Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

3392

Vragen van de leden **Slootweg** en **Kuik** (beiden CDA) aan de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties en de Minister van Justitie en Veiligheid over *het bericht «WhatsApp en Signal dreigen VK te verlaten vanwege breken encryptie» van AG Connect:* (ingezonden 16 mei 2023).

Antwoord van Minister **Yeşilgöz-Zegerius** (Justitie en Veiligheid) (ontvangen 22 augustus 2023). Zie ook Aanhangsel Handelingen, vergaderjaar 2022–2023, nr. 2830.

Vraag 1
Bent u bekend met het bericht «WhatsApp en Signal dreigen VK te verlaten vanwege breken encryptie»?[1]

Antwoord 1
Ja.

Vraag 2
Wat regelt het wetsvoorstel Online Safety Bill in het Verenigd Koninkrijk precies?

Antwoord 2
Het gaat hier om een wetsvoorstel uit het Verenigd Koninkrijk dat nog niet volledig is behandeld in het Britse parlement. Terughoudendheid bij de beoordeling daarvan is derhalve gepast. In grote lijnen kan worden aangegeven wat dit voorstel behelst, voor zover nu bekend. In de Online Safety Bill worden regels en zorgplichten gesteld voor internetdiensten rondom de aanpak van online illegale inhoud en de bescherming van kinderen, journalisten en democratische waarden. Een apart hoofdstuk is ingericht over het rapporteren van online materiaal van seksueel kindermisbruik (CSAM) en een hoofdstuk rondom de verplichtingen die internetdiensten hebben op het gebied van online pornografie. Tenslotte krijgt the Office of Communications, OFCOM, de rol van handhaver op het gebied van de Online Safety Bill.

[1] «WhatsApp en Signal dreigen VK te verlaten vanwege breken encryptie», AG Connect, 3 mei, via https://www.agconnect.nl/artikel/whatsapp-en-signal-dreigen-vk-te-verlaten-vanwege-breken-encryptie.

ah-tk-20222023-3392
ISSN 0921 - 7398
's-Gravenhage 2023

Vraag 3
Hoe beoordeelt u dit wetsvoorstel?

Antwoord 3
Zoals ik onder vraag 2 heb geschetst is dit wetsvoorstel nog in behandeling en is het lastig om een definitieve beoordeling te geven van de waarde hiervan. Vooral omdat nog niet bekend is wat de eventuele effecten van dit wetsvoorstel voor Nederland zullen zijn, als die er al zijn. Voor zover op dit moment het beoordeeld kan worden, komt de voorgestelde regelgeving grotendeels overeen met de regels die zijn gesteld in de Digital Services Act, die voor Nederland in februari 2024 in werking zal treden. Ook hier worden regels opgelegd aan tussenhandeldiensten rondom transparantie en het modereren op illegale inhoud. Voor online materiaal van seksueel kindermisbruik onderhandelen lidstaten momenteel in de Europese Unie over een verordening die hier specifieke regelgeving op maakt (CSAM-verordening). Zonder teveel op de inhoud in te gaan, kan het worden toegejuicht dat ook het Verenigd Koninkrijk, net als de Europese Unie, stappen neemt in het beter reguleren van tussenhandeldiensten en online illegale inhoud. Het internet is niet gebonden aan landsgrenzen en overheden hebben een gezamenlijke verantwoordelijkheid om het schoon en veilig te houden.

Vraag 4
Ziet u het nut van de mogelijkheid om chatapps te kunnen scannen op materiaal van kindermisbruik om makers en verspreiders daarvan te kunnen opsporen, vervolgen en te bestraffen?

Antwoord 4
Interpersoonlijke communicatiediensten worden steeds vaker gebruikt om materiaal van seksueel kindermisbruik te verspreiden.[2] Juist deze diensten maken vaak gebruik van end-to-end encryptie. Zoals gezegd vinden in Brussel momenteel onderhandelingen plaats over een verordening om de verspreiding van online kinderpornografisch materiaal tegen te gaan. Een onderdeel uit deze concept-Verordening betreft het voorstel voor het instellen van een zogeheten «detectiebevel». Op basis van dit detectiebevel kunnen bedrijven – onder meer aanbieders van interpersoonlijke communicatiediensten, zoals Whatsapp en Signal – onder voorwaarden worden verplicht om op hun diensten te scannen op de aanwezigheid van materiaal van online seksueel kindermisbruik.
Zoals ik onder andere in mijn brief van 2 februari 2023 aan uw Kamer heb weergegeven, is het detectiebevel een maatregel die inbreuk maakt op verschillende grondrechten.[3] Voor Nederland staat bij de onderhandelingen voorop dat die inbreuk moet kunnen worden gerechtvaardigd. Uw Kamer is daar reeds uitgebreid over geïnformeerd. In alle gevallen geldt dat voorstellen die end-to-end encryptie onmogelijk maken niet kunnen worden ondersteund, conform de in juli 2022 door de Tweede Kamer aangenomen motie-Van Raan c.s.[4]

Vraag 5
Wat vindt het kabinet ervan dat encryptie wordt gebruikt om materiaal van kindermisbruik te kunnen delen en te verspreiden?

