat het bekijken van beeldmateriaal op het *Darkweb* voorbehouden zou moeten zijn aan justitiële organisaties en politie. Zijn stichting zou strafbaar kunnen worden gesteld voor het bekijken van kinderpornografische afbeeldingen (G. van Aartsen, persoonlijke communicatie, 15 juni 2022). Het CPRC ziet haar werkzaamheden als onafhankelijke organisatie als aanvullend op wat er al door justitie gedaan wordt.

[19] In 2015 zette Van Aartsen voor *Terre des Hommes* (met Fier/CKM en ECPAT/*Defence for Children*) WATCH Nederland op, gericht op de aanpak van 'loverboys' (tegenwoordig genoemd: binnenlandse mensenhandel).
[20] OSINT staat voor *Open Source Intelligence*, en betreft het legaal verzamelen van data en informatie uit open en publiek beschikbare bronnen zoals open databases, overheidsrapporten, kranten- en tijdschriftartikelen, socialemediawebsites, afbeeldingen en video's of het *Darkweb*.

Slachtoffers en overige professionals die te maken hebben met beeldmateriaal

De commissie heeft in de gesprekken die zijn gevoerd met slachtoffers, therapeuten en belangenorganisaties voor slachtoffers van georganiseerd sadistisch misbruik gevraagd of er volgens hen foto's of video's gemaakt zijn van het misbruik en van de aanwezigen bij het misbruik.

Meerdere slachtoffers geven in de persoonlijke interviews aan dat er beeldmateriaal gemaakt zou zijn. Ze hebben dit meestal niet zelf onder ogen gehad. Wel vertellen ze het beeldmateriaal van misbruik van andere kinderen gezien te hebben. Onduidelijk is of zij zelf in bezit zijn van dit materiaal of weten wie het in bezit heeft. Onbekend is of het op gegevensdragers zou staan of dat het materiaal online is gezet op het *Clearweb* of het *Darkweb*. Redenen die ze noemen dat ze eventueel aanwezig beeldmateriaal niet kunnen geven is omdat het netwerk hen straft als zij dit doen. Ook geven slachtoffers aan ze door het netwerk bedreigd of gechanteerd worden met het feit dat er beeldmateriaal is van henzelf terwijl ze andere kinderen of dieren pijn (moesten) doen. De gehouden interviews betreffen volwassenen die aangeven als kind misbruikt te zijn. Het beeldmateriaal van hen is naar hun eigen zeggen oud materiaal en om die reden niet meer te vinden, als het al op internet gezet zou zijn. Therapeuten die de Commissie gesproken heeft die één of meerdere slachtoffers in behandeling hebben gehad, geven aan dat slachtoffers soms rapporteren dat er beeldmateriaal is (geweest). In één geval zegt een therapeut zelf ook beeldmateriaal gezien te hebben van het misbruik, of dat er een foto als chantage aan het slachtoffer is gestuurd.[21] In zulk soort gevallen is het overigens strafbaar om het beeldmateriaal in bezit te hebben, en het is volgens de professionele richtlijnen van therapeuten toegestaan melding van het beeldmateriaal te maken bij de politie (vertegenwoordigers OM, persoonlijke communicatie, 3 juni 2022). Het Kenniscentrum Transgenerationeel Geweld (KTGG) is een stichting die zich inzet voor slachtoffers van satanisch ritueel misbruik. Zij geven aan geen beeldmateriaal waarover de slachtoffers rapporteren te hebben gezien (KTGG, persoonlijke communicatie, 16 maart 2022).

Een beroepsgroep die direct of indirect te maken kan krijgen met gevallen van seksueel misbruik zijn juristen. Er is navraag gedaan naar beeldmateriaal van seksueel misbruik met riuele en/of satanische kenmerken bij minderjarigen. Via een nieuwsbrief aan gewelds- en zedenadvocaten aangesloten bij Stichting LANGZS[22] is – ook na een herhaalverzoek – geen respons teruggekomen van de ongeveer 150 aangesloten advocaten. De Commissie heeft ook via andere kanalen geen juristen gesproken die bekend zijn met georganiseerd sadistisch seksueel misbruik met rituele en/of satanische aspecten.

[21] Leidsch Dagblad (27 maart 2021). *'Cult' beheerst lijf en geest van Esther*. Haar therapeut deelt haar ervaringen.

[22] Stichting LANGZS is de afkorting voor Stichting Landelijk Advocaten Netwerk Gewelds- en Zedenslachtoffers.

Ook een aantal journalisten in Nederland heeft onderzoek gedaan naar het voorkomen van beeldmateriaal van seksuele handelingen met minderjarigen. In de meeste gevallen ging het het om relatief milde vormen van seksuele handelingen bij minderjarigen. RTL Nieuws heeft in 2019 enkele maanden undercoveronderzoek[23] gedaan op het *Darkweb*. Binnen deze online kinderpornonetwerken is een grote groep Nederlandse leden specifiek op zoek naar Nederlands beeldmateriaal van minderjarigen. RTL Nieuws heeft veertien online netwerken onderzocht. Elk van de veertien onderzochte netwerken heeft de beelden onderverdeeld in verschillende leeftijdscategorieën en er zijn categorieën voor allerlei fetisjen. Er werd daarbij niets gerapporteerd over sadistisch misbruik of misbruik met rituele of satanische aspecten.

Journalisten van Pointer, het platform voor onderzoeksjournalistiek van KRO-NCRV op tv, radio en online, deden in 2021 onderzoek naar *online shaming*[24] op Telegram in zogeheten exposegroepen, groepen waarin ongevraagd naaktbeelden getoond en verspreid worden. Desgevraagd geven ze via mailcontact aan dat ze geen enkele aanwijzing hebben gevonden voor (sadistisch) kindermisbruik omdat het gaat om een geheel ander soort misbruik (geen lichamelijk letsel bijvoorbeeld) in dit soort groepen en dat het niet waarschijnlijk is hiertussen beeldmateriaal van sadistisch kindermisbruik te vinden.

Bellingcat is een burger-onderzoeksjournalistiek netwerk. Het is gespecialiseerd in onder meer het uitvoeren van OSINT en maakt daarbij onder andere gebruik van online bronnen, zoals sociale media en open data. Relevant voor dit deelrapport is werk dat zij doen naar aanleiding van foto's die Europol deelt op internet van mogelijke locaties waar misbruik met minderjarigen plaatsvindt in het kader van hun *Stop Child Abuse*-campagne. Journalisten van Bellingcat werken mee aan het vinden van de geo-locaties van die foto's om zo bij te dragen aan de opsporing van personen die het materiaal uploadden.[25] Desgevraagd geven ze via mailcontact aan dat zij alleen werken met beelden (foto's veelal) die aangeleverd zijn door justitiële instanties. Het bezit en verspreiding van dit materiaal is immers strafbaar. Zij komen beeldmateriaal van georganiseerd sadistisch seksueel misbruik van minderjarigen niet tegen.

Overige informatiebronnen over beeldmateriaal

Op alternatieve mediawebsites wordt ook informatie gedeeld over beeldmateriaal van ritueel satanisch misbruik. Het materiaal wordt niet getoond, maar er wordt geschreven dat

[23] Daniël Verlaan beschrijft de werkwijze die hij als uitvoerend onderzoeksjournalist bij RTL nieuws hanteerde: https://www.rtlnieuws.nl/nieuws/nederland/artikel/4702991/rtl-nieuws-undercover-kinderporno-netwerken

[24] Pointer. Geraadpleegd op 31 mei 2022, van https://pointer.kro-ncrv.nl/naaktbeelden-honderden-slachtoffers-telegram-groepen-gedeeld

[25] Romein, D. (2019, 6 december). *More Europol's "Stop Child Abuse" Photographs Geolocated.* Bellingcat. Geraadpleegd op 12 mei 2022, van https://www.bellingcat.com/news/uk-and-europe/2019/07/02/more-europols-stop-child-abuse-photographs-geolocated/

het bestaat. Dit kan bijvoorbeeld een bijdrage zijn van iemand die ritueel (satanisch) misbruik en beeldmateriaal onder de aandacht wil brengen, en andere keren betreft het volwassenen die als kind op deze wijze misbruikt zouden zijn geweest.[26] Tot slot wordt vaak aangegeven dat er beeldmateriaal is, maar onduidelijk blijft waarvan dan en waar het te vinden zou zijn. Burgers die niet op professionele manier bezig zijn met de opsporing van beeldmateriaal op bijvoorbeeld het *Darkweb*, en hier ook geen expliciete vergunning hebben, kunnen voor het bezitten of bekijken van beelden met seksuele handelingen van minderjarigen strafbaar worden gesteld.[27]

Conclusie

Dit deelonderzoek beschrijft de toename van online beeldmateriaal sinds de eeuwwisseling. Ook de aard van seksueel misbruik van minderjarigen is over de jaren heen veranderd. De opsporing van dit beeldmateriaal is geïntensiveerd en de technische opsporingsmogelijkheiden zijn verder ontwikkeld. Ook is er in de politiek steeds meer aandacht voor het bestrijden van beeldmateriaal van minderjarigen.

De Commissie heeft met relevante instanties in Nederland gesproken en gevraagd of zij beeldmateriaal van georganiseerd sadistisch seksueel misbruik, al dan niet met rituele of satanische aspecten, zijn tegengekomen. De officiële instanties, ofwel de politie (het TBKK), het OM en de Nationaal Rapporteur Mensenhandel en Seksueel Geweld tegen Kinderen geven aan weliswaar beeldmateriaal van sadistisch misbruik van minderjarigen te zien, maar geen misbruik met rituele of satanische aspecten. Ook private instanties en individuen zoals het EOKM, het CPRC en journalisten van RTL Nieuws, Pointer en Bellingcat geven aan geen beeldmateriaal van deze vorm van misbruik gezien te hebben, maar wel van sadistisch misbruik bij minderjarigen. Alleen slachtoffers zelf, een enkele therapeut en verschillende alternatieve mediabronnen zeggen beeldmateriaal van ritueel (satanisch) ritueel misbruik gezien te hebben of geven aan dat dit bestaat. Van het beeldmateriaal van sadistisch misbruik van minderjarigen zeggen de ondervraagden dat de mate van organisatie van de daders moeilijk te achterhalen is, omdat vaak alleen het slachtoffer in beeld is.

Op basis van dit deelonderzoek is niet eenduidig te zeggen of beeldmateriaal van georganiseerd sadistisch misbruik van minderjarigen met satanische of rituele aspecten bestaat. Slachtoffers geven dit wel aan, maar het beeldmateriaal is niet aan de politie

[26] Argos schonk hier in 2019 aandacht aan en ging met slachtoffers op zoek naar 'hun materiaal'. Geraadpleegd op 24 juni 2022, van https://www.vpro.nl/argos/media/afleveringen/2019/waarom-stefanie-en-beatrix-hun-eigen-kinderporno-willen-vinden.html

[27] Een voorbeeld is een zaak uit 2017 waarin anderhalf jaar gevangenisstraf wordt geëist tegen een promovendus die in het bezit is van pornografische afbeeldingen van porno en dieren, naar eigen zeggen omdat hij die nodig had voor zijn wetenschappelijke onderzoek (De Stentor, 30-08-2017).

overhandigd en alle gesproken experts hebben dit nooit aangetroffen. Een beperking van de gebruikte methodiek is dat bestaande experts bevraagd zijn, en dat andere of voormalige experts (ook in het buitenland) dit type beeldmateriaal wél gezien zouden kunnen hebben. Er wordt noch in Nederland noch op internationaal niveau een database onderhouden met beschrijvingen van het beeldmateriaal, dus hierin kan ook niet gezocht worden. Anderzijds is het zo dat als zulk type beeldmateriaal gezien zou zijn, dit door de aard ervan zoveel aanknopingspunten voor onderzoek zou geven, dat er ongetwijfeld een politieonderzoek ingezet zou zijn (aldus de coördinator van het TBKK). Met de hoge mate van internationale samenwerking tussen opsporingsdiensten op het gebied van online kindermisbruik zou het daarom onwaarschijnlijk zijn dat geen van de ondervraagde personen van zulk onderzoek gehoord zou hebben. In de toekomst zouden eventueel automatische opsporingsmethoden ingezet kunnen worden, waarbij een algoritme actief zoekt naar rituele en satanische aspecten in beeldmateriaal of titels en beschrijvingen daarvan.

Tenslotte moet ook de motivatie van daders in acht genomen worden. In het geval van bekend beeldmateriaal van seksueel misbruik van minderjarigen wordt dit door daders veelal gedeeld via discussiefora op het *Darkweb*. Daarbij bespreken forumleden vaak eerst zaken van allerlei aard, waarna na een opbouw van vertrouwen beeldmateriaal gedeeld wordt. Beeldmateriaal van meer extreme vormen van misbruik vereist vaak ook een langere opbouw van vertrouwen. De functie van deze fora is echter veelal het vinden van gelijkgestemden en de motivatie is vaak om status te verwerven. Bij beeldmateriaal dat binnen een (satanische) groepering vervaardigd wordt, werkt dit naar alle waarschijnlijkheid anders. De sociale status zal afhankelijk zijn van andere aspecten. Beeldmateriaal zal binnen een misbruiknetwerk wellicht gebruikt worden, bijvoorbeeld voor dreiging tot afpersing voor het geval dat iemand het netwerk wil verlaten. Het delen van beeldmateriaal met vreemden van buiten het netwerk, of op internet in het algemeen, zou echter de kans op opsporing vergroten. Dit is een mogelijke verklaring voor waarom beeldmateriaal van ritueel (satanisch) misbruik niet door opsporings- of andere instanties gezien wordt.

Literatuurlijst

Edwards, G., Christensen, L. S., Rayment-McHugh, S., & Jones, C. (2021). *Trends & issues in crime and criminal justice Cyber strategies used to combat child sexual abuse material*.

European Commission. (2020). *EU strategy for a more effective fight against child sexual abuse*.

Europol. (2020). *Internet organised crime threat assessment*.

Janssen, D. (2022, 5 augustus). *Wat is het Darkweb?* Https://Www.Vpngids.Nl/Privacy/Anoniem-Browsen/Wat-Is-Het-Dark-Web/.

Kloess, J. A., & van der Bruggen, M. (2021). Trust and Relationship Development Among Users in Dark Web Child Sexual Exploitation and Abuse Networks: A Literature Review From a Psychological and Criminological Perspective. In *Trauma, Violence, and Abuse*. SAGE Publications Ltd. https://doi.org/10.1177/15248380211057274

Leclerc, B., Drew, J., Holt, T. J., Cale, J., & Singh, S. (2021). *Trends & issues in crime and criminal justice Child sexual abuse material on the darknet: A script analysis of how offenders operate*.

Lee, H. E., Ermakova, T., Ververis, V., & Fabian, B. (2020). Detecting child sexual abuse material: A comprehensive survey. *Forensic Science International: Digital Investigation*, *34*. https://doi.org/10.1016/j.fsidi.2020.301022

Lone, Q., Gañán, C. H., & van Eeten, M. (2020). *CSAM Hosting Monitor Rapport september 2020*.

Lone, Q., Gañán, C. H., & van Eeten, M. (2022). *CSAM Hosting Monitor*.

Microsoft. (n.d.). *Photo DNA*. Https://Www.Microsoft.Com/En-Us/Photodna.

Negreiro, M. (2020). *Curbing the surge in online child abuse. The dual role of digital technology in fighting and facilitating its proliferation*.

NPOKennis. (n.d.). *Wat is het Darkweb?* Https://Npokennis.Nl/Longread/7642/Wat-Is-Het-Dark-Web.

Steel, C., Newman, E., O'Rourke, S., & Quayle, E. (2022). Technical behaviours of child sexual exploitation material offenders. *Journal of Digital Forensics, Security and Law*. https://doi.org/10.15394/jdfsl.2022.1794

Teunissen, C., & Napier, S. (2022). *Child sexual abuse material and end-to-end encryption on social media platforms: An overview*.

Van der Bruggen, M., & Blokland, A. (2021a). *Child Sexual Exploitation Communities on the Darkweb: How Organized Are They?* (pp. 259–280). https://doi.org/10.1007/978-3-030-60527-8_15

Van der Bruggen, M., & Blokland, A. (2021b). *Netwerken van Seksueel Kindermisbruik op het Darkweb*.

Van der Bruggen, M., & Blokland, A. (2021c). Profiling Darkweb Child Sexual Exploitation Material Forum Members Using Longitudinal Posting History Data. *Social Science Computer Review*. https://doi.org/10.1177/0894439321994894

Zieniūtė, U. (2022, June 22). *Wat is het dark web en hoe kom je er veilig op?* Https://Nordvpn.Com/Nl/Blog/Hoe-Kom-Ik-Op-Dark-Web/.