De preventie en bestrijding van seksueel misbruik van kinderen in de online omgeving

de Hingh, Anne

published in
Tijdschrift voor Internetrecht
2023

document version
Publisher's PDF, also known as Version of record

citation for published version (APA)
de Hingh, A. (2023). De preventie en bestrijding van seksueel misbruik van kinderen in de online omgeving: een controversieel Europees voorstel. *Tijdschrift voor Internetrecht*, *2023* (2), 53-65. https://denhollander.info/artikel/17703

De preventie en bestrijding van seksueel misbruik van kinderen in de online omgeving: een controversieel Europees voorstel

dr. mr. A.E. de Hingh[1]

Op 11 mei 2022 publiceerde de Europese Commissie het Voorstel voor een Verordening van het Europees Parlement en de Raad tot vaststelling van regels ter voorkoming en bestrijding van seksueel misbruik van kinderen.[2] **Het doel van deze Verordening, namelijk het beschermen van kinderen tegen verschillende vormen van (online) seksueel misbruik, staat niet ter discussie. Maar de manier waarop de Europese Commissie dat doel wil bereiken, mag gerust controversieel genoemd worden. Met name het gebruik van technologieën door internetbedrijven bij het online opsporen van materiaal van seksueel kindermisbruik en het bestrijden van online grooming zal leiden tot significante risico's ten aanzien van de privacy van álle EU-burgers.**

De voorgestelde Verordening ter voorkoming en bestrijding van seksueel misbruik van kinderen vloeit voort uit diverse kinderrechtenstrategieën van de EU die zich richten op de rechten van kinderen in de digitale omgeving enerzijds en de bestrijding van geweld tegen kinderen, met inbegrip van online seksueel misbruik, anderzijds. Dat laatste vormt, volgens de Europese Commissie, een reëel en alsmaar groeiend gevaar. De toenemende digitalisering en het groeiende gebruik van internet en sociale media hebben er immers voor gezorgd dat seksueel misbruik van kinderen voor een groot deel is verplaatst naar de online omgeving.

Met het voorstel worden twee specifieke vormen van online seksueel kindermisbruik aangepakt: het online verspreiden van kinderpornografisch materiaal (dat men tegenwoordig liever aanduidt als 'afbeeldingen van seksueel kindermisbruik' of, met de Engelse afkorting, CSAM)[3] en het online benaderen van kinderen (oftewel online grooming). De aanbieders van diensten van de informatiemaatschappij spelen een centrale rol bij het voorkomen en bestrijden van online seksueel kindermisbruik aangezien de verspreiding van dat (kinderpornografische) materiaal en ook (strafbare) communicatie met kinderen grotendeels via hun diensten verlopen.[4]

Sommige aanbieders maken al vrijwillig gebruik van technologieën om online misbruik van kinderen op hun diensten op te sporen en te melden. Maar een groot aantal aanbieders onderneemt momenteel niet of nauwelijks actie. Om die reden wil de Commissie met de voorgestelde Verordening nieuwe verplichtingen in het leven roepen voor de aanbieders van hostingdiensten en aanbieders van diensten voor interpersoonlijke communicatie die kunnen worden gebruikt voor online seksueel misbruik van kinderen.

In deze bijdrage wordt een overzicht gegeven van de meest opvallende onderdelen van de voorgestelde Verordening. Na een bespreking van enkele algemene aspecten en de achtergrond van het voorstel (paragraaf 2) komen de verplichtingen voor de aanbieders van hostingdiensten en interpersoonlijke communicatiediensten aan de orde (paragraaf 3). Paragraaf 4 gaat in op de daarbij te gebruiken technologieën, onder meer om toegang te verkrijgen tot versleutelde communicatie. De bijdrage wordt afgesloten met enkele punten van kritiek en discussie (paragraaf 5). Gelet op de politieke en maatschappelijke commotie die het voorstel heeft teweeggebracht, sta ik eerst kort stil bij de kern van die controverse (paragraaf 1).

1. Anne de Hingh is universitair docent Internetrecht aan de VU Amsterdam.
2. Voorstel van het Europees Parlement en de Raad tot vaststelling van regels ter voorkoming en bestrijding van seksueel misbruik van kinderen, COM(2022)209, 11 mei 2022.
3. In de wandelgangen wordt het voorstel ook wel aangeduid als de CSAM-verordening, waarbij de afkorting CSAM staat voor *child sexual abuse material.*
4. Toelichting Voorstel, p. 2.

1. Controverse en de CSAM-cijfers

De voorgestelde Verordening houdt de gemoederen al geruime tijd bezig. Een groot aantal Europese en internationale organisaties die zich inzetten voor de rechten en de (online) bescherming van kinderen (zoals Missing Children Europe, Eurochild, het Duitse kinderfonds, ECPAT International, en het Amerikaanse Thorn) ondersteunen het voorstel van ganser harte. Zo ondertekenden inmiddels meer dan 90 organisaties een open brief waarin zij het voorstel 'tijdig en historisch' noemen, en een 'critical step toward better protection of children's rights' voor Europa en de hele wereld.[5]

Anderen zijn kritischer. Voor hen vormen de technologische maatregelen die aanbieders verplicht worden te nemen bij het opsporen en bestrijden van CSAM en online grooming, en het daarbij zo nodig doorbreken van (alle) vertrouwelijke, versleutelde communicatie, juist een schrikbeeld.[6] Al ruim 120 NGO's ondertekenden een petitie om Europarlementariërs ervan te overtuigen dat met dit voorstel de online privacy en security, de vertrouwelijkheid van communicatie en de uitingsvrijheid van alle burgers gevaar zouden lopen, ook van kinderen die het voorstel juist beoogt te beschermen.[7] De termen 'chatcontrole' en 'massasurveillance' werden in verband gebracht met de voorgestelde Verordening.[8] En de Europese privacywaakhonden EDPS en EDPB, die overeenkomstig artikel 42, tweede lid van de AVG werden geraadpleegd over het voorstel, brachten in juli 2022 middels een gezamenlijke opinie een negatief advies uit.[9]

1.1. Cijfers

Ter onderbouwing van het voorstel speelt cijfermateriaal een cruciale rol. Zo begint de toelichting bij het voorstel met een indrukwekkende opsomming van bronnen die zouden aantonen dat het online seksueel misbruik van kinderen in de laatste jaren explosief is toegenomen.[10] En Eurocommissaris Johansson hield niet op in al haar media-uitingen de boodschap te verkondigen dat met de ontwikkeling van de digitale wereld fenomenen als CSAM en online grooming dramatisch zijn gegroeid.[11] Zij baseerde zich daarbij onder meer op de cijfers van het Amerikaanse National Centre for Missing and Exploited Children (NCMEC), waaraan aanbieders in de VS seksueel misbruik via hun diensten moeten melden. NCMEC ontving in 2020 meer dan 21 miljoen meldingen van CSAM, waarvan ruim een 1 miljoen betrekking had op EU-lidstaten.[12] En tussen 2010 en 2020 zouden die EU-gerelateerde meldingen zijn toegenomen met een indrukwekkende 6000%.[13]

Zonder daarmee ook maar iets aan de ernst van het CSAM-probleem te willen afdoen, hebben verschillende organisaties hun kanttekeningen geplaatst bij de betrouwbaarheid van deze cijfers. Er is, bij een nadere beschouwing, wel wat af te dingen op de interpretatie van de statistieken die in wezen de onderbouwing van de noodzaak voor het voorstel vormen. Zo benadrukte het Nederlandse Expertisecentrum Online Kindermisbruik (EOKM) in zijn reactie op het voorstel dat een toename van het aantal meldingen niet (per se) een groei van het volume aan CSAM-materiaal impliceert en ook niet meteen iets zegt over de omvang van het daadwerkelijke misbruik.[14] De stijging van het aantal meldingen kan

