Child Sexual Abuse ACT – Q&A

EU-verordening betreffende voorschriften ter voorkoming en bestrijding van seksueel kindermisbruik

HOOFDVRAGEN/-BOODSCHAPPEN

1. ***Wat is de CSA (Child Sexual Abuse Act)?***

In mei 2022 heeft de Europese Commissie een wetsvoorstel neergelegd om online seksueel misbruik van kinderen te voorkomen en te bestrijden. Digitale dienstverleners zoals Meta en Google moeten hun verantwoordelijkheid nemen voor wat er zich op hun platforms voordoet om ze zo veiliger te maken voor kinderen. Ze moeten maatregelen nemen opdat seksuele misbruikbeelden op hun platforms worden opgespoord en verwijderd. Dit is een noodzakelijk wapen in de strijd tegen online seksuele uitbuiting.

2. ***Op welk niveau moet dit gestemd worden, door wie en wanneer?***

Begin oktober 2023 volgt een stemming in de commissie van het Europees Parlement en maakt de Europese Raad haar positie kenbaar. Een gunstige positie is een noodzakelijke stap voor het verdere verloop van het wetgevend proces, bestaande uit onderhandelingen tussen de drie Europese instellingen. Daarna is het zaaks om de wet te stemmen voor het verstrijken van de Interim Verordening op 3 augustus 2024.

Deze Interim Verordening kwam in allerijl, als tijdelijke afwijking op de E-privacy wetgeving, opdat bepaalde dienstverleners toch nog op hun eigen platformen beelden van seksueel misbruik kunnen blijven screenen zoals dat doorgaans in de Verenigde Staten mogelijk is.

Het voorstel betreft een verordening, waardoor de regels rechtstreeks van toepassing zijn in alle EU-lidstaten.

3. ***Wat vindt Child Focus van dit voorstel? Waarom is dit zo belangrijk?***

Child Focus ziet een kans in dit voorstel om kinderen beter te beschermen online. Jaar na jaar zien we het aantal dossiers van seksuele uitbuiting stijgen. Achter elk dossier schuilt een kind dat getekend is voor het leven. Onze organisatie vraagt al jaren een Europees kader die de digitale spelers meer verantwoordelijkheid oplegt. We moeten gebruikmaken van de technologische mogelijkheden om kinderen te helpen en te beschermen. We zijn ervan overtuigd dat seksueel misbruik van kinderen online fors zal dalen dankzij deze wetgeving.

Daarbovenop zullen kinderen hun verschillende rechten effectief kunnen uitoefenen: hun recht op privacy, hun recht op bescherming tegen online seksuele uitbuiting en hun recht op informatie.

4. ***Seksuele misbruikbeelden, hoe worden wij hier in België mee geconfronteerd?***

Child Focus heeft een burgerlijk meldpunt www.misbruikbeelden.be waar iedereen (anoniem) vermoedelijke seksuele misbruikbeelden van kinderen kan melden. Een tiental werknemers van Child Focus analyseert deze gemelde beelden. In 2022 ontving Child Focus 1.832 meldingen. België ontvangt eveneens meldingen uit het buitenland die betrekking hebben op Belgische slachtoffers en daders. In 2022 stuurde onze moederorganisatie NCMEC 50.299 meldingen naar Europol met een link naar België (een toename van 319% t.o.v. 2021). Maar niet alle meldingen konden effectief onderzocht worden door een gebrek aan informatie, vandaar het belang van een Europese aanpak.

ALGEMEEN

1. <u>Waarom is het belangrijk om dit op Europees niveau aan te pakken?</u>

De digitale wereld kent geen grenzen. Als slachtoffer heb je weinig controle op je beelden of weinig zekerheden over je rechten, want je bent afhankelijk van het land van de dienst of het platform. Volgens de Internet Watch Foundation, gebaseerd in het Verenigd Koninkrijk, had 66% van al het misbruikmateriaal in 2022 oorsprong in de Europese Unie. Deze wetgeving geeft slachtoffers in de EU een gelijke bescherming, want alle bedrijven die diensten leveren in de EU moeten dezelfde regels handhaven.

