Bits of Freedom
Prinseneiland 97hs
1013 LN Amsterdam

Rejo Zenger
+31 6 3964 2738
rejo@bitsoffreedom.nl

bitsoffreedom.nl
IBAN: NL73 TRIO 0391 1073 80
KVK: 34 12 12 86, Amsterdam

Beste leden van de Commissie Justitie en Veiligheid,

Op 4 oktober aanstaande vindt er een technische briefing plaats over de Europese Verordening ter voorkoming en bestrijding van seksueel kindermisbruik online.[1] De bestrijding van seksueel misbruik van kinderen is ontzettend belangrijk. Daarom is het cruciaal om juist in te zetten op effectieve en duurzame maatregelen. In dat kader geef ik u graag enkele suggesties voor vragen.

1. **Hoe wordt de ontwikkeling, beschikbaarheid en toepassing van end-to-end encryptie gewaarborgd?** Op grond van artikel 7 kunnen aanbieders van diensten zoals WhatsApp of Signal gedwongen om materiaal van seksueel misbruik van kinderen te detecteren. Voor de veiligheid van de gebruikers is de communicatie van deze diensten versleuteld met end-to-end encryptie. De essentie van die technologie: alleen de verzender en de beoogd ontvanger hebben toegang tot de inhoud van het bericht. De aanbieder heeft geen optie om mee te kijken met de inhoud. Zou zij daartoe gedwongen worden, zal zij haar systeem zodanig aanpassen dat de essentie van end-to-end encryptie ondermijnt wordt.
2. **Hoe kunnen internettoegangsproviders de toegang tot specifieke adressen blokkeren, als zij daarvan geen weet hebben?** Op grond van artikel 16 zouden zulke providers, zoals KPN of VodafoneZiggo, gedwongen kunnen worden om de toegang tot zogenaamde “uniform resource locators” te blokkeren. Die “URL’s” zijn adressen van specifieke pagina’s of specifieke afbeeldingen op een website. Tegenwoordig zijn vrijwel alle websites alleen toegankelijk via een beveiligde TLS-verbinding (de “s” in “https://”). Het gevolg daarvan is dat een provider enkel en alleen kan zien dat u de website van de Tweede Kamer bezoekt, maar niet welke specifieke pagina of afbeelding u ziet. Het is voor zo’n provider dan ook technisch onmogelijk uitvoering te geven aan zo’n bevel.
3. **Valt het op vrijwillige basis monitoren van de communicatie van gebruikers door aanbieders van diensten als WhatsApp of Signal ook onder de reikwijdte van de risk mitigation maatregelen uit artikel 4?** Op grond van artikel 7 kunnen aanbieders van diensten zoals WhatsApp of Signal gedwongen om materiaal van seksueel misbruik van kinderen te detecteren. Zo’n bevel kan pas gegeven worden indien de *risk mitigation measures* uit artikel 4 onvoldoende effectief blijken. Is het mogelijk dat zo’n aanbieder op grond van artikel 4 reeds op “vrijwillige basis” de communicatie van haar gebruikers monitored met als doel de verspreiding van seksueel misbruik van kinderen te detecteren?
4. **Vallen traditionele telefoongesprekken en SMS-berichten ook onder de reikwijdte van deze wet?** De spraakdiensten van aanbieders zoals KPN of VodafoneZiggo, inclusief gerelateerde diensten zoals SMS en MMS, vallen onder de zogenaamde “interpersonal communications service” (zoals gedefinieerd in de European Electronic

1 Agenda-item op tweedekamer.nl

Communications Code (EECC)). Die zouden op grond van artikel 7 dan ook verplicht kunnen worden om ongericht alle gesprekken en berichten van hun gebruikers af te luisteren. (!)