5. "Open Letter: Thorn and 90+ Organizations Welcome the EU's Proposal to Prevent and Combat Child Sexual Abuse"21 mei 2022 op www.thorn.org/blog/open-letter-thorn-and-50-organizations-welcome-the-eus-proposal-to-prevent-and-combat-child-sexual-abuse/.
6. Zie bijvoorbeeld https://www.bitsoffreedom.nl/2022/05/09/jouw-berichtjes-zijn-alleen-voor-jou-en-je-gesprekspartner-en-niemand-anders/. Zie ook een gezamenlijke opinie van BoF en EOKM: https://www.trouw.nl/opinie/vader-post-foto-van-badderend-kind-is-dat-straks-verdacht~baadb567/.
7. https://edri.org/our-work/children-deserve-a-secure-and-safe-internet/.
8. Zie bijvoorbeeld https://www.patrick-breyer.de/en/posts/chat-control/. Zie voor een uitgebreid overzicht ook https://tweakers.net/reviews/10144/online-priveberichten-scannen-antikindermisbruikwet-zet-privacy-onderdruk.html. En zie bijvoorbeeld het draadje https://twitter.com/matthew_d_green/status/1634252397919739921 van Matthew Green, Amerikaanse cryptograaf en beveiligingstechnoloog werkzaam als computerwetenschapper aan het Johns Hopkins Information Security Institute: "It is essentially a design for the most powerful text and image-based mass surveillance system the free world has ever seen".
9. EDPB-EDPS Joint Opinion 04/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, 28 juli 2022. Zie ook overweging 84 considerans.
10. Toelichting Voorstel, p. 1. Bij nadere beschouwing blijken die bronnen niet allemaal even relevant te zijn voor het onderhavige Voorstel omdat ze bijvoorbeeld zien op het gebruik van fysiek geweld tegen kinderen, of de verwaarlozing van gehandicapte kinderen en ook op offline seksueel geweld tegen kinderen. Zie met name de bronnen genoemd in de voetnoten 3-5 op pagina 1 van de Toelichting bij het Voorstel.
11. Zie bijvoorbeeld https://www.trouw.nl/nieuws/pakt-nieuwe-eu-wet-kindermisbruik-aan-of-zorgt-deze-voor-massasurveillance~b4fe2f3c/.
12. De NCMEC-cijfers over het jaar 2021 bedroegen zelfs meer dan 29 miljoen meldingen wereldwijd.Annual Report 2021 NCMEC, p. 3. Zie https://www.missingkids.org/footer/about/annual-report#pdf. https://www.missingkids.org/ourwork/ncmecdata.
13. Van 17.500 meldingen in 2010 naar ruim een miljoen in 2020. Zie ook Commission staff working document impact assessment report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse SWD/2022/209, 11 mei 2022 (Hierna: 'Impact Assessment Report bij het Voorstel'), p. 22.
14. Zie https://www.eokm.nl/standpunten-van-het-eokm-over-de-europese-verordening-ter-voorkoming-en-bestrijding-van-seksueel-kindermisbruik/, 22 november 2022.

immers ook samenhangen met het toegenomen gebruik van het internet, met betere detectiemiddelen of een grotere meldingsbereidheid.[15]

Op verzoek van het EOKM voerden onderzoekers van de TU Delft een fact-check uit waarin zij de cijfers nader analyseerden.[16] Zij concludeerden onder meer dat de genoemde stijging van EU-gerelateerde meldingen tussen 2010 en 2020 met 6000% een valse voorstelling van zaken is. Niet elke CSAM-melding staat gelijk aan een uniek materiaalbestand (foto, video) en alhoewel het aantal EU-gerelateerde meldingen inderdaad fors is gestegen, was het aantal aangetroffen en gemelde bestanden volgens de TU Delft in de jaren 2018 en 2021 nagenoeg gelijk.[17] Deze conclusie is in lijn met de kanttekening die Facebook/Meta (de grootste melder bij NCMEC) plaatst bij haar eigen meldingen. Uit onderzoek van het bedrijf zelf blijkt dat bijna 90% van alle circa 20 miljoen meldingen van misbruikmateriaal die Facebook/Meta deed, slechts vijf of zes dezelfde, unieke beelden betrof.[18] Een handvol CSAM-beelden zwerft blijkbaar langdurig op het internet rond, wordt frequent gedeeld en steeds opnieuw gedetecteerd en gemeld: op zichzelf een ernstig probleem, maar geen aanwijzing voor een explosieve groei van het misbruik zelf.

Met betrekking tot het online benaderen van kinderen (online grooming) zijn minder datasets voorhanden. Volgens het NCMEC bedroeg het aantal meldingen in 2020 van online grooming wereldwijd 37.872 – maar dat is inclusief gemelde gevallen van sextortion.[19] Ten opzichte van het jaar 2019 zou dat bijna een verdubbeling van het aantal meldingen betekenen, die volgens de organisatie te verklaren is door de coronapandemie als gevolg waarvan potentiële slachtoffers én groomers meer tijd online doorbrachten. Het aantal bij NCMEC bekende grooming-gevallen dat betrekking had op de EU bedroeg in 2020 ruim 1400.[20]

2. Algemene aspecten en achtergrond van de voorgestelde Verordening

2.1. Interimregeling

Haastige spoed biedt zelden garanties voor een zorgvuldig besluitvorming. Toch wil de Commissie vaart zetten achter het besluitvormingsproces rond dit voorstel. Het voorstel vervangt een interim Verordening die nu van kracht is en in augustus 2024 afloopt.[21] Die tijdelijke Verordening staat nummeronafhankelijke interpersoonlijke communicatiediensten toe om onlinemateriaal van seksueel misbruik van kinderen vrijwillig op te sporen en te melden. Tot en met december 2020 kon dat zonder problemen en was voor die betreffende aanbieders uitsluitend de AVG van toepassing, voor zover ze binnen de reikwijdte van de AVG vallen. Na die datum moest de Richtlijn (EU) 2018/1972 zijn omgezet[22], wat deze aanbieders binnen het toepassingsgebied van de e-Privacy Richtlijn bracht.[23] Het feit dat deze laatste richtlijn geen specifieke bepalingen bevatte betreffende de verwerking van persoonsgegevens door aanbieders van elektronische-communicatiediensten met het oog op het opsporen, melden en verwijderen van online seksueel misbruik van kinderen op hun diensten en het melden ervan, noopte tot de voormelde interim Verordening.[24] Deze tijdelijke afwijking van de e-privacy Richtlijn geldt tot uiterlijk 3 augustus 2024 – een "harde deadline" dus voor de voorgestelde inwerkingtreding van de CSAM-Verordening.[25]

2.2. Lex specialis

Het voorstel is een *lex specialis* ten opzichte van het algemeen toepasselijke kader dat is vastgesteld in

15. Zie https://www.eokm.nl/standpunten-van-het-eokm-over-de-europese-verordening-ter-voorkoming-en-bestrijding-van-seksueel-kindermisbruik/, 22 november 2022.
16. Zie M. van Kesteren, M. van Eeten & R. van Wegberg, *CSAM Data. Factcheck of recent European Commission statements*, ongedateerd: https://www.bitsoffreedom.nl/wp-content/uploads/2023/02/TUDelft_CSAM_Factcheck_English.pdf. Zie ook https://www.euractiv.com/section/platforms/news/fact-checkers-call-out-commission-on-anti-child-abuse-material-proposal/ en https://www.bitsoffreedom.nl/2023/02/09/europese-commissie-doet-een-slecht-voorstel-met-een-slechte-onderbouwing/.
17. Het aantal bestanden dat werd aangetroffen en gemeld aan NCMEC was in de jaren 2018 en in 2021 nagenoeg gelijk (85 miljoen). Een afname van het aantal bestanden in 2019 en 2020 (respectievelijk 70 en 20 miljoen) hangt volgens de onderzoekers mogelijk samen met de coronapandemie. Zie M. van Kesteren, M. van Eeten & R. van Wegberg, *CSAM Data. Factcheck of recent European Commission statements*, ongedateerd, p. 6-7.
18. EOKM, *Standpunten van het EOKM over de Europese Verordening ter voorkoming en bestrijding van seksueel kindermisbruik*, 22 november 2022, zie www.eokm.nl.
19. Dit betreft meldingen via de CyberTipline van NCMEC: https://www.missingkids.org/content/ncmec/en/blog/2021/online-enticement-reports-skyrocket-in-2020.html In 2021 werden er 44.155 gevallen van "online enticement" inclusief sextortion gemeld.
20. Impact Assessment Report bij het Voorstel, p. 22.
21. Verordening (EU) 2021/1232 van het Europees Parlement en de Raad van 14 juli 2021 betreffende een tijdelijke afwijking van sommige bepalingen van Richtlijn 2002/58/EG ten aanzien van het gebruik van technologieën door aanbieders van nummeronafhankelijke interpersoonlijke communicatiediensten voor de verwerking van persoonsgegevens en andere gegevens ten behoeve van de bestrijding van online seksueel misbruik van kinderen (Interimregeling).
22. Europees wetboek voor elektronische communicatie.
23. Richtlijn 2002/58/EG.
24. Overweging 9 considerans Voorstel.
25. De Interimregeling moet dan bijgevolg worden ingetrokken, zie Overweging 78 considerans Voorstel.

de Digitaledienstenverordening (DSA).[26] Het voorstel bevat met name specifieke voorschriften voor de bestrijding van bepaalde vormen van illegale onlineactiviteiten (CSAM) en uitgewisselde 'illegale' online-inhoud (grooming), gekoppeld aan een reeks waarborgen.[27] Op die manier vormt het voorstel een aanvulling op het algemene kader waarin de DSA voorziet. Verder zijn de regels die in de DSA zijn uiteengezet van toepassing op aangelegenheden die niet of niet volledig zijn geregeld in de voorgestelde Verordening.[28]

2.3. Aanbieders

De voorgestelde Verordening is van toepassing op een brede waaier aan aanbieders van diensten van de informatiemaatschappij die kunnen worden misbruikt voor online seksueel kindermisbruik.[29] Dat zijn allereerst de aanbieders van hostingdiensten, dat wil zeggen diensten van de informatiemaatschappij die bestaan in de opslag van de door een afnemer van de dienst verstrekte informatie, op diens verzoek.[30] Hiertoe behoren in de systematiek van de DSA alle aanbieders van hostingdiensten, online platforms en zeer grote online platforms. Die laatste twee categorieën worden gezien als een subcategorie van de hostingdiensten in de zin van de DSA, namelijk als dienstverleners die informatie van hun gebruikers (*user generated content*) niet alleen opslaan maar ook publiekelijk verspreiden.[31]