2. <u>Hoe beschermt het kinderen online?</u>

Het voorstel heeft 3 hoekstenen, die samen het probleem bij de wortel aanpakken:
Effectieve preventie → Meldplicht & detectie → Centralisering

- **Preventie**: Digitale dienstverleners moeten gerichte maatregelen nemen om zo online seksueel misbruik te voorkomen.
- **Meldplicht en detectieplicht**: Alle gevallen van online seksueel misbruik moeten gemeld worden aan het Europees expertisecentrum. Een detectiebevel zal volgen als de dienstverlener geen of onvoldoende maatregelen neemt. Een detectiebevel verplicht de dienstverlener om scantechnologie in te zetten om het misbruik op te sporen. Deze bevelen zijn slechts in laatste orde aan zet.
- **Centraal gecoördineerd Europees expertisecentrum:** ontvangt alle meldingen en bezorgt de meldingen aan de politie voor verder onderzoek. Het centrum kan ook het slachtoffer bijstaan om de beelden op te sporen.

3. <u>Waarom is het belangrijk om dit voorstel in haar geheel (lees ruimte toepassing) te stemmen?</u>

Het voorstel is gericht op alle types diensten, waaronder de publieke en versleutelde chatdiensten. Het is essentieel om alle diensten aan hetzelfde regime te onderwerpen, zodat we de verplaatsing van het probleem kunnen voorkomen. Child Focus stelt immers nu al vast dat seksuele uitbuiting online van openbare platforms naar besloten groepen en versleutelde chats wordt verplaatst. De daders weten waar hun misbruik te plegen. Door een ruimte toepassing te voorzien, geven we een duidelijk signaal aan daders: ga niet op zoek naar achterpoortjes.

Vergelijk de rapporten van het sociale netwerk Facebook, dat automatische detectietechnologie gebruikt, en bijvoorbeeld Instagram, dat vertrouwt op meldingen. De cijfers liegen er niet om: Facebook deed bij NCMEC vorig jaar 21.165.208 meldingen van misbruikbeelden versus Instagram 5.007.902 of WhatsApp 1.017.555. Gezien de populariteit van deze verschillende platforms zouden de cijfers anders verdeeld moeten zijn.

4. <u>Hoe staan andere landen hier tegenover?</u>

Child Focus maakt zich ernstig zorgen over het gebrek aan steun voor het wetsvoorstel vanuit een aantal landen, inclusief vanuit de Belgische overheid. Het debat lijkt te verengen naar een technologische discussie rond encryptie en privacy, zonder nog oog te hebben voor de belangen van het kind. Uiteraard is Child Focus begaan met onze privacy. Maar het wetsvoorstel heeft een goed evenwicht gevonden tussen bescherming van kinderen en privacy. Volgens een recente enquête van de Eurobarometer staat trouwens 73% van de Belgische bevolking achter dit voorstel.

5. <u>Waarom is er een bepaalde tegenwind?</u>

Zoals bij elk voorstel zijn er voor –en tegenstanders. In dit dossier komt de tegenwind uit de commerciële en de privacyhoek. De digitale giganten zullen concrete maatregelen moeten nemen die

gepaard gaan met financiële uitgaven. Er is ook tegenwind uit de privacyhoek die sinds de E-privacy richtlijn de toon zet binnen de EU. Zij vinden dat het huidige voorstel door de mogelijkheid van detectie op versleutelde berichten de privacy kan schenden. Child Focus vindt dat de bescherming van kinderen een absolute prioriteit moet worden. Achter elk beeld van seksueel kindermisbruik schuilt een kind dat slachtoffer is en dat ook recht heeft op privacy.

