Aan Dhr. D.M. van Weel, minister van Justitie en Veiligheid

CC: de woordvoerders van de Commissie Justitie en Veiligheid in de Tweede Kamer

Betreft: EU Verordening ter voorkoming en bestrijding van seksueel misbruik van kinderen

30 september 2024, Leiden

Geachte Minister van Weel,

Namens twaalf organisaties willen wij met klem benadrukken dat Nederland zich tijdens de JBZ-raad op 10-11 oktober positief moet uitspreken over de EU-verordening ter bescherming en voorkoming van kindermisbruik online. Het is hoog tijd om een lans te breken vóór deze verordening. De bescherming van kinderen heeft de afgelopen maanden te weinig aandacht gekregen. Het negatieve frame rond deze verordening is hardnekkig, onze mening is: privacy en bescherming hoeven elkaar niet uit te sluiten, en kinderen hebben recht op beide.

Wanneer de wetgever vooral gehoor geeft aan privacybelangen, kunnen online diensten routinematig worden gebruikt om seksueel misbruik van kinderen te verbergen en worden miljoenen kinderen onvoldoende beschermd. De overheid heeft de taak om dit te voorkomen. In deze brief onderstrepen we het doel en de noodzaak van de verordening en laten we oplossingen zien die recht doen aan ieders belang.

De verordening past in een grotere Europese aanpak

Wij horen verschillende partijen zeggen dat er moet worden geïnvesteerd in preventie, in plaats van in de verordening voor online dienstverleners. Echter, het voorstel voor de verordening is slechts één element in de EU strategie voor een effectievere strijd tegen seksueel kindermisbruik dat de Europese Commissie in 2020 heeft vastgesteld. De strategie behelst een holistische aanpak, waarvan preventie één van de pijlers is (naast wetgeving, rechtshandhaving, samenwerking, EU centrum en rol van de sector). Bovendien heeft de verordening juist een sterke preventieve insteek door álle online dienstverleners te verplichten risico's voor online seksueel misbruik en uitbuiting van kinderen in kaart te brengen en maatregelen voor te stellen om deze te beperken. Dit heeft een substantiële invloed op het verminderen van deze ernstige vorm van criminaliteit. Dat is nodig, want de schaal waarop kinderen te maken hebben met online seksueel misbruik en uitbuiting is enorm groot en stijgt ieder jaar. Wereldwijd is 1 op de 8 kinderen slachtoffer van zonder toestemming maken, delen of vertonen van seksueel getinte afbeeldingen en video's.[1] In Nederland heeft maar liefst 68% van de 18-jarigen als kind ongewenst online seksueel gedrag ervaren.[2]

Detectie redt kinderen

De mogelijkheid om kindermisbruik te detecteren door online dienstverleners is een essentieel en betwist onderdeel van de verordening. Detectie is echter een onmisbaar onderdeel in de strijd tegen online seksueel kindermisbruik. In maart van dit jaar meldde Facebook bij NCMEC[3] dat via Facebook Messenger een filmpje van seksueel misbruik van een jong meisje was gedeeld. Ook Google meldde dat een filmpje van het meisje op YouTube was geüpload. Kort daarna is het meisje in veiligheid gebracht en zijn twee verdachten (waaronder de vader van het meisje) aangehouden door de politie. Zonder wetgeving die het mogelijk maakt dat online dienstverleners hun eigen platformen kunnen

[1] https://www.childlight.org/

[2] https://www.weprotect.org/economist-impact-european-survey/

[3] National Centre for Missing and Exploited Children waar bedrijven in VS verplicht zijn online kindermisbruik te melden

scannen om te voorkomen dat deze worden misbruikt voor het delen of vervaardigen van kindermisbruik, kan dit bijna straffeloos plaatsvinden. META, het moederbedrijf van Facebook, heeft besloten Facebook Messenger volledig te versleutelen, waardoor beeldmateriaal van seksueel kindermisbruik niet kan worden gedetecteerd. Het misbruik kan dan nog jarenlang voortduren.