Verder vallen binnen de werkingssfeer van de voorgestelde Verordening ook de al eerdergenoemde 'voor het publiek beschikbare (nummeronafhankelijke) interpersoonlijke communicatiediensten'[32], dat wil zeggen VoIP, berichtendiensten en webgebaseerde e-maildiensten, aangezien deze, zo staat in de toelichting te lezen, in toenemende mate voor online seksueel misbruik van kinderen worden gebruikt.[33]

Bovendien heeft het voorstel betrekking op diensten "waarbij de directe interpersoonlijke en interactieve uitwisseling van informatie louter een onbeduidend nevenelement vormt dat intrinsiek verbonden is met een andere dienst" - het gaat dan bijvoorbeeld om chatfuncties en dergelijke als onderdeel van games, het delen van beelden en het hosten van video's.[34]

En ook aanbieders van appstores, in het licht van hun rol als tussenpersonen die de toegang vergemakkelijken tot softwaretoepassingen die kunnen worden misbruikt om kinderen te benaderen, vallen binnen het toepassingsbereik van de voorgestelde Verordening.[35]

Tot slot vallen ook de internettoegangsdiensten onder het voorstel waar het gaat om een eventueel blokkeringsbevel dat aanbieders van internettoegangsdiensten ertoe verplicht redelijke maatregelen te nemen om te voorkomen dat gebruikers toegang hebben tot bekend materiaal van seksueel misbruik van kinderen (zie de volgende paragraaf).[36]

In zijn algemeenheid heeft de voorgestelde Verordening betrekking op specifieke *diensten* die door de aanbieders geleverd worden en niet op de aanbieders als zodanig. Als een aanbieder meerdere diensten aanbiedt, is het dus goed mogelijk dat sommige diensten wel en andere niet onder het voorstel vallen.[37]

De plaats van vestiging van de betrokken aanbieder is niet van belang. De regels in de voorgestelde Verordening gelden voor alle aanbieders, ongeacht hun plaats van vestiging of verblijf, die diensten in de EU aanbieden, "hetgeen moet blijken uit een reële band met de Unie".[38] Een dergelijke reële band moet worden aangenomen wanneer de aanbieder een vestiging heeft in de EU of, indien dit niet het geval is, op grond van het bestaan van een aanzienlijk aantal gebruikers in of activiteiten gericht op een of meer EU-lidstaten.[39]

2.4. Content

Zoals al eerder aangestipt, ziet het voorstel op verschillende categorieën online seksueel misbruik van kinderen.[40] In de eerste plaats gaat het om de verspreiding van beeldmateriaal van seksueel misbruik

26. Verordening (EU) 2022/2065 van het Europees Parlement en de Raad van 19 oktober 2022 betreffende een eengemaakte markt voor digitale diensten en tot wijziging van Richtlijn 2000/31/EG (digitaledienstenverordening). Zie Overweging 8 considerans Voorstel.
27. Toelichting Voorstel, p. 6.
28. Overweging 8 considerans Voorstel
29. Overweging 5 considerans Voorstel.
30. Zie artikel 3 punt g, onder iii DSA. In Artikel 2 sub a van de voorgestelde Verordening wordt nog verwezen naar artikel 2, punt f, derde streepje van het voorstel voor de DSA.
31. Artikel 3 punt i en k DSA. Zie onder meer F. Wilman, 'De *Digital Services Act* (DSA): een belangrijke stap naar betere regulering van onlinedienstverlening', *Nederlands tijdschrift voor Europees Recht* 2022, afl. 9/10, p. 222.
32. In de zin van art 2 sub 5 van het Europees Wetboek voor elektronische communicatie.
33. Overweging 5 considerans Voorstel.
34. Overweging 5 considerans voorstel.
35. En dus ook worden verplicht bepaalde redelijke maatregelen te nemen om dat risico te beoordelen en te beperken (zie daarover de volgende paragraaf). Zie ook Overweging 19 considerans en artikel 6 Voorstel.
36. Artikel 16 Voorstel.
37. F. Wilman, 'De *Digital Services Act* (DSA): een belangrijke stap naar betere regulering van onlinedienstverlening', *Nederlands tijdschrift voor Europees Recht* 2022, afl. 9/10, p. 221-222.
38. Zie Overweging 6 considerans en Art 1 lid 2 van het Voorstel.
39. Overweging 11 considerans Voorstel. Zie ook art. 2 lid 1 DSA en art. 3 onder d en e DSA.
40. Waarbij een kind wordt gedefinieerd als een natuurlijk persoon die jonger is dan 18 jaar, zie art. 2 onder i van het voorstel.

van kinderen: audiovisuele content, zoals foto's, video's en streaming materiaal, waarop seksueel misbruik van kinderen wordt getoond (CSAM).[41] Dit kan zowel *bekend* kinderpornografisch materiaal zijn, waarvan eerder al is vastgesteld dat het materiaal van seksueel misbruik van kinderen betreft, als ook *nieuw,* dat wil zeggen onbekend kinderpornografisch materiaal.[42] Daarnaast gaat het om activiteiten die neerkomen op het online benaderen van kinderen voor seksuele doeleinden, in de Engelse versie van het voorstel aangeduid als de 'solicitation of children', of online grooming. Hierbij speelt 'talige' content een rol, de geschreven of gesproken tekst die wordt uitgewisseld in de mondelinge of schriftelijke communicatie tussen een potentiële groomer en een minderjarige.[43]

Daarmee is het scala aan uitingen dat de Commissie met het voorstel wil aanpakken tamelijk breed. Het betreft hetzij online content die in zichzelf strafbaar is (als het gaat om kinderpornografisch materiaal) hetzij niet-strafbare content die mogelijk leidt tot strafbare gedragingen (als het gaat om online grooming). De aanpak middels een en dezelfde regeling is nodig, aldus de Commissie, om niet alleen misbruik uit het verleden, de daaruit voortvloeiende hervictimisatie en schending van de rechten van de slachtoffers (bij bekend materiaal) aan te pakken, maar ook om recent en huidig misbruik (bij nieuw materiaal) op te sporen en dreigend misbruik (bij grooming) zoveel mogelijk te voorkomen.[44]

Bij het Impact Assessment van het voorstel is een totaal van vijf verschillende beleidsopties onderzocht. Deze liepen qua impact en omvang op: van geheel afzien van wetgevend ingrijpen (optie A), via vrijwillige opsporing van CSAM door aanbieders (optie B), verplicht detecteren van uitsluitend bekende CSAM (optie C), de aanpak van bekende en nieuwe CSAM (optie D) tot de meest ingrijpende en veelomvattende optie waarbij aanbieders ook verplicht zijn grooming op te sporen (optie E).[45] Deze laatste optie E, die in het nu voorliggende voorstel is uitgewerkt, werd het meest effectief geacht om dreigend misbruik te voorkomen en houdt in grote lijnen in: de oprichting van een EU-centrum als gedecentraliseerd EU-agentschap, verplichte opsporing door aanbieders van bekende en onbekende CSAM en grooming gebaseerd op opsporingsbevelen, verplichte melding van mogelijk online seksueel misbruik van kinderen aan het EU-centrum, en een verplichting tot het verwijderen van CSAM.[46]

2.5. EU-centrum en Coördinerende Autoriteit

Naast de Europese Commissie, de relevante aanbieders van online diensten, en de talloze nationale en internationale organisaties die zich bezighouden met de strijd tegen CSAM, zullen de opsporingsautoriteiten van de lidstaten, en ook Europol betrokken zijn bij de uitvoering van het voorstel.[47] Bovendien worden aan dat toch al drukbevolkte CSAM-ecosysteem nog twee nieuwe entiteiten toegevoegd: het eerdergenoemde "EU-centrum" en een "Coördinerend Autoriteit van vestiging".

Het "EU-centrum" is een nieuw op te richten gedecentraliseerd agentschap dat in samenwerking met nationale Coördinerende Autoriteiten in de EU-lidstaten uitvoering zal geven aan de nieuwe Verordening. Het zal worden gevestigd in Den Haag, op dezelfde locatie als Europol, waarmee het intensief zal gaan samenwerken.[48] Het takenpakket van dit nieuwe Centrum is breed.[49] Het zal onder meer de aanbieders ondersteunen bij hun risicobeoordeling, en bij het opsporings-, meldings- en verwijderingsproces (zie paragraaf 3). Het gaat ook de Coördinerende Autoriteiten assisteren bij hun taken, de samenwerking tussen die autoriteiten ondersteunen en zorgen voor slachtofferbegeleiding.

Een centrale taak van het Centrum is het opzetten, onderhouden en beheren van een databank waarin indicatoren van CSAM worden opgeslagen en van een taalidentificatoren-databank ten behoeve van de opsporing van grooming. Het zal kosteloos technologieën beschikbaar stellen aan de aanbieders ter ondersteuning van de opsporing van CSAM en grooming. En het fungeert als een centraal punt waar de meldingen van CSAM en grooming door de aanbieders worden ontvangen, beoordeeld en gecontroleerd op valse positieven. Na controle stuurt het Centrum de meldingen door aan Europol en de nationale autoriteiten. Het idee is dat de nationale instanties baat zullen hebben bij deze facilitering door het EU-centrum, met name doordat de controle van de CSAM-meldingen garandeert dat de meldingen die uiteindelijk naar de nationale instanties gaan relevant zullen zijn en voldoende informatie bevatten voor nader onderzoek.[50]

41. Artikel 2 onder l. Voor de definitie van materiaal van seksueel misbruik van kinderen wordt aangehaakt bij de definitie in artikel 2 punten c en e van de Richtlijn 2011/93/EU.
42. Zie Overweging 13 considerans en artikel 2 onder m en n van het Voorstel.
43. Artikel 2 onder o van het Voorstel.
44. Overweging 13 considerans Voorstel. Online grooming wordt immers (in het strafrecht) beschouwd als een voorbereidingsdelict dat een eerste aanzet kan vormen voor andere (fysieke) seksuele delicten.
45. Impact Assessment Report bij het Voorstel, p. 16.
46. Toelichting bij het Voorstel, p. 12; Impact Assessment Report bij het Voorstel, p. 112.
47. Toelichting bij het Voorstel, p. 4 en p. 120. De meldingen die binnenkomen en worden gecontroleerd bij het EU-centrum worden doorgestuurd naar Europol en de nationale rechtshandhavingsinstanties.
48. Artikel 42 en p. 4 Toelichting bij het Voorstel. Een vertegenwoordiging van Europol zal deel uitmaken van de raad van bestuur van het EU-centrum.
49. Impact Assessment Report bij het Voorstel, p. 81.
50. Voorstel, p. 120.

2.6. ATKM

In het voorstel worden nieuwe, door de afzonderlijke lidstaten aan te wijzen nationale Coördinerende Autoriteiten geïntroduceerd.[51] De Coördinerende Autoriteit speelt een centrale rol bij de toepassing en handhaving van de voorgestelde Verordening in de betrokken lidstaat, met name van het pakket verplichtingen voor de aanbieders waarin dit Voorstel voorziet (zie verder paragraaf 3). Voor het uitvoeren van hun taken beschikken deze Coördinerende Autoriteiten over een reeks stevige onderzoeks- en handhavingsbevoegdheden ten aanzien van de aanbieders van relevante diensten, variërend van inspecties ter plaatse tot het gelasten van een tijdelijke toegangsbeperking voor gebruikers van de dienst.[52]

Naar verluidt zal in Nederland de ATKM i.o. (Autoriteit Online Terroristisch en Kinderpornografisch Materiaal) als Coördinerend Autoriteit gaan fungeren.[53] De ATKM zal zich gaan richten op de bestrijding van online kinderpornografisch materiaal en online grooming, maar ook van online terroristische content - dit laatste ter uitvoering van de Europese Verordening inzake het tegengaan van terroristische online-inhoud.[54] Dat die verschillende taken binnen één autoriteit zullen worden verenigd was al eerder door de Minister aangekondigd.[55]

De instelling van de ATKM wordt geregeld in de Wet bestuursrechtelijke aanpak online kinderpornografisch materiaal waarover de Raad van State in mei 2022 advies heeft uitgebracht en die volgens de planning begin 2023 zou worden behandeld in de Tweede Kamer.[56] In december 2022 kondigde minister Yeşilgöz aan dat de oprichting van de ATKM, waarvoor inmiddels een kwartiermaker is aangesteld, eveneens op de agenda staat voor begin 2023.[57]

51. Artikelen 25 en verder van het Voorstel.
52. Artikel 27 respectievelijk artikelen 28-32 van het Voorstel.
53. Zie https://www.rijksoverheid.nl/ministeries/ministerie-van-justitie-en-veiligheid/organisatie/organogram/directoraat-generaal-rechtspleging-en-rechtshandhaving-dgrr/autoriteit-online-terroristisch-en-kinderpornografisch-materiaal-atkm.
54. Verordening (EU) 2021/784 van het Europees Parlement en de Raad van 29 april 2021 inzake het tegengaan van de verspreiding van terroristische online-inhoud.
55. Kamerstukken II 2020/21, 31015, nr. 208. En zie https://www.rijksoverheid.nl/actueel/nieuws/2020/11/20/toezichthouder-tegen-kinderporno-en-terroristisch-materiaal-online.
56. https://www.raadvanstate.nl/actueel/nieuws/mei/aanpak-online-kinderpornografisch/@127611/w16-21-0337/
57. Vaste Kamercommissie J&V, 4 oktober 2022 (technische briefing). Zie ook: https://www.tweedekamer.nl/nieuws/kamernieuws/debat-over-tegengaan-verspreiding-terroristisch-online-materiaal.

3. Verplichtingen voor aanbieders

Een aanzienlijk deel van het toch al tamelijk omvangrijke voorstel (met zijn 89 artikelen en een considerans bestaande uit 84 overwegingen) heeft betrekking op de verplichtingen voor de aanbieders. Deze - deels nieuwe, en deels aansluitend bij de uit de DSA voortvloeiende - verplichtingen zijn in te delen in een fase waarin aanbieders zelfstandig actie dienen te ondernemen om het risico op hun diensten aan te pakken en een fase waarin zij ter uitvoering van een opsporingsbevel verplicht zijn technische maatregelen te nemen om online seksueel misbruik van kinderen via hun diensten op te sporen.

3.1. Risicobeoordeling en -beperking

Het CSAM-voorstel schrijft voor dat in eerste instantie alle relevante aanbieders, voor de diensten die zij in de EU aanbieden, het risico identificeren, analyseren en beoordelen dat die dienst wordt gebruikt voor de verspreiding van bekend of nieuw materiaal van seksueel misbruik van kinderen of het benaderen van kinderen.[58] Bij het uitvoeren van die beoordeling van het risicomisbruik werken de aanbieders met een aan hen verstrekte, niet-limitatieve lijst van beoordelingselementen. Hierop staan zaken als: eerder vastgestelde gevallen van het gebruik van de diensten voor online seksueel misbruik van kinderen; bestaand intern beleid omtrent de aanpak van dat risico, zoals functies voor leeftijdsverificatie; meldingsmogelijkheden; de mate waarin de dienst wordt gebruikt door kinderen, enzovoorts.[59] De risicobeoordeling vindt in beginsel elke drie jaar opnieuw plaats.[60] In het geval dat aanbieders al verplicht zijn een risicobeoordeling uit te voeren uit hoofde van de DSA, kunnen zij zich baseren op die risicobeoordeling en deze aanvullen met een meer specifieke beoordeling van het misbruikrisico van hun dienst(en) voor online seksueel misbruik van kinderen.[61]

Na de risicobeoordeling worden de aanbieders geacht (waar en indien nodig) "redelijke", dat wil zeggen doeltreffende, op maat gesneden en evenredige risicobeperkende maatregelen te nemen.[62] Ook dan geldt dat aanbieders die reeds verplicht zijn uit hoofde van de DSA dergelijke maatregelen te nemen kunnen nagaan of er nog andere, gerichte maatregelen nodig zijn.[63]

Het voorstel bedoelt met risicobeperkende maatregelen algemene ingrepen als: het technisch, operationeel of middels personeel aanpassen van de

58. Afdeling 1 (artikelen 3-6) van het Voorstel.
59. Artikel 3 lid 2 Voorstel. Zie ook Overweging 14 considerans Voorstel.
60. Artikel 3 lid 4 Voorstel.
61. Overweging 15 considerans Voorstel.
62. Artikel 4 leden 1 en 2 Voorstel. Zie ook Toelichting p. 19 en Overweging 16 considerans Voorstel.
63. Overweging 16 considerans Voorstel.

inhoudsmoderatie- en aanbevelingssystemen, of het aanpassen van de besluitvormingsprocessen, het versterken van de werking en functies van de dienst, de inhoud en handhaving van de algemene voorwaarden, het aangaan van samenwerking en het nemen van noodzakelijke maatregelen voor leeftijdsverificatie en leeftijdsbepaling (met name door aanbieders van diensten die kunnen worden gebruikt voor het benaderen van kinderen).[64] Al bij al nogal voor de hand te liggende maatregelen waarin, zeker door grotere aanbieders, al wel zal zijn voorzien. Met het oog op de transparantie dienen aanbieders duidelijk in hun algemene voorwaarden te beschrijven welke risicobeperkende maatregelen zij hebben genomen, zonder daarbij informatie weg te geven die de effectiviteit van de maatregelen zou kunnen verminderen.[65]

Aan appstores, ten slotte, worden gerichte verplichtingen opgelegd om te beoordelen of via hen verspreide toepassingen mogelijk worden gebruikt om kinderen te benaderen en om, indien dit het geval is en het risico aanzienlijk is, redelijke maatregelen te nemen om kind-gebruikers te identificeren en te voorkomen dat zij toegang tot de toepassing krijgen.[66]

De aanbieders brengen vervolgens over hun risicobeoordeling en de door hen getroffen risicobeperkende maatregelen verslag uit, zowel aan het EU-centrum[67] als aan de door de EU-lidstaat aangewezen Coördinerend Autoriteit die de risicobeoordeling en de getroffen risicobeperkende maatregelen toetst.[68]

3.2. Opsporingsverplichtingen

Een tweede regime treedt in werking wanneer na deze toetsing de Coördinerende Autoriteit van mening is dat er bewijs is van een "significant" risico dat de dienst (nog steeds) wordt gebruikt voor online seksueel misbruik van kinderen en dat de maatregelen die de aanbieder neemt om zijn misbruikrisico te reduceren ontoereikend zijn. Hieronder wordt toegelicht hoe dat significante risico precies wordt vastgesteld voor de verschillende aanbieders.