ANDERE REGELGEVING

1. Wat bestaat er in Europa al op vlak van wetgeving?

De Europese Unie heeft de laatste jaren de pen niet neergelegd:

- De Europese Commissie maakt van de strijd tegen seksueel misbruik van kinderen een prioriteit. Op 24 juli 2020 verscheen de EU-strategie voor een efficiëntere bestrijding van seksueel misbruik van kinderen met o.a. een herziening van de Directieve 2011/93/EG (richtlijn seksueel misbruik van kinderen) van 2011 tot doel.
- Interim Verordening van 14 juli 2021 (2021/1232/EU) betreffende een tijdelijke afwijking van sommige bepalingen van Richtlijn 2002/58/EG met betrekking tot het gebruik van technologieën door aanbieders van nummeronafhankelijke interpersoonlijke communicatiediensten voor de verwerking van persoonsgegevens en andere gegevens ter bestrijding van seksueel misbruik van kinderen online.
- Op 5 juli 2022 trad de Digital Services Act in werking met een breed kader om de digitale markt te reguleren. Daarin staan regels vervat die raken aan de online veiligheid van kinderen, zoals maatregelen ter bestrijding van illegale content.
- De Europese strategie voor een beter internet voor kinderen (BIK+) verscheen op 11 mei 2022 en streeft naar veilige digitale ervaringen en digitale zelfredzaamheid voor kinderen.

Het voorliggende voorstel vloeit voert uit de EU-strategie van 2020. In vergelijking met andere wetgevende stukken legt het een operationeel kader op met verstrekkende verplichtingen voor de digitale dienstverleners.

2. Wat gebeurt er als de verordening niet gestemd wordt?

Als de verordening niet wordt gestemd, zal het niet langer mogelijk zijn om online seksueel misbruik te detecteren in chats. De impact daarvan hebben we eind 2020 al ondervonden. Toen zag onze moederorganisatie NCMEC, de Amerikaanse Cybertipline, een scherpe daling van 58% van meldingen van online seksuele uitbuiting. En dit lag niet aan minder gevallen, maar wel aan een knik in de kabel. META, het bedrijf met het grootst aantal meldingen, detecteerde niet langer meldingen van seksueel misbruik gelinkt aan Europese gebruikers, omdat ze geen wettelijk mandaat hadden.

3. Hoe verhoudt deze Europese verordening zich tot wat vandaag in de Verenigde Staten gebeurt?

Het voorstel haalt heel wat inspiratie bij de Amerikaanse Cybertipline NCMEC, waar online bedrijven verplicht seksuele misbruikbeelden moeten melden. NCMEC verzamelt alle rapporten en bezorgt ze aan Europol. Het gaat ook een stap verder: naast meldplicht aan een Europees expertisecentrum, is er ook detectieplicht voor digitale spelers die hun verantwoordelijkheid verzuimen. Het Europees expertisecentrum gaat hiervoor *state-of-the-art* scantechnologie identificeren.

4. Waarom is de Digital Services Act als wetgevend kader onvoldoende in de strijd tegen online seksuele uitbuiting?

Op 5 juli 2022 trad de Digital Services Act (DSA) in werking met een breed kader om de digitale markt te reguleren. Daarin staan regels vervat die raken aan de online veiligheid van kinderen. De DSA legt

de basis voor verantwoordelijkheid van de digitale dienstverleners, wat al een belangrijke stap is in de juiste richting. Als de dienstverleners geen maatregelen nemen om illegale inhoud van hun servers weg te halen, dan zijn zij niet langer vrijgesteld van aansprakelijkheid.

Eén van de maatregelen is duidelijke en kindvriendelijke rapporteringsmechanismen voorzien. Dit is ongetwijfeld belangrijk voor jongeren wiens intieme beelden onder valse voorwendselen of buiten hun wil verspreid worden. Het probleem is dat slachtoffers van seksueel kindermisbruik voor meer dan 90% bestaan uit pre-puberale kinderen. In de databank van Interpol tonen 40% van de 7 miljoen bestanden seksueel misbruik met een baby – peuter. Als we deze groep willen redden en beschermen, moeten we scantechnologie inzetten.

