Datum: 9 november 2023

Betreft: LIBE voorstel tot vaststelling van regels ter voorkoming en bestrijding van seksueel misbruik van kinderen

---

Geachte leden van de LIBE commissie,

Als vertegenwoordigers van meerdere kinderrechtenorganisaties schrijven wij u met betrekking tot het voorstel van de LIBE commissie op 26 oktober 2023 aangaande de verordening om te komen tot regels ter voorkoming en bestrijding van seksueel misbruik van kinderen in de online wereld, waarover u op 14 november zult stemmen. Vanwege de grote schaal van online seksueel kindermisbruik[1] is iedereen het erover eens dat er maatregelen moeten komen om het internet veilig te maken voor kinderen.

Wij juichen toe dat de LIBE Commissie meer rechten aan slachtoffers toekent door hen het recht op steun en bijstand van zowel het EU-centrum als de nationale coördinerende autoriteiten toe te kennen en een 'Victim's Rights and Survivors Forum' op te zetten. Ook vinden wij het goed dat er een uniforme meldingsknop komt op alle platformen. Het is belangrijk dat het melden makkelijker wordt gemaakt, maar we zien dit niet als dé oplossing. We weten dat slachtoffers van kindermisbruik en uitbuiting zelf nauwelijks een melding doen omdat zij onder druk of invloed staan van hun uitbuiter of misbruiker, of simpelweg niet weten waar hun materiaal op internet wordt gedeeld. We weten ook dat omstanders niet altijd handelen in het belang van het kind.

Onze **belangrijkste bezwaren** op het recente voorstel van de LIBE commissie:

- Detectiebevelen zijn enkel gericht op (groepen) gebruikers die een link hebben met kindermisbruik: via het strafprocesrecht bestaan reeds mogelijkheden om communicatie van deze groep te monitoren.
- Detectietools die al meer dan tien jaar door techbedrijven worden gebruikt om bekend materiaal van kindermisbruik van hun platforms te weren, zullen zij niet meer kunnen gebruiken. Hiermee wordt de hoeveelheid onderschepte strafbaar materiaal van kindermisbruik vele malen minder.
- Het EU centrum kan proactief opsporen naar online materiaal van kindermisbruik op het publieke gedeelte van het internet, maar niet in (niet-versleutelde) interpersoonlijke communicatie en ook niet bij de opslag van data. Dit kunnen techbedrijven die deze diensten aanbieden wel. Daarom is ook door deze aanpassing een vermindering van de signalering en verwijdering van strafbaar materiaal van kindermisbruik.
- Wij begrijpen niet dat in het proces van het detectiebevel een verzoek tot detectie twee keer langs een rechter zou moeten.
- Door end-to-end encryptie eruit te halen worden alle (toekomstige) mogelijkheden uitgesloten om online kindermisbruik binnen deze omgevingen tegen te gaan, zelfs wanneer deze geen inbreuk maken op de vertrouwelijkheid en veiligheid van onze interpersoonlijke online communicatie.

Hieronder lichten wij enkele van de bovengenoemde bezwaren nader toe:

Detectiebevel enkel gericht op (groepen) gebruikers
Detectiebevelen kunnen in het nieuwe voorstel alleen nog gericht zijn op individuele gebruikers of specifieke groepen gebruikers, die een (indirecte) link hebben met beeldmateriaal van kindermisbruik op basis van informatie die betrouwbaar en legaal is verkregen – als individuele gebruiker of als abonnee van een specifiek communicatiekanaal. Het bevel was in het originele voorstel gericht op een identificeerbaar deel of onderdeel van de online dienst, zoals specifieke soorten kanalen, én op specifieke gebruikers of specifieke groepen gebruikers, voor zover zij geïsoleerd kunnen worden. Aangezien er reeds mogelijkheden zijn via het strafrecht om communicatie in te zien van verdachten van seksueel kindermisbruik, heeft het voorstel daarmee geen toegevoegde waarde. Bovendien leidt

---

[1] Recent onderzoek heeft aangetoond dat maar liefst 68% van de 18-jarigen als kind in Nederland op enig moment ongewenst online seksueel gedrag heeft ervaren: https://www.weprotect.org/wp-content/uploads/WeProtect_Economist-Impact_European-online-sexual-harms-study_report_Dutch-translation.pdf
Cijfers van de Nationaal Rapporteur laten zien dat 1 op 4 meisjes en bijna 1 op 10 jongens een vorm van online seksuele intimidatie meemaakt: https://www.nationaalrapporteur.nl/publicaties/rapporten/2022/11/08/slachtoffermonitor-seksueel-geweld-tegen-kinderen

het tot een drastische vermindering van de hoeveelheid gedetecteerd, gerapporteerd en verwijderd strafbaar materiaal van kindermisbruik.