Daarmee komt de aanbieder in de tweede fase en ook in een tweede regime terecht, namelijk die van de zogenaamde "opsporingsverplichtingen" voor aanbieders, die als het ware de kern en tegelijkertijd het meest controversiële onderdeel van de voorgestelde Verordening vormt. Het lijkt mij overigens geen onrealistische inschatting dat voor het merendeel van de aanbieders dat "significante risico" voor hun diensten(en) bewezen wordt en dat het gros van de aanbieders te maken krijgt met die opsporingsverplichtingen. In Afdeling 2 van het Voorstel, de artikelen 7 tot en met 11, worden de regels, procedures en waarborgen rond de uitvaardiging en uitvoering van opsporingsbevelen uitgewerkt.

De door de EU-lidstaat aangewezen Coördinerende Autoriteit kan de bevoegde gerechtelijke autoriteit van de lidstaat of een andere onafhankelijke administratieve autoriteit verzoeken een opsporingsbevel ("detection order") uit te vaardigen.[69] Dit opsporingsbevel verplicht een aanbieder ertoe maatregelen te nemen, dat wil zeggen technologieën te installeren en te gebruiken, om de verspreiding van bekend of nieuw materiaal van seksueel misbruik van kinderen of het benaderen van kinderen op te sporen.[70]

Een opsporingsbevel kan alleen maar worden verzocht en uitgevaardigd wanneer de Coördinerende Autoriteit van mening is dat er, zoals hierboven reeds besproken, bewijs is van een significant risico dat de dienst wordt gebruikt voor online seksueel misbruik van kinderen en de redenen voor het uitvaardigen van het opsporingsbevel (de bescherming van kinderen) zwaarder wegen dan de negatieve gevolgen ervan voor de rechten en gerechtvaardigde belangen van alle getroffen partijen.[71]

De invulling van de term significant risico (dat in artikel 7 lid 5 overigens wordt aangeduid met *aanzienlijk* risico) hangt direct samen met het specifieke type seksueel misbruik waarop het opsporingsbevel betrekking heeft (bekende CSAM, nieuwe CSAM of grooming). Een aanzienlijk risico op de verspreiding van bekend CSAM-materiaal is aanwezig wanneer het waarschijnlijk is dat de dienst ondanks de risicobeperkende maatregelen in belangrijke mate wordt gebruikt voor die verspreiding en er bewijs is dat de dienst in de afgelopen twaalf maanden in belangrijke mate is gebruikt voor die verspreiding.[72]

Wat betreft nieuw (onbekend) CSAM-materiaal is sprake van een significant risico wanneer het waarschijnlijk is dat de dienst ondanks de risicobeperkende maatregelen in belangrijke mate wordt gebruikt voor die verspreiding, als er bewijs is dat de dienst in de afgelopen twaalf maanden in belangrijke mate is gebruikt voor de verspreiding van onbekend CSAM, er een opsporingsbevel is uitgevaardigd met betrekking tot de verspreiding van bekend materiaal en de aanbieder een aanzienlijk aantal meldingen van bekend materiaal heeft ingediend dat is opgespoord aan de hand van de getroffen maatregelen in het kader van dat opsporingsbevel.[73]

64. Artikel 4 lid 3 Voorstel.
65. Artikel 4 lid 4 Voorstel.
66. Artikel 6 Voorstel. Toelichting bij het Voorstel, p.19.
67. Artikel 5 lid 5 Voorstel.
68. Artikel 5 lid 1 Voorstel.
69. Artikel 7 lid 1 Voorstel.
70. Artikelen 7 en 8 Voorstel.
71. Artikel 7 lid 4 Voorstel. Er moet dus sprake zijn van een *fair balance* tussen de erdoor geraakte grondrechten.
72. Artikel 7 lid 5 Voorstel.
73. Artikel 7 lid 6 Voorstel.

Als het gaat om een significant risico op het benaderen van kinderen wordt aangenomen dat dat bestaat wanneer de aanbieder een aanbieder is van interpersoonlijke communicatiediensten en het waarschijnlijk is dat de dienst ondanks de risicobeperkende maatregelen in belangrijke mate wordt gebruikt voor het benaderen van kinderen en er bewijs is dat de dienst in de afgelopen twaalf maanden in belangrijke mate is gebruikt voor het benaderen van kinderen. Daarbij is het van belang dat opsporingsbevelen betreffende het benaderen van kinderen alleen van toepassing zijn op interpersoonlijke communicatie waarbij een van de gebruikers een kindgebruiker is.[74]

Met de aanduiding "in belangrijke mate" wordt in deze bepalingen overigens bedoeld dat de dienst "in meer dan in geïsoleerde en relatief zeldzame gevallen" voor dergelijk misbruik wordt gebruikt.[75]

De duur van de periode waarin een opsporingsbevel van toepassing is, hangt af van de aard van de content waarop dat opsporingsbevel ziet. Wanneer een bevel betrekking heeft op de verspreiding van bekend of nieuw CSAM-materiaal is de toepassingsperiode maximaal 24 maanden; wanneer het betrekking heeft op het benaderen van kinderen (grooming) is de duur van het bevel maximaal 12 maanden.[76] Het is overigens moeilijk voorstelbaar dat, wanneer een aanbieder eenmaal opsporingstechnologieën heeft geïnstalleerd en die in gebruik heeft genomen, hij deze na die toepassingsperiode van het opsporingsbevel, dus na een jaar of twee jaar weer zou verwijderen uit zijn systeem of buiten werking zou stellen. Alleen al omdat hij in dat geval binnen de kortste keren de toets van de risicobeoordeling en -beperking waarschijnlijk (opnieuw) niet zou doorstaan en te maken krijgt met een nieuwe opsporingsverplichting. Aannemelijker is dat eenmaal geïnstalleerde en in gebruik genomen opsporingstechnologieën een permanente plek krijgen in het "opsporingsbeleid" van aanbieders.

Aanbieders die een opsporingsbevel hebben ontvangen en ook gebruikers die worden getroffen door de maatregelen die worden genomen ter uitvoering van een opsporingsbevel hebben het recht op doeltreffende verhaalmogelijkheden, waaronder het recht om het opsporingsbevel te betwisten voor de gerechten van de lidstaat van de autoriteit die het opsporingsbevel heeft uitgevaardigd.[77] Het is goed voorstelbaar dat de toepassing van deze regels omtrent de verplichtingen voor aanbieders zal leiden tot de nodige klachten, geschillen en procedures, net zoals dat overigens wordt verwacht van de DSA.[78]

3.3. Meldings-, verwijderings- en blokkeerverplichtingen

Naast de opsporingsverplichtingen voorziet het voorstel ook in bepalingen met betrekking tot verplichtingen om CSAM te melden, te verwijderen en te blokkeren (Afdelingen 3-5 van het Voorstel).

Wanneer aanbieders kennisnemen van informatie die duidt op potentieel online seksueel misbruik van kinderen via hun diensten, dienen zij dit te melden bij het EU-centrum.[79] Hoe zij aan die informatie komen, is niet van belang. Zij kunnen daarvan op de hoogte raken door de uitvoering van opsporingsbevelen, door meldingen van gebruikers of organisaties die zich toeleggen op het opsporen van seksueel misbruik van kinderen, of door activiteiten op hun eigen initiatief.[80] Daarbij is van belang dat mogelijke twijfels over de leeftijd van potentiële slachtoffers de aanbieders er niet van mogen weerhouden om een melding in te dienen. Het is de bedoeling dat het EU-centrum de meldingen screent en vaststelt of deze bruikbaar zijn, de valse positieven verwijdert en de rest vervolgens doorzendt naar Europol en/of de nationale opsporingsautoriteiten. Het Centrum zal zelf uiteraard geen verdere onderzoeks- of opsporingsbevoegdheden krijgen.[81]

Om ervoor te zorgen dat CSAM zo snel mogelijk na ontdekking ervan verwijderd wordt, is de Coördinerende Autoriteit van een lidstaat bevoegd om de bevoegde gerechtelijke autoriteit of een andere administratieve autoriteit van die lidstaat te verzoeken een verwijderingsbevel uit te vaardigen dat een aanbieder verplicht een of meer specifieke items te verwijderen of materiaal ontoegankelijk te maken dat is geïdentificeerd als CSAM.[82] Verwijderingsbevelen moeten binnen 24 uur na de ontvangst ervan worden uitgevoerd.[83] Aanbieders die een verwijderingsbevel hebben ontvangen alsook gebruikers die het materiaal hebben verstrekt hebben recht op effectieve verhaalmogelijkheden.[84]

Verder kan een Coördinerende Autoriteit de bevoegde gerechtelijke autoriteit of een onafhankelijke administratieve autoriteit van de lidstaat verzoeken een blokkeringsbevel uit te vaardigen dat een aanbieder van internettoegangsdiensten ertoe verplicht redelijke maatregelen te nemen om te voorkomen dat gebruikers toegang hebben tot bekend materiaal van seksueel misbruik van kinderen. Dergelijke blokkeringsbevelen zijn gebaseerd op de lijst van URL's die naar specifieke gevallen van geverifieerd seksueel misbruik van kinderen leiden en die zijn

74. Artikel 7 lid 7 Voorstel.
75. Overweging 21 considerans Voorstel.
76. Artikel 7 lid 9 Voorstel.
77. Artikel 9 Voorstel.
78. Zie F. Wilman, 'Het voorstel voor de Digital Services Act. Op zoek naar nieuw evenwicht in regulering van onlinediensten met betrekking tot informatie van gebruikers, Nederlands tijdschrift voor Europees Recht, afl. 1/2, 2021.
79. Artikel 12 lid 1 Voorstel.
80. Overweging 29 considerans Voorstel.
81. Impact Assessment Report bij het Voorstel, p. 68.
82. Artikel 14 lid 1 Voorstel. Overweging 30 considerans Voorstel.
83. Artikel 14 lid 2 Voorstel.
84. Artikel 15 Voorstel.

opgenomen in de indicatorenbank van het EU-centrum.[85] Blokkeringsbevelen moeten gelimiteerd zijn in tijd en mogen maximaal vijf jaar van toepassing zijn.[86] Aanbieders van internettoegangsdiensten die een blokkeringsbevel hebben ontvangen en ook gebruikers die een specifiek item hebben verstrekt of die geen toegang hebben gekregen tot een specifiek geblokkeerd item hebben het recht op doeltreffende verhaalmogelijkheden.[87]

Sancties

In aanvulling op de hierboven besproken (aanvullende) handhavingsbevoegdheden stellen de EU-lidstaten zelf de regels vast inzake sancties die van toepassing zijn op inbreuken op deze voorgestelde Verordening door aanbieders.[88] Het maximale bedrag van de sancties die kunnen worden opgelegd bij een inbreuk op (verplichtingen uit hoofde van) de Verordening is maximaal 6% van de jaarlijkse inkomsten of totale omzet.[89]

Al met al komen er met dit voorstel veel nieuwe taken en verplichtingen op aanbieders af. Zeker voor degenen die op dit moment nog niet (vrijwillig) CSAM monitoren en melden. Met name voor het MKB zal het ook een extra praktische en financiële belasting met zich brengen. En niet in de laatste plaats heeft het voorstel ingrijpende gevolgen voor de aanbieders die op dit moment versleutelde uitwisseling en communicatie tussen gebruikers mogelijk maken, waarover in de volgende paragraaf meer.[90]

4. Opsporingstechnologieën en E2EE communicatie

Zoals in de vorige paragraaf al enkele malen aangestipt bestaat de uitvoering van het opsporingsbevel door een aanbieder grotendeels uit het installeren en in gebruik nemen van opsporingstechnologieën, en het daarbij in acht nemen van bepaalde waarborgen. Deze onderwerpen zijn geregeld in artikel 10 van het voorstel dat stelt dat aanbieders het opsporingsbevel uitvoeren door opsporingstechnologieën te installeren en te gebruiken om online seksueel misbruik van kinderen op te sporen, waarbij ze gebruik maken van de indicatoren die beschikbaar worden gesteld door het EU-centrum.

Aanbieders zijn daarbij niet verplicht een bepaalde specifieke technologie te gebruiken; zij mogen hun eigen technologie ontwikkelen of technologie gebruiken die hen "free of charge" ter beschikking wordt gesteld door het EU-centrum, zolang de technologieën maar voldoen aan de volgende vereisten[91]:

1. Doeltreffend voor het opsporen van de verspreiding van CSAM en grooming;
2. Niet bruikbaar om andere informatie uit de communicatie te halen dan die informatie die strikt noodzakelijk is voor het met behulp van de indicatoren opsporen van patronen die duiden op CSAM of grooming;
3. In overeenstemming met *state of the art* techniek in de sector en het minst ingrijpend voor de privacy, de vertrouwelijkheid van communicatie en de bescherming van persoonsgegevens;
4. Voldoende betrouwbaar in de zin dat ze het foutenpercentage (*valse positieve en valse negatieve meldingen*) zo veel mogelijk beperken.

De aanbieder moet ervoor zorgdragen dat de technologieën, indicatoren en persoonsgegevens uitsluitend worden gebruikt voor het opsporen van CSAM en grooming, hij voorkomt misbruik van de technologieën, de indicatoren en persoonsgegevens, zorgt voor regelmatig menselijk toezicht, en stelt een klachtenprocedure in voor gebruikers. Verder informeert de aanbieder gebruikers over het feit dat en de manier waarop hij de opsporingstechnologieën gebruikt en de gevolgen ervan voor de vertrouwelijkheid van de communicatie van de gebruikers, over zijn meldingsplicht en over de klachtenprocedure. De aanbieder verstrekt geen informatie die de doeltreffendheid van de maatregelen zou kunnen beperken.[92]

Bijlage 8 van het Impact Assessment rapport bij het voorstel gaat uitgebreid in op de verschillende toe te passen technologieën zoals beeldherkenningssoftware (classifiers, AI), hashing technologie en taalherkenningssoftware en wat die zoal behelzen. Heel in het kort gaat het om de volgende tools:

4.1. Classifiers en A.I.

Technologieën die gebruikt kunnen worden voor het opsporen van nieuw CSAM-beeldmateriaal bestaan uit *classifiers* en kunstmatige intelligentie (AI). Een classifier is een algoritme dat informatie categoriseert door middel van patroonherkenning - zij kunnen bijvoorbeeld naaktheid, vormen en kleuren herkennen. Classifiers hebben gegevens nodig om op te trainen en hun nauwkeurigheid neemt toe naarmate ze meer gegevens ontvangen (*machine learning*).[93]

85. Artikel 16 lid 1 Voorstel
86. Artikel 16 lid 6 Voorstel.
87. Artikel 18 lid 1 Voorstel.
88. Artikel 35 lid 1 Voorstel. Het gaat onder meer om inbreuken waarbij de aanbieder de bevelen zoals hierboven beschreven niet naleeft en inbreuken op verplichtingen inzake gegevensverzameling en transparantieverslaglegging, respectievelijk hoofdstuk II en V van het Voorstel.
89. Artikel 35 lid 2 Voorstel. Bij het verstrekken van onjuiste informatie, het nalaten antwoord te geven of onjuiste informatie te rectificeren, of het weigeren van een inspectie bedraagt de sanctie maximaal 1% van de jaarlijkse inkomsten respectievelijk jaaromzet, zie Artikel 35 lid 3 jo artikel 27 Voorstel.
90. Zie ook Impact Assessment Report bij het Voorstel, p. 175.
91. Artikel 10 lid 3 Voorstel.
92. Artikel 10 lid 5 Voorstel.
93. https://deepai.org/machine-learning-glossary-and-terms/classifier.

Een bestaande classifier is de zogenaamde Safer-tool die voorzien is van een machine learning classificatiemodel.[94] De tool is ontwikkeld door het Amerikaanse Thorn, een van de organisaties die zich groot voorstander heeft getoond van de voorgestelde CSAM-verordening. De Thorn-classifier is getraind op datasets van in totaal honderdduizenden afbeeldingen en kan dus zowel nieuw als ook bekend CSAM herkennen. Ook Google en Facebook bieden vergelijkbare tools aan.

4.2. Hashing

Eenmaal opgespoord en geclassificeerd kunnen CSAM-beelden worden opgeslagen als een hashwaarde in een database. Hashing-technologie produceert een unieke digitale vingerafdruk van elk kinderpornografisch beeld (foto en video) waarbij het beeld wordt omgezet in een unieke letter/cijfercode die onomkeerbaar is (waardoor het oorspronkelijke beeld niet meer uit de hashwaarde is terug te halen). Om bekende CSAM op te sporen worden technologieën gebruikt die meestal zijn gebaseerd op de hashingmethode. Bij het opsporen van bekend materiaal dat wordt gedeeld op de dienst van een aanbieder moet dan elk gedeeld beeld in principe worden omgezet in een hash die dan vervolgens kan worden vergeleken met hashwaarden van bekende CSAM die zijn opgeslagen in een indicatorendatabank.[95] Wanneer er geen match plaatsvindt tussen de hash van het opgespoorde beeld en de hashes in de databank, wordt verder geen informatie over dat beeld opgeslagen. Wanneer een treffer plaatsvindt, verhinderen de aanbieders de verdere verspreiding van het materiaal.