Antwoord 5
Het is juist dat interpersoonlijke communicatiediensten die gebruik maken van end-to-end encryptie, in toenemende mate worden misbruikt voor het delen van materiaal van kindermisbruik.[5] Dit vind ik een zorgelijke ontwikkeling. Er moet worden voorkomen dat criminelen op deze diensten vrij spel hebben bij het verspreiden van online materiaal van seksueel kindermisbruik. We hebben het vaak over «online materiaal», «beelden», of «video's». Maar achter dit digitale materiaal gaat een verschrikkelijke fysieke waarheid schuil

[2] Zie WODC Onderzoek «De rol van encryptie in de opsporing, belemmeringen en mogelijkheden»; Internet Watch Foundation, Annual report 2022, https://annualreport2022.iwf.org.uk/.
[3] Kamerstuk 26 643, nr. 998, d.d. 2 februari 2023.
[4] Kamerstuk 26 643, nr. 885, d.d. 30 juni 2023.
[5] Zie WODC Onderzoek «De rol van encryptie in de opsporing, belemmeringen en mogelijkheden».

waar we onze ogen niet voor mogen sluiten. Ik zal mij blijvend inzetten om, binnen de grenzen van de motie Van Raan c.s., te zoeken naar mogelijkheden (zie antwoord 4) om de omloop van dit verwerpelijke materiaal te stoppen.

Vraag 6
Deelt u de mening dat de mogelijkheid om berichtendiensten te kunnen scannen op materiaal van kindermisbruik zwaarder moet wegen dan het recht van aanbieders om volledige encryptie aan te bieden aan gebruikers?

Antwoord 6
Encryptie stelt de opsporing voor grote uitdagingen. In opsporingsonderzoeken blijkt het in veel gevallen zeer lastig en soms onmogelijk om gegevens die nodig zijn om criminelen op te sporen te verkrijgen. Tegelijkertijd is sterke encryptie van groot belang voor het beschermen van de vertrouwelijkheid van communicatie als grondrecht en de beveiliging van communicatie. Het vinden van oplossingen die voldoende recht doen aan alle betrokken belangen is lastig. Ik zie de absolute noodzaak om het bestaan en de verspreiding online van beeldmateriaal van seksueel kindermisbruik te voorkomen, en daarmee de grondrechten van deze kinderen te beschermen. Maar tegelijkertijd is het de absolute noodzaak om grondrechten, zoals eerbiediging van de persoonlijke levenssfeer en bescherming van het telecommunicatiegeheim, te eerbiedigen. Met *client-side scanning* bestaat de mogelijkheid om binnen interpersoonlijke communicatiediensten te scannen op bestaand materiaal van seksueel kindermisbruik zonder dat end-to-end encryptie onmogelijk wordt gemaakt, zoals ook toegelicht in mijn brief van 2 februari 2023.[6] Het blijft van belang om bij de mogelijkheden die Nederland ziet steeds aandacht te besteden aan de noodzakelijkheid, proportionaliteit en subsidiariteit ervan en daarbij steeds een weging te maken van alle betrokken belangen.

Vraag 7
Zo ja, is het kabinet voornemens het Britse voorbeeld te volgen en te komen met een Nederlandse versie van de Online Safety Bill?

Antwoord 7
Zoals gezegd zal in Nederland de Digital Services Act van toepassing zijn vanaf februari 2024. Specifiek voor de handhaving op het gebied van online materiaal van seksueel kindermisbruik heb ik onlangs de wet bestuursrechtelijke bevoegdheden aanpak online kinderpornografisch materiaal naar uw Kamer verzonden en onderhandel ik momenteel in Brussel over de reeds aangehaalde CSAM-Verordening.[7]

Vraag 8
Bent u het eens met de bewering van Ciaran Martin, de voormalige baas van het Britse Cyber Security Centre tegen Politico dat «Client-side scanning lijkt, ondanks de claims van tegenstanders, wel een bepaald niveau van toegang te omvatten, een soort mogelijkheid om te sorteren en te scannen»[8], waardoor opsporings- en veiligheidsdiensten wel degelijk delen en verspreiden van online kindermisbruik kunnen aanpakken?

Antwoord 8
In mijn brief van 31 januari jl. aan uw Kamer heb ik *client-side scanning* expliciet als optie benoemd om materiaal van seksueel misbruik te onderkennen wanneer deze worden verstuurd via diensten die gebruik maken van

---

[6] Kamerstuk 26 643, nr. 998, d.d. 2 februari 2023; zie ook Brief inzake motie over de Europese Verordening ter bestrijding en voorkoming van seksueel misbruik d.d. 8 mei 2023l; Brief Brief inzake het niet uitvoeren van de op 9 mei door de Tweede Kamer aangenomen motie-Van Ginneken c.s.] d.d. 27 juni 2023.

[7] Kamerstuk 36 377, nr. 1.

[8] «WhatsApp en Signal dreigen VK te verlaten vanwege breken encryptie», AG Connect, 3 mei, via https://www.agconnect.nl/artikel/whatsapp-en-signal-dreigen-vk-te-verlaten-vanwege-breken-encryptie.

end-to-end encryptie.[9] Met *client-side scanning* kunnen berichten die zijn verstuurd binnen de desbetreffende interpersoonlijke communicatiediensten op het apparaat van de verzender worden geanalyseerd op materiaal van seksueel kindermisbruik vóórdat dit materiaal wordt versleuteld en verzonden. De end-to-end versleuteling van het bericht tijdens het transport naar de ontvanger blijft dan ongemoeid, waardoor het bericht niet kan worden onderschept door derden. Uitgangspunt bij het nemen van