Detectiebevel 2x door rechterlijke instanties beoordeeld
Het verzoek tot detectie is twee keer opgenomen in het proces van het detectiebevel. Het aangepaste artikel 7 bevat een extra stap in het proces, namelijk dat de nationale coördinatie autoriteiten nog voor zij het concept detectieverzoek delen met de provider en het EU Centrum dit eerst moeten delen met rechterlijke autoriteiten. In het originele voorstel was dit alleen aan het eind van het detectiebevel-proces. Het is onduidelijk of de rechterlijke autoriteit ook een uitspraak doet bij de eerste keer. Het proces van het detectiebevel is zo opgesteld dat allerlei informatie wordt opgehaald, bijvoorbeeld van de technische commissie van het EU centrum, de online dienstverlener en de Europese databeschermingsautoriteit. Zo hebben rechters input om een afweging te kunnen maken van fundamentele rechten. In het aangepaste voorstel lijkt een rechter twee keer naar hetzelfde verzoek te kijken, alleen de tweede keer met meer informatie.

End-to-end encryptie eruit
Veiligheid van onze communicatie is van groot belang voor onze samenleving en vertrouwelijkheid van communicatie is een fundamenteel recht. Er zijn in E2EE omgevingen mogelijkheden om detectie uit te voeren zonder de vertrouwelijkheid van de communicatie in gevaar te brengen zonder de versleuteling te compromitteren. Dit gebeurt voor het detecteren van malware en spam en link previews te genereren. Dit zou in theorie ook kunnen voor het detecteren van online kindermisbruik. Zo zou er kunnen worden gescand op bekend misbruikmateriaal om te voorkomen dat het (opnieuw) wordt gedeeld of zelfs viraal gaat, zonder dit te melden. Hierdoor blijft communicatie end-to-end versleuteld. Bovendien kan er geïnvesteerd worden in waarschuwingssystemen die mensen bewust maken van risico's en mogelijkheden bieden om misbruikmateriaal te blokkeren, melden en hulp te zoeken, bijvoorbeeld via speciale portals bij kindertelefoon en hulplijnen. Door E2EE volledig uit te sluiten worden al deze (toekomstige) mogelijkheden uitgesloten, zelfs wanneer deze geen inbreuk maken op de vertrouwelijkheid en veiligheid van onze interpersoonlijke online communicatie. Volgens het VN Kinderrechtencomité (General Comment 25, paragraaf 70) moeten landen nadenken over goede maatregelen om het opsporen en melden van online seksueel misbruik en misbruikmateriaal mogelijk te maken in versleutelde omgevingen, met toepassing van gedegen waarborgen.

Oproep
Laat het belang van het kind de primaire overweging zijn in het wetgevingsproces rondom deze verordening. Online seksueel kindermisbruik komt op grote schaal voor en heeft levenslange gevolgen voor slachtoffers en hun omgeving. We hebben met deze wetgeving de kans om de online wereld veiliger te maken voor kinderen en hun welzijn in de digitale wereld te beschermen. Zorg ervoor dat de verordening behelst waar het voor is opgesteld: de bescherming van kinderen tegen alle gevaren voor online kindermisbruik. De wijzigingen beperken het signaleren en verwijderen van online kindermisbruik in vergelijking met wat online dienstverleners op dit moment op vrijwillige basis al doen. Dat kan toch niet de bedoeling zijn.

Hoogachtend,

M. Blaak
Directeur-Bestuurder Defence for Children – ECPAT

J. Verhaar
Directeur Terre des Hommes

Namens de volgende organisaties: