Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

26 643 **Informatie- en communicatietechnologie (ICT)**

34 843 **Seksuele intimidatie en geweld**

Nr. 1069 **BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 18 september 2023

In een tweeminutendebat op 20 april jl. (Handelingen II 2022/23, nr. 77, item 7) diende het lid Van Ginneken c.s. een motie in over de Europese Verordening ter bestrijding en voorkoming van seksueel kindermisbruik (Kamerstuk 26 643, nr. 1011). Hierin wordt de regering verzocht om:

«ervoor te zorgen dat het voorstel geen encryptie bedreigende chatcontrol bevat, zoals client side scanning, en anders de verordening niet goed te keuren».

Uw Kamer heb ik op 28 juni jl. geïnformeerd over de beslissing van het kabinet om deze motie niet uit te voeren en heb ik dat besluit nader toegelicht (Kamerstuk 26 643, nr. 1043). Uw Kamer heeft mij tijdens het commissiedebat over online veiligheid en cybercriminaliteit, gehouden op 29 juni jl., verzocht om een nadere onderbouwing van feiten en cijfers ter ondersteuning van dat besluit toe te sturen, alsmede een uitleg van *client-side scanning*. Ook heeft uw Kamer daarbij verzocht in te gaan op de zorgen over de effectiviteit van het detectiebevel van Offlimits (voorheen Expertisebureau Online Kindermisbruik, EOKM) en het voorbeeld van *client-side scanning* van Apple.

De vragen die uw Kamer op 29 juni jl. stelde, hadden onder meer betrekking op de veronderstelling dat interpersoonlijke communicatiediensten – zoals bijvoorbeeld Whatsapp of Signal – (in toenemende mate) worden gebruikt om materiaal van online seksueel kindermisbruik, waaronder beelden en video's, te verspreiden. Hieronder beschrijf ik de bronnen waarop deze veronderstelling mede is gebaseerd.

WODC-rapport «De rol van encryptie in de opsporing: Belemmeringen en mogelijkheden» (2023)

In mei 2023 publiceerde het Wetenschappelijk Onderzoek en Documentatie Centrum het rapport «De rol van encryptie in de opsporing: Belemmeringen en mogelijkheden». Daarin wordt onder meer geconstateerd dat

kst-26643-1069
ISSN 0921 - 7371
's-Gravenhage 2023

online kindermisbruikers in toenemende mate online anonimiteit- en encryptiehulpmiddelen gebruiken om materiaal te maken en delen.[1] Het gebruik van end-to-end versleutelde communicatie-apps, zoals Signal en Telegram, wordt populairder onder daders van kindermisbruik, blijkt ook uit wetenschappelijk onderzoek en meldingen die wereldwijd van de vondst van dit materiaal worden gedaan.[2] Uit een analyse van de meldingen van het gezaghebbende Amerikaanse National Center for Missing and Exploited Children (NCMEC) blijkt de EU wereldwijd de grootste geografische hub waar materiaal van seksueel kindermisbruik gedeeld wordt. Negen van de tien gerapporteerde url's worden gehost in Europa. 94% van deze meldingen waren afkomstig van platformen van het bedrijf Facebook (tegenwoordig Meta), zoals Messenger, Instagram en WhatsApp.[3]

Europol

Europol bevestigt dat de toename van end-to-end versleutelde applicaties en sociale media platforms van invloed zijn op de toename van «grooming» (kinderlokken) en de wijze van verspreiding van online materiaal van seksueel kindermisbruik.[4] Het gaat hierbij zowel om het een-op-een delen van materiaal als het delen in grotere communicatiegroepen. In hetzelfde rapport signaleert Europol ook een stijging van het gebruik van *social media*-platforms voor het delen van online materiaal van seksueel kindermisbruik. In sommige gevallen gaat het om zelfgemaakt materiaal dat na het delen met anderen verder verspreid wordt; in andere gevallen om het gebruik van nepaccounts om materiaal snel met elkaar te delen om vervolgens het account te verwijderen. Dat maakt de opsporing van dergelijke daders zeer lastig.

National Center for Missing and Exploited Children (NCMEC)

Het *National Center for Missing and Exploited Children* is een Amerikaanse non-profitorganisatie opgericht door het Congres van de Verenigde Staten. Deze organisatie beheert ook de CyberTipline die door het Congres is opgericht. Dit is een meldsysteem om indicaties van online materiaal van seksueel kindermisbruik te melden, waarna het *National Center for Missing and Exploited Children* de informatie verifieert en doorzet naar opsporingsinstanties. Grote techbedrijven maken gebruik van verschillende methoden om online materiaal van seksueel kindermisbruik op hun platformen op te sporen en te verwijderen, zoals hashdatabases, PhotoDNA en artificiële intelligentie. Deze manieren voor techbedrijven om inhoud op hun platformen te «zien», zijn ook vaak de enige manieren om meldingen bij opsporingsinstanties te doen.

In 2019 uitte het *National Center for Missing and Exploited Children* voor het eerst haar grote zorgen over de groeiende impact van encryptie bij de aanpak van seksueel kindermisbruik. De organisatie schat in dat als end-to-end versleuteling wordt geïmplementeerd zonder oplossingen om kinderen te beschermen, ze meer dan de helft minder meldingen zullen ontvangen. Dat betekent dus niet dat minder materiaal online aanwezig is,

---

[1] WODC-rapport «De rol van encryptie in de opsporing: belemmeringen en mogelijkheden», 2023, p. 32.

[2] Zie o.a.: Child Sex Abuse Images and Exploitation Materials, R. Broadhurst, Australian National University Cybercrime Observatory (2019) en Assessing the challenges affecting the investigative methods to combat online child exploitation material offenses, T.J. Holt, J. Holt, J. Cale, B. Leclerc & J. Drew, Aggression and Violent Behavior 55 (2020), Elsevier.

[3] National Center for Missing and Exploited Children (NCMEC) (2020). 2020 CyberTipline reports by electronic service providers (ESP). Verkregen via: https://www.missingkids.org/content/dam/missingkids/pdfs/2020-reports-by-esp.pdf.

[4] Europol, Internet Organized Crime Threat Assessment, 2021.

maar het biedt daders de mogelijkheid om hun criminele activiteiten beter te verbergen.[5]

In het rapport van meldingen over 2022 staan meer dan twintig miljoen meldingen over Facebook, vijf miljoen meldingen die over Instagram zijn binnengekomen, ruim 2 miljoen meldingen over Google en één miljoen meldingen van online materiaal van seksueel kindermisbruik die over WhatsApp werden gedeeld.[6] Vergeleken met de meldingen over 2020 zijn dus een miljoen meer meldingen binnengekomen over een interpersoonlijke communicatiedienst die gebruik maakt van end-to-end encryptie.[7] Dit zijn enorme aantallen waartoe opsporingsinstanties moeilijk toegang hebben.

Client-side scanning

Uw Kamer verzocht tijdens het commissiedebat op 29 juni jl. (Kamerstukken 26 643 en 30 821, nr. 1064) in deze brief ook stil te staan bij de betekenis van *client-side scanning*. *Client-side scanning* is een check die plaatsvindt vóór verzending van een bericht, dus ook vóór dat het bericht wordt versleuteld. Het gaat hierbij om een check in de app zelf van een te verzenden bericht en niet een check op al het materiaal op een telefoon. Deze techniek wordt onder andere gebruikt om spelfouten uit berichten te halen («autocorrect») of linkjes naar websites te scannen op kwaadaardige software voordat een bericht wordt verzonden. Een ander voorbeeld hiervan is de mogelijkheid die Apple in apparaten van Apple (zoals de iPhone) heeft ingebouwd om bij gebruik van de app Messages kinderen te beschermen tegen het ontvangen en verzenden van naaktbeelden. Deze functionaliteit kan door ouders worden ingeschakeld. De techniek die Apple hiervoor gebruikt, maakt gebruik van *on device machine learning* om te analyseren of een bijgevoegde foto naaktbeelden bevat. Hiermee worden bijvoorbeeld foto's en/of video's gescand op naakt materiaal voordat het kind de inhoud ervan te zien krijgt of voordat het kind de foto zou willen verzenden. Deze scan in de app Messages is gericht op het materiaal zelf; zowel Apple als de ouders krijgen hier geen notificatie van.[8]

Factcheck TU Delft over interpersoonlijke communicatiediensten

De TU Delft heeft op verzoek van Offlimits (voorheen EOKM) een «factcheck» uitgevoerd waarin uitspraken van Eurocommissaris Johansson worden gecheckt over de verplaatsing van het delen van online materiaal van seksueel kindermisbruik naar interpersoonlijke, vaak end-to-end versleutelde, communicatiediensten zoals Whatsapp en Telegram.[9] In de factcheck worden cijfers aangehaald van meldpunten als het *National Center for Missing and Exploited Children* en Offlimits zelf waaruit volgt dat een klein gedeelte van de meldingen afkomstig is van chatdiensten als Whatsapp en Telegram, reden voor uw Kamer om vragen te stellen ten aanzien van de effectiviteit van detectie binnen deze diensten. Zoals ook hierboven is geschetst, is er wel degelijk een stijging te zien van meldingen over het gebruik van interpersoonlijke communicatiediensten voor het delen van online materiaal van seksueel kindermis-

---

[5] Zie https://www.missingkids.org/content/dam/missingkids/pdfs/End-to-End%20Encryption%20Media%20Kit.pdf.

[6] 2022 CyberTipline Reports by ESP (missingkids.org).

[7] Child sexual abuse material and end-to-end encryption on social media platforms: An overview, Teunissen & Napier, 2022 en National Center for Missing and Exploited Children (NCMEC) (2020). 2020 CyberTipline reports by electronic service providers (ESP). Verkregen via: https://www.missingkids.org/content/dam/missingkids/pdfs/2020-reports-by-esp.pdf.

[8] Child Safety – Apple.

[9] Pakt nieuwe EU-wet kindermisbruik aan of zorgt deze voor massasurveillance? (trouw.nl); Q&A: EU new rules to fight child sexual abuse (europa.eu).

bruik. Dat op het totaal bezien relatief weinig meldingen van deze services afkomstig zijn, kan goed worden verklaard doordat deze services niet zelden end-to-end versleuteld zijn en het dus lastig is om zicht te krijgen op het materiaal dat via deze diensten wordt verspreid. De effectiviteit van het detectiebevel kan om die reden niet op voorhand worden gemeten.

Ik zie gelet op het bovenstaande geen reden om de mogelijkheden van detectie van reeds bekend materiaal van online seksueel kindermisbruik binnen end-to-end versleutelde interpersoonlijke communicatiediensten per definitie uit te sluiten tijdens de onderhandelingen over de Europese Verordening ter bestrijding en voorkoming van seksueel misbruik. Voor verdere toelichting over dit standpunt verwijs ik u graag naar de eerder verzonden brieven over deze onderhandelingen.

Onder verwijzing naar de motie van het lid Van Weerdenburg c.s. (Kamerstuk 26 643, nr. 1047), maak ik uw Kamer er ten slotte op attent dat de Verordening, ten behoeve van het bereiken van een (gedeeltelijke) algemene oriëntatie, door het voorzitterschap is geagendeerd voor de JBZ-Raad van 28 september a.s. De voorgenomen inzet van het Kabinet tijdens deze Raad, inclusief de inzet met betrekking tot de CSAM-verordening, is op de gebruikelijke wijze als geannoteerde agenda vandaag (18 september) met uw Kamer gedeeld. In de motie van Weerdenburg c.s., wordt verzocht geen onomkeerbare stappen te nemen voorafgaand aan een gedachtewisseling hierover met de Tweede Kamer. In dat licht verwijs ik graag naar het schriftelijk overleg over de Nederlandse inzet tijdens de JBZ raad dat gepland staat voor 25 september a.s.

De Minister van Justitie en Veiligheid,
D. Yeşilgöz-Zegerius