5. ***Waarom niet gewoon een voortzetting van de Interim Verordening, die vrijwillige detectie mogelijk maakt, zoals sommige bedrijven en experten vragen?***

Het doel van de Interim Verordening was nooit om een structurele wet te worden, vandaar de tijdelijkheid. Deze is beperkt tot een aantal dienstverleners van interpersoonlijke communicatie, waardoor nieuwe spelers uit de boot vallen. Bovenal volstaat vrijwillige detectie niet om het probleem van online seksueel misbruik effectief aan te pakken. Ten eerste is de overgrote meerderheid van meldingen afkomstig van een handvol van dienstverleners, terwijl er duidelijke aanwijzingen zijn dat het probleem zich niet alleen op één platform voordoet: 95% van de meldingen in de VS is afkomstig van META. Ten tweede vallen versleutelde berichten buiten het toepassingsgebied met een grote onderrapportering tot gevolg. De cijfers zijn alleszeggend – Facebook 21 165 208 versus WhatsApp 1 017 555.

SCANTECHNOLOGIE & PRIVACY

1. ***Hoe werkt de scantechnologie die gebruikt zou worden?***

Vandaag bestaan er al verschillende types van technologie op de markt die seksuele misbruikbeelden kunnen opsporen. Het is mogelijk om deze methoden te combineren.

- De meest gangbare zijn *file hashing* (*vb.* SHA-1) en *perceptual hashing (vb. fotoDNA)*, gebruikt voor de detectie van **gekende beelden van seksueel misbruik** (sinds +/- 15 jaar). Een *hash* is een digitale vingerafdruk van een beeld. De scantechniek is geautomatiseerd en vergelijkt beelden online met gekende beelden van seksueel misbruik op basis van een cijfermatige berekening. De technologie is niet in staat om beelden te herkennen of te analyseren. Deze technologieën worden breed toegepast. Ook Child Focus werkt met dit type van technologie in Arachnid, het project van het Canadees Centrum voor de bescherming van kinderen. Arachnid heeft al 160 miljard beelden gescreend.
- Een relatieve nieuwkomer op de markt is artificiële intelligentie (sinds +/- 5 jaar). *AI classifiers* combineren verschillende technieken om **nieuwe beelden van seksueel misbruik** op te sporen. Deze scantechniek is geautomatiseerd en kan geen beelden erkennen of analyseren. Het werkt volgens het principe van een boomstructuur: ja/nee. De betrouwbaarheid van de technologie kan je zelf bepalen. Hoe nauwkeuriger, hoe lager de detectie van seksuele misbruikbeelden. Een 99,9% betrouwbaarheid, genereert nog steeds 84% detectie. Door de hoge betrouwbaarheid is de kans op vals positieven (een legitiem beeld dat onterecht wordt gedetecteerd) en vals negatieven (een illegaal beeld wordt niet gedetecteerd) lager.
- Het zusje van de AI classifier is de *Tekst classifier*, die patronen van **grooming** opspoort op basis van 9 categorieën.

2. ***Waarom is scantechnologie nodig?***

De omvang van online seksueel misbruik neemt duizelingwekkende proporties aan. Het internet is besmeurd met miljarden beelden van gekende slachtoffers. En daar komen elke dag duizenden nieuwe beelden bij. Neem het voorbeeld van een 10-jarig Belgisch meisje, misbruikt door haar papa. Haar beelden werden al in 190 000 bestanden van 12 900 criminelen teruggevonden. Politie,

hulporganisaties, slachtoffers en burgers werken de klok rond het internet te kuisen en slachtoffers te beschermen. Het is dweilen met de kraan open, want alle handen samen houdt het stromend water niet tegen. We hebben scantechnologie nodig om te voorkomen dat reeds gekende beelden opnieuw circuleren, gekende en nieuwe beelden te detecteren en onderscheid te maken tussen beelden met een gekend en niet gekend slachtoffer.

3. ***Wanneer kan scantechnologie ingezet worden?***

Scantechnologie kan in verschillende fases worden ingezet:

- De fase van *upload*: voorkomen dat seksuele misbruikbeelden op het internet circuleren.
- De fase van verspreiding: op zoek gaan naar beelden op het internet.
- Op de telefoon (*scanning-on-device*): beelden detecteren voor de versleuteling.

4. ***Worden alle foto's gescand?***

We kunnen scantechnologie het best vergelijken met een flitspaal. Alle auto's komen in aanmerking, maar enkel de bestuurders die boven de toegelaten snelheid rijden, worden geflitst.

5. ***Worden ook andere intieme beelden, bijvoorbeeld van volwassenen, door deze scantechnologie tegengehouden?***

Geen enkele technologie is perfect. Er bestaat altijd een kans dat een beeld onterecht wordt weerhouden of dat een illegaal beeld niet wordt weerhouden. De kans dat dit effectief gebeurt, kan tot een minimum worden gebracht, door de betrouwbaarheid te verhogen. De technologie is niet in staat om het beeld te zien zoals jij en ik het zien. Als een beeld toch onterecht weerhouden wordt, dan zal het na controle opnieuw vrijgegeven worden. Het is een klein ongemak voor een grote maatschappelijke winst.

6. ***Gaat deze technologie alles screenen op een toestel (client side scanning)?***

CSS of *client side scanning* is een applicatie waarbij geautomatiseerde technologie wordt ingebouwd in het toestel, waardoor het mogelijk is om beelden van seksueel misbruik nog voor versleuteling op te sporen. De technologie is geautomatiseerd en gaat enkel beelden weerhouden die matchen met seksuele misbruikbeelden.

7. ***Is deze technologie veilig?***

De scantechnologie is afdoende veilig en betrouwbaar voor de detectie van gekende, nieuwe beelden van seksueel kindermisbruik en voor patronen van grooming. Meer dan bij andere types van materiaal, denk aan *malware* en *spam*, zijn heel wat controlemechanismes voorzien omdat seksuele misbruikbeelden zeer gevoelige informatie bevatten. Elke technologie houdt een risico in, maar door een degelijk beleid te ontwikkelen, beperken we de risico's.

8. ***Hoe draagt dit kader bij tot veiligheid?***

In tegenstelling tot vandaag waar de digitale bedrijven zelf op vrijwillige basis scantechnologie inzetten, voorziet de verordening momenteel in een sterk omkaderd gebruik. De beslissing komt toe aan een gerechtelijke autoriteit wanneer er bewijs is van een "aanzienlijk risico dat de dienst wordt gebruikt voor online seksueel misbruik van kinderen", bijvoorbeeld als er veel rapporteringen zijn van gebruikers. Meer dan tevoren zal er controle zijn op de inzet van scantechnologie. De zogenaamde detectiebevelen komen tot stand in samenwerking met de Gegevensbeschermingsautoriteit en het EU Centrum, zijn gelimiteerd in de tijd, technologie-neutraal en doelgericht. De verordening draagt juist veel meer bij aan een veilig gebruik van de technologie. Het EU centrum waakt over de technologieën en kan via een technisch comité de technologieën laten testen voor gebruik.

9. Wordt de privacy van gebruikers op deze manier aangetast?

De bepalingen van het voorstel zijn een uitkomst van een evenwichtsoefening tussen het belang van privacy en van de bescherming van kinderen. Deze voorzien tal van waarborgen wezenlijk voor de bescherming van privacy. Vandaag bestaan er al technologieën, die de privacy niet zwaarder aantasten dan een gewone virusbeschermer of spamfilter.