5. **Hoe verhoudt zich de ongerichte toezichtsverplichting zoals volgt uit een bevel op grond van artikel 7 met het verbod op een algemene toezichtsverplichting?** Op grond van artikel 15 van de E-Commerce Directive mogen "de lidstaten de dienstverleners geen algemene verplichting op om toe te zien op de informatie die zij doorgeven of opslaan, noch om actief te zoeken naar feiten of omstandigheden die op onwettige activiteiten duiden." Op grond van het voorgestelde artikel 7 zouden aanbieders van bepaalde diensten op het internet een bevel opgelegd kunnen worden om te zoeken naar materiaal van seksueel misbruik van kinderen (in een stroom van onschuldige informatie.) Zo'n verplichting kan alleen opgelegd worden indien de toezichtverplichting ook is beperkt tot *potential infringers*.[2] Dat is hier niet het geval, omdat het toezicht op alle gebruikers van de dienst betrekking toegepast zal worden.
6. **Op welke wijze zijn de ervaringen van de huidige meldpunten, zoals het Amerikaanse NCMEC en het Nederlandse EOKM meegenomen in het voorstel?** Het Amerikaanse NCMEC heeft in 2021 bijna 30 miljoen meldingen van materiaal van seksueel misbruik van kinderen ontvangen. Het NCMEC geeft zelf aan niet elke melding, laat staan elke afbeelding, te kunnen beoordelen, door het enorme volume.[3] Een groot deel van deze meldingen heeft betrekking op materiaal dat in de Europese Unie wordt verzonden of gehost. Hoeveel mensen is er bij het EU Center naar schatting nodig om al het materiaal te controleren en daarop actie te ondernemen? Is er bij die inschatting ook rekening gehouden met het feit dat, met name bij de detectie van onbekend materiaal en grooming, grote foutmarges bestaan?
7. **Bestaat er onafhankelijk en wetenschappelijk verantwoord onderzoek naar de betrouwbaarheid en effectiviteit van de software die wordt ingezet om onbekend en bekend materiaal van seksueel misbruik van kinderen en grooming te detecteren?** De mate van effectiviteit is belangrijk voor de vraag of de inzet van zulke software proportioneel kan zijn: als de software heel veel *false negatives* kent (en dus veel problemen ten onrechte niet opmerkt) verkleint dat de proportionaliteit van de inbreuk (van het moeten monitoren van alle berichten van alle gebruikers). De mate van betrouwbaarheid is belangrijk omdat in geval van *false positives* gebruikers ten onrechte van seksueel misbruik van kinderen worden beschuldigd én deze *false positives* een groot beslag leggen op de kostbare capaciteit van opsporingsdiensten. Voor zover bekend bestaat er geen onafhankelijk en wetenschappelijk verantwoord onderzoek naar de betrouwbaarheid en effectiviteit van de software die de Europese Commissie voor ogen heeft.
8. **Het is onmogelijk om materiaal van seksueel misbruik van kinderen foutloos te detecteren. Soms wordt materiaal als problematisch aangemerkt, terwijl dat niet het geval is. Welke foutmarge is ethisch te verdedigen?** In antwoord op de vragen van de Duitse regering stelde de Europese Commissie dat de betrouwbaarheid van de software

2 "The Odyssey of the Prohibition on General Monitoring Obligations on the Way to the Digital Services Act", Senftleben en Angelopoulos (bron)
3 "Declaration of John Shehan" (bron)

voor het herkennen van *grooming*[4] rond 90 procent ligt.[5] Dat betekent dat 1 op de 10 door de software aangewezen conversaties van grooming geen misbruik van kinderen betreft (maar bijvoorbeeld een seksueel getint gesprek tussen twee jongeren of het gesprek tussen een kind en een hulpverlener). Dat betekent dat regelmatig een gebruiker ten onrechte wordt beschuldigd van het schokkende misdrijf van seksueel misbruik van kinderen. Dat kan onder omstandigheden iemand de rest van zijn leven achtervolgen.

9. **Zijn er waarborgen tegen het misbruik van het systeem door kwaadwillenden om onschuldigen te belasteren?** Zo ontving een Nederlander in 2020 via WhatsApp van iemand anders en ongevraagd een grappig bedoelde foto met op de achtergrond twee blote kinderen. Zijn telefoon stond zo ingesteld dat die foto's automatisch werden gekopieerd naar Microsoft's computers. Microsoft's kunstmatige intelligentie bestempelde de foto als seksueel misbruik van kinderen en blokkeerden vervolgens direct het account van de gebruiker.[6] In de voorgestelde wetgeving zou Microsoft ook de gebruiken moeten rapporteren bij een instantie (en daarmee een gebruiker ten onrechte beschuldigen).[7] De vraag is: zijn er in het voorstel van de Europese Commissie waarborgen die er voor moeten zorgen dat het systeem niet *weaponized* kan worden?

Vanzelfsprekend ben ik graag bereid tot een nadere toelichting, mocht daar behoefte aan bestaan.

Met vriendelijke groet,

Rejo Zenger

4 Politie Nederland: "Grooming is digitaal kinderlokken. Er is sprake van grooming als een volwassene via ICT contact legt met een kind, met de intentie om dat kind te ontmoeten met het doel om seksueel misbruik te plegen of kinderpornografische afbeeldingen te produceren."
5 "EU-Kommission nimmt hohe Fehlerquoten bei Chatkontrolle in Kauf", Netzpolitik.org (bron)
6 "Pas maar op met wat iemand anders jou stuurt", Bits of Freedom (bron)
7 "Google beschuldigt jou van kindermisbruik? Kan niet! Toch?", Bits of Freedom (bron)