Er bestaan vele soorten hashingtechnologieën, waaronder het veelgebruikte PhotoDNA van Microsoft.[96] Het Impact Assessment rapport merkt hierover op dat PhotoDNA inmiddels meer dan tien jaar oud is en wel een periodieke update kan gebruiken om het minder kwetsbaar te maken voor manipulatie, bijvoorbeeld het lichtelijk aanpassen van CSAM-materiaal zodat er geen match meer is met de oorspronkelijke hash-waarde.[97]

4.3. Taalherkenningssoftware

Tools voor de opsporing van het benaderen van kinderen in tekstcommunicatie maken gebruik van technologieën die taalpatronen en "verdachte" woorden herkennen, die mogelijk wijzen op het (seksualiserend) benaderen van kinderen online (zonder daarbij de inhoudelijke betekenis te kunnen afleiden) Ook hiervoor zal een databank met bekende taalpatronen, en -structuren en verdachte woorden en begrippen nodig zijn om de gescande communicatie mee te kunnen vergelijken. De technologie die hierbij wordt gebruikt heeft wel iets weg van de technologie die wordt gebruikt bij spamfilters. Een bekende taalherkenningstool is Microsofts Artemis.[98]

In een reactie op het voorstel benadrukte het EOKM dat de A.I. die momenteel beschikbaar is voor het scannen en analyseren van teksten en gesprekken op eventuele schadelijke inhoud, nog in de kinderschoenen staat. Navraag leerde bovendien, aldus het EOKM, dat ontwikkelaars van dit soort software scannen op teksten als "Is je moeder thuis?". Het moge duidelijk zijn dat dit zou leiden tot een overvloed aan valse positieven aangezien dit soort teksten door heel veel onschuldige burgers kunnen worden gebruikt.[99] Het trainen van A.I. met dit soort content zou een schoolvoorbeeld vormen van het verschijnsel "garbage in, garbage out". Het voorstel benadrukt dan ook dat bij het gebruik van deze technologieën menselijk toezicht en waar nodig menselijke tussenkomst vereist is, onder meer om valse positieven en valse negatieven te voorkomen.[100]

4.4. Databanken

In het voorafgaande is een enkele keer verwezen naar de databanken waarin indicatoren worden opgeslagen die kunnen worden gebruikt voor het classificeren en herkennen van CSAM-materiaal.
Het gaat tot de kerntaken van het EU-centrum behoren om deze databanken te creëren, te onderhouden en te beheren.[101] De indicatorenbanken zullen, volgens artikel 44 lid 2 van het voorstel, uitsluitend het volgende materiaal bevatten:

a. relevante indicatoren bestaande uit digitale identificatoren zoals hashes en AI beeld- en taal-*classifiers*,
b. een lijst van URL's die duiden op specifieke items van materiaal waarvan is vastgesteld dat het CSAM betreft en dat wordt gehost door partijen die geen diensten aanbieden in de Unie en

94. https://safer.io/.
95. NCMEC bezit bijvoorbeeld een databank van ongeveer 1,5 miljoen hashes. Ook het Nederlandse EOKM beschikt over een hash-database die bestaat uit 1,4 miljoen hashcodes van eerder gedetecteerd beeldmateriaal en afkomstig is van de Nationale Politie: Instant Image Identifier (voorheen bekend als Hashcheckserver): https://www.eokm.nl/lancering-baanbrekende-internationale-aanpak-van-online-seksueel-beeldmateriaal/
96. Impact Assessment Report bij het Voorstel, p. 279.
97. Impact Assessment Report bij het Voorstel, p. 310.
98. Impact Assessment Report bij het Voorstel, p. 282-283. Zie https://medium.com/themeetgroup/project-artemis-an-overview-9ce4174489db.
99. EOKM, *Standpunten van het EOKM over de Europese Verordening ter voorkoming en bestrijding van seksueel kindermisbruik*, 22 november 2022, zie www.eokm.nl.
100. Overweging 28 considerans Voorstel.
101. Artikel 44 Voorstel.

het materiaal weigeren te verwijderen of ontoegankelijk te maken,[102]

c. en noodzakelijke aanvullende informatie om het gebruik van de indicatoren te vergemakkelijken, zoals identificatoren voor afbeeldingen en video's en taalidentificatoren voor het opsporen van grooming.

Het idee is dat het EU-Centrum bij het voorbereiden en het "vullen" van de indicatorendatabanken onder meer nauw gaat samenwerken met Europol, daarbij voortbouwend op bestaande databanken. Nieuwe meldingen (van aanbieders, hotlines en het publiek) en afgerond onderzoek van opsporingsinstanties worden toegevoegd aan de centrale databanken bij het Centrum zodat ze zo actueel en relevant mogelijk blijven.[103]

4.5. E2EE en decryptie

De meest controversiële toe te passen technologie bij het opsporen van CSAM en grooming is de technologie die toegang moet geven tot (eind-tot-eind) versleutelde communicatie. Sommige van de relevante aanbieders (met name die van interpersoonlijke communicatiediensten) waarop dit voorstel betrekking heeft, bieden hun gebruikers immers de mogelijkheid om hun communicatie versleuteld te laten verlopen. Daarbij valt te denken aan berichtendiensten als Whatsapp, Signal en Telegram. Deze diensten gebruiken standaard of optioneel (Telegram) end-to-end-encryptie van berichten, zodat deze uitsluitend zichtbaar zijn voor de zender en de ontvanger. Willen deze aanbieders aan hun opsporingsverplichtingen kunnen voldoen dan zullen zij eerst en vooral op enigerlei wijze toegang moeten krijgen tot de communicatie die zij vervolgens moeten controleren op CSAM. In wezen houdt het opsporingsbevel, althans voor de aanbieders die versleutelde communicatiediensten aanbieden, daarmee tevens de facto een ontsleutelbevel in.

De voorgestelde Verordening zelf is niet scheutig in haar informatie over E2EE-communicatie en de technologieën die aanbieders, ter ontsleuteling ervan, zouden kunnen toepassen. De term wordt in het hele document maar één keer gebruikt, in Overweging 26 van de considerans bij het voorstel, en dan ook nog op tamelijk cryptische wijze.[104] De overweging luidt vrij vertaald: Het staat aanbieders vrij om eender welke technologieën te gebruiken voor het aanbieden van hun diensten en daartoe behoort zeker ook eind-tot-eindversleuteling, een belangrijk instrument om de veiligheid en vertrouwelijkheid van communicatie van gebruikers, waaronder die van kinderen, te waarborgen. Maar het gebruik van eind-tot-eindversleuteling ontslaat deze aanbieders niet van de verplichting om maatregelen te nemen ter uitvoering van aan hen gerichte opsporingsbevelen. De aanbieders zelf hebben de vrije keuze wat betreft de te gebruiken technologieën om op doeltreffende wijze aan opsporingsbevelen te voldoen.[105]

Gelukkig voorziet het Impact Assessment Report bij het voorstel in een uitgebreide en informatieve toelichting op dit onderwerp, waarin een tiental mogelijke manieren om toegang te verkrijgen tot E2EE-communicatie worden besproken. [106] Het voert te ver om de verschillende technieken hier te door te nemen – voor de liefhebber zijn de details terug te vinden in het rapport.[107] In het kort gaat het bijvoorbeeld over het zogenaamde *Client-side Scanning* (CSS) waarbij voordat de versleuteling van content plaatsvindt beeldmateriaal op het apparaat van de gebruiker wordt gescand, waarna het materiaal wordt gehasht en gematcht met hashes die op de server van de aanbieder staan (*on-device full hashing with matching on server*).[108] Maar ook *state of the art* en toekomstige mogelijkheden als decryptie in een *secure*

102. Artikel 44 lid 2 punt b, juncto lid 3 tweede alinea juncto artikel 36 lid 1 punt b.
103. Impact Assessment Report bij het Voorstel, p. 68.
104. In de EU-strategie voor een doeltreffendere bestrijding van seksueel misbruik van kinderen uit 2020 wond de Commissie er overigens volstrekt geen doekjes om: "De invoering van eind-tot-eindversleuteling is weliswaar bevorderlijk voor de privacy en de beveiliging van communicatie, maar vergemakkelijkt voor daders ook de toegang tot beveiligde kanalen, met behulp waarvan zij hun praktijken, zoals de handel in afbeeldingen en video's, voor de rechtshandhavingsautoriteiten kunnen verbergen. Het gebruik van encryptietechnologie voor criminele doeleinden moet daarom onmiddellijk worden aangepakt door middel van eventuele oplossingen aan de hand waarvan bedrijven seksueel misbruik van kinderen in eind-tot-eind versleutelde elektronische communicatie zouden kunnen opsporen en melden. Elke oplossing moet zowel de privacy van elektronische communicatie en de bescherming van kinderen tegen seksueel misbruik en seksuele uitbuiting waarborgen, alsook de bescherming van de privacy van de kinderen die in het materiaal betreffende seksueel misbruik zijn afgebeeld". Zie EU strategie COM 2020(607) 24 juli 2020, p. 2.
105. Overweging 26 considerans Voorstel.
106. Bijlage 9 van het Impact Assessment Report bij het Voorstel. In het rapport luidt de centrale vraag: "Zijn er, gegeven het vóórkomen van E2EE elektronische communicatie, technische oplossingen waarmee CSA-content kan worden opgespoord terwijl dezelfde of vergelijkbare voordelen van encryptie (zoals privacy) behouden blijven?"
107. Impact Assessment Report bij het Voorstel: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX.
108. https://www.internetsociety.org/resources/doc/2020/fact-sheet-client-side-scanning/. En: https://www.eff.org/deeplinks/2019/11/why-adding-client-side-scanning-breaks-end-end-encryption.

enclave in de ESP server en *on-device homomorphic encryption*.[109]

Van belang is nog te vermelden dat de Nederlandse regering tot nu toe een terughoudend standpunt heeft ingenomen ten aanzien van het detectiebevel en het daarbij doorbreken van encryptie. De regering verwijst daarbij naar het kabinetsstandpunt omtrent encryptie uit 2016 dat het "op dit moment niet wenselijk is om beperkende wettelijke maatregelen te nemen ten aanzien van de ontwikkeling, de beschikbaarheid en het gebruik van encryptie binnen Nederland. In de internationale context zal Nederland deze conclusie en de afwegingen die daaraan ten grondslag liggen uitdragen".[110] In een recente Kamerbrief bevestigt de minister dat het kabinet de (Europese) voorstellen die end-to end encryptie onmogelijk maken niet zal steunen. Wel stelt de minister dat de "maatregelen genoemd in de verordening [wél] kunnen worden uitgevoerd met behulp van technische middelen die end-to-end encryptie niet aantasten". Zij doelt hier met name op technische oplossingen die zien op *on device scanning*.[111] Een dergelijke oplossing laat inderdaad formeel de versleuteling ongemoeid maar doet uiteindelijk wel afbreuk aan de vertrouwelijkheid van versleutelde communicatie.[112]

5. Conclusie en enkele discussiepunten

De hier besproken voorgestelde Verordening is complex, veelomvattend en ingrijpend, en alle aspecten en gevolgen ervan kunnen niet in het bestek van één bijdrage worden behandeld. Wel is duidelijk dat een wetgevingsinstrument dat ziet op de rechten van het kind en de bescherming van kinderen tegen seksueel misbruik op het internet, de afgelopen tijd het onderwerp is geworden van een verhit debat over de vrijheid van meningsuiting, vertrouwelijke communicatie, privacy, security en een veilig internet voor iedereen. De flexibele omgang met het cijfermateriaal dat een belangrijke rol speelt bij de onderbouwing van de noodzaak van het voorstel lijkt die discussie, zoals we hiervoor zagen, soms wat te vertroebelen. Terwijl de Europese Commissie tamelijk luidruchtig campagne voert voor het voorstel op basis van in wezen onbetrouwbare data[113], toonde de TU Delft aan dat deze cijfers geen directe of acute aanleiding geven voor het invoeren van een dergelijk vergaand voorstel. Immers, de hoeveelheid (unieke) CSAM-bestanden die door aanbieders werd onderschept is al vier jaar op rij niet significant gegroeid.

Maar er zijn nog meer heikele punten. Zo draagt het voorstel het risico in zich van *overblocking* en valse positieven. Het is bijvoorbeeld heel goed voorstelbaar dat bepaalde content - van de categorie foto van een badderend kind, moeder met kind aan de borst - in de nabije toekomst (ten onrechte) als CSAM zal worden geclassificeerd en vervolgens wordt geblokt.[114] Het voorstel laat evenmin ruimte voor het onderscheid tussen de verspreiding van CSAM en het door jongeren onderling delen van seksueel beeldmateriaal met wederzijdse toestemming (het zogenaamde *sexting*). Sommige auteurs wijzen op het schadelijke en mogelijk *chilling effect* van het voorstel op de seksuele ontwikkeling van deze tieners.[115]

Ook bestaat bij sommigen de vrees van "repurposing", de mogelijkheid om bestaande opsporingstechnologieën in te zetten voor andere doeleinden, zodra deze eenmaal zijn ingeburgerd. Zo zouden bestaande taalidentificatie-technologieën en -databanken in een later stadium vrij eenvoudig kunnen worden omgevormd en uitgebreid om andere content te detecteren, zoals bepaalde categorieën van desinformatie of onwenselijk geachte politieke communicatie. Hetzelfde geldt voor het "ontsleutelingsbevel": eenmaal toegang tot E2EE communicatie geeft dat ineens de ruimte voor allerlei andere onderzoeks- en opsporingsmogelijkheden.

Problematisch is ook het deel van het voorstel dat ziet op de opsporing van online grooming. We zagen al hoe lastig het zal zijn om de technologische, talige maatstaven aan te leggen die grooming-communicatie van andere, dagelijkse communicatie moet onderscheiden (in de categorie "Is je moeder thuis?").

109. Impact Assessment Report bij het Voorstel, p. 290-306.
110. Zie BNC-fiche bij het Voorstel, 17 juni 2022: https://www.rijksoverheid.nl/documenten/publicaties/2022/05/11/fiche-2-verordening-voorkoming-bestrijding-seksueel-kindermisbruik, en Kamerstukken II 2015/2016, 26643, nr. 383.
111. *Kamerstukken II*, 2022/2023, 26643, nr. 968, p. 11.
112. Zie https://www.bitsoffreedom.nl/2023/02/01/kabinet-speelt-woordspelletje-met-tweede-kamer/.
113. Zie https://home-affairs.ec.europa.eu/whats-new/campaigns/legislation-prevent-and-combat-child-sexual-abuse_nl: "Op 3 augustus 2024 verloopt de EU-wetgeving die dienstverleners toestaat om online seksueel misbruik van kinderen en de verwijdering van materiaal betreffende seksueel misbruik van kinderen vrijwillig op te sporen en te melden. Dit zal het voor daders gemakkelijker maken om ongestraft kinderen seksueel te misbruiken. Als de nieuwe wet van kracht is, zullen technologiebedrijven verplicht zijn kinderen te beschermen. **Laten we ervoor zorgen dat dit vóór 3 augustus 2024 gebeurt.**"
114. Zie ook de gezamenlijke opinie van BoF en EOKM: https://www.trouw.nl/opinie/vader-post-foto-van-badderend-kind-is-dat-straks-verdacht~baadb567/.
115. Zie hier https://www.coe.int/en/web/children/-/launch-of-an-interdisciplinary-outcomes-report-on-the-potential-implications-of-the-eu-s-proposal-for-a-regulation-to-prevent-and-combat-child-sexual-abuse voor een link naar een expert workshop rapport van de hand van S.K. Witting en M.R. Leiser. Zie ook S.K. Witting 'Regulating bodies: the moral panic of child sexuality in the digital era' *KritV* 1/2019, DOI: 10.5771/2193-7869-2019-1-5.

Het is voorstelbaar dat nationale opsporingsautoriteiten niet meteen zitten te springen om grote hoeveelheden vals positieve meldingen van online grooming. Daar komt bij dat op korte termijn in Nederland ook *online sexchatting* met kinderen strafbaar wordt.[116] Betekent dit dat aanbieders vanaf dan op alle verdachte seksuele communicatie met minderjarigen moeten gaan scannen? Is er overigens in het voorstel rekening gehouden met het feit dat er in de Europese Unie 24 verschillende talen worden gesproken, en gaat de databank van het EU-centrum grooming-identificatoren in al die talen verzamelen? Veel vragen waarop op dit moment nog geen antwoorden zijn.

Overigens benadrukte onze eigen minister onlangs dat in Nederland het detecteren van grooming exclusief is belegd bij opsporingsinstanties en dat men dit zo wil houden.[117] In de onderhandelingen zal de Nederlandse regering dit standpunt actief uitdragen. Er wordt in bepaalde welingelichte kringen rekening gehouden met de mogelijkheid dat in een later stadium van onderhandelingen over dit voorstel wordt teruggevallen op beleidsoptie D (waarin geen opsporingsverplichting geldt ten aanzien van online grooming).

Tot slot moet worden opgemerkt dat op dit moment de kosten voor het EU-centrum alleen al worden geraamd op 25 miljoen euro op jaarbasis.[118] Deze middelen zouden wellicht beter worden geïnvesteerd in projecten rond dader- en slachtofferpreventie en voorlichting aan kinderen, ouders en scholen. Op die manier worden de verspreiding van CSAM en online grooming - in mijn ogen - veiliger, effectiever en bij de wortel aangepakt.[119]

116. Door de introductie van de nieuwe strafbepaling - artikel 251 Sr - in het Wetsvoorstel seksuele misdrijven, zie ook: A.E. de Hingh, 'Het wetsvoorstel seksuele misdrijven. Over online én offline sexchatten en het opsporen van het online seksueel benaderen van kinderen', *Computerrecht* 2023/3.
117. *Kamerstukken II*, 2022/2023, 26643, nr. 968.
118. Impact Assessment rapport Voorstel, p. 364.
119. Zie bijvoorbeeld het in maart 2023 door het EOKM opgestarte dader-preventieprogramma: het Protech-project, https://www.eokm.nl/nieuws/ dat 2 miljoen euro zou kosten.