10. Is scantechnologie combineerbaar met encryptie?

Er zijn drie theoretische mogelijkheden om te scannen in E2EE (*End-to-End Encryption*) elk met zijn voordelen en nadelen. De meest neutrale, is de *client side scanning*. Deze mogelijkheid verandert niets aan de cyberveiligheid van versleutelde omgevingen. Het is detectie die voor of na encryptie wordt gebruikt. CSS wordt op dezelfde manier gebruikt voor *spam* en *malware*.

Vandaag bestaan er al beproefde technieken, die dankzij voorliggend kader verder getest en gebruikt kunnen worden. Het is ook een stimulans om de technieken van morgen te ontwikkelen en nieuwe tendensen voor te blijven.

11. Is het momenteel technisch haalbaar om betrouwbare scans uit te voeren?

Het gaat over beproefde technologie, die getest is en al succesvol wordt ingezet. Voor de uitrol op grote schaal/ de vermarkting moeten de laatste belemmeringen weggewerkt worden. Hoe meer de technologie wordt gebruikt, hoe beter ze werkt en hoe dichter ze de perfectie bereikt.

BETROKKEN PARTIJEN

1. Welke partijen zijn hiermee betrokken?

- Elektronische dienstverleners uit de EU en derde landen met dienstverlening in de EU:
    - Risicoanalyse drie maanden na inwerkingtreding en, risico beperkende maatregelen.
    - Meldplicht aan het EU centrum.
    - Verwijderingsbevelen wanneer seksuele misbruikbeelden niet tijdig offline worden gehaald.
    - Detectiebevelen wanneer het bedrijf geen of onvoldoende maatregelen neemt.
    - Centraal aanspreekpunt in EU, ook voor bedrijven uit derde landen met diensten in EU.
- Coördinerende autoriteiten op niveau van elke lidstaat:
    - Onderzoeksbevoegdheden.
    - Slachtoffers bijstaan om seksuele misbruikbeelden op te sporen.
    - Handhavingsbevoegdheden.
    - Samenwerking met coördinerende autoriteiten van andere lidstaten.
- EU expertisecentrum:
    - Databank indicatoren online seksuele uitbuiting (o.a. lijsten van *hashes* van gekende beelden van seksueel misbruik).
    - Behandelen meldingen van de elektronische dienstverleners.
    - Expertise cel.
    - Proactief zoeken naar seksuele misbruikbeelden van slachtoffers.

2. Wat is de rol van sociale media?

Sociale mediabedrijven moeten een grondige risicoanalyse uitvoeren op hun diensten, een veiligheidsbeleid uitwerken en andere maatregelen nemen om online seksueel misbruik te voorkomen. Wanneer zij dit nalaten of de maatregelen niet afdoend werken, dan kunnen zij met

behulp van een detectiebevel het probleem aanpakken. Na detectie kunnen zij nieuwe maatregelen nemen om het risico te beperken.

3. Wat is de rol van de politie?

De politie is melder en ontvanger van meldingen. De politie en andere expertise organisaties zullen gevallen van online seksueel misbruik melden aan de elektronische dienstverleners. De politie als bevoegde autoriteit zal meldingen van het EU centrum ontvangen, analyseren voor dader- en slachtofferidentificatie. Nieuwe beelden kunnen na bekrachtiging van de bevoegde autoriteiten opgenomen worden in de indicatorenlijst van het EU centrum, waardoor de scantechnologie de verspreiding van nieuwe beelden kan opsporen.

4. Gaat de politie niet overbelast worden met foutieve meldingen?

Het EU centrum gaat alle meldingen filteren en vervolgens dispatchen naar de bevoegde politie. Door het centraal beheer vermijden we dubbel werk. Europol zal ook zicht houden over de dossiers waar meerdere politiezones in betrokken zijn.