Detectie met behoud van briefgeheim – het kan wel

In het Nederlandse parlement zijn moties met betrekking tot deze verordening aangenomen. De motie van het lid Van Ginneken (D66) stelt dat de verordening niet moet worden gesteund als deze "chat-control" toestaat, zoals client-side scanning. Het is belangrijk op te merken dat end-to-end versleutelde (E2EE) diensten zoals berichtendiensten of e-maildiensten client-side scanning gebruiken om malware en spam te detecteren en link previews te genereren, zonder de versleuteling te compromitteren. Dit scannen op inhoud gebeurt lokaal op het apparaat van de gebruiker, waarbij de inhoud van het bericht alleen zichtbaar blijft voor de zender en de ontvanger. In E2EE omgevingen zijn wel degelijk mogelijkheden te bedenken om kindermisbruik tegen te gaan, zonder de vertrouwelijkheid van de communicatie in gevaar te brengen. Zo kan er worden gescand op bekend misbruikmateriaal om te voorkomen dat het (opnieuw) wordt gedeeld, zonder dit te melden. Bovendien kan geïnvesteerd worden in waarschuwingssystemen die mensen bewust maken van risico's en mogelijkheden bieden om misbruikmateriaal te blokkeren, melden en hulp te zoeken, bijvoorbeeld bij de Kindertelefoon en hulplijnen als Stop it Now. Door het volledig uitsluiten van client-side scanning voor kindermisbruik worden al deze (toekomstige) mogelijkheden uitgesloten, zelfs wanneer deze geen inbreuk maken op de vertrouwelijkheid van onze interpersoonlijke online communicatie. Wij vinden het daarom goed dat het Hongaarse voorzitterschap in het voorstel aan de Raad van de Europese Unie end-to-end-encryptie niet uitsluit, maar extra waarborgen inbouwt.

Detecteren van nieuw materiaal – maatregelen om privacy te beschermen

Er bestaan zorgen over het relatief hoog percentage vals-positieve uitkomsten bij de opsporing van nieuw materiaal van kindermisbruik.[4] Elke detectiemethode heeft een risico op vals-positieven. Denk aan radarpistolen, camera's voor verkeershandhaving, beveiligingsscanners op luchthavens en postpakketten, drugsspeurhonden, maar dit wil niet zeggen dat we technologieën niet gebruiken. Beperkingen en risico's van het systeem worden aangepakt om ervoor te zorgen dat vals-positieven geen gevolgen hebben voor onschuldige individuen. Ook voor de detectie van online kindermisbruik kunnen maatregelen worden genomen om te voorkomen dat onschuldige mensen negatieve gevolgen ondervinden of hun identiteit bekend is bij instanties. Middels een menselijke check door techbedrijven en door het EU Centrum, met *geblurde* gezichten en zonder identiteitsinformatie, kunnen vals-positieven eruit worden gefilterd. Alleen wanneer het echt om strafbaar materiaal gaat, kunnen identiteitskenmerken zichtbaar worden gemaakt en worden doorgestuurd naar autoriteiten. Behoud daarom het voorstel van het Hongaarse voorzitterschap om het detecteren van nieuw materiaal en grooming niet helemaal uit te sluiten, maar een clausule op te nemen dat de Commissie in staat stelt om in de toekomst de noodzaak en haalbaarheid opnieuw te beoordelen.

Consensuele seksuele exploratie onder adolescenten

Het is niet de bedoeling dat deze verordening de seksuele exploratie van jongeren beperkt of zelfs als illegaal wordt aangemerkt. Wij pleiten dan ook voor een ontwikkelingsgerichte aanpak, waarbij preventie- en controlemaatregelen zijn afgestemd op de leeftijd, capaciteiten en rechten van kinderen. Wij achten investering in veilige vormen van leeftijdsverificatie een kansrijk middel om online kindermisbruik tegen te gaan. In ieder geval dient in de Europese wetgeving te zijn vastgelegd dat vrijwillige sexting onder jongeren in dezelfde leeftijdsgroep niet strafbaar is. Dit moet worden geregeld in de herziening van de *Richtlijn 2011/93 - Bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie*, waarvoor op dit moment de onderhandelingen plaatsvinden. In dit kader is het relevant om te melden dat de detectietools zijn geënt om jongere kinderen te identificeren.

[4] Een vals-postieve uitkomst betreft materiaal dat in eerste instantie wordt gedetecteerd als misbruikmateriaal maar achteraf geen materiaal van seksueel misbruik blijkt te zijnl

Zodra tieners secundaire geslachtskenmerken ontwikkelen, kan de technologie niet goed het verschil met volwassenen onderscheiden. Daarom was 94% van de kinderen in het beeldmateriaal dat door IWF in 2022 werd gevonden onder de 14 jaar.[5] Ook Offlimits vond in dat jaar het vaakst strafbaar beeldmateriaal van meisjes tussen de 4 en 11 jaar. De technologie is daarom vooral gericht om jongere kinderen te beschermen.

OPROEP: Laat het belang van het kind de primaire overweging zijn in het wetgevingsproces rondom de verordening. Behoud de essentie van de verordening: gericht op preventie, bescherming tegen alle vormen van online kindermisbruik, toekomstbestendig en met een rechterlijke toets om fundamentele rechten te waarborgen.

Hoogachtend, namens de volgende organisaties:

DEFENCE for CHILDREN · ecpat · Terre des Hommes · IJM · FREE A GIRL · voor kinderen door kinderen KINDERPOSTZEGELS

Child Helpline International · fier! · ckm! CENTRUM KINDERHANDEL MENSENHANDEL · Spine · MISBRUIKT! · Praat · Jeugdhulp JVB

[5] https://annualreport2022.iwf.org.uk/trends-and-data/analysis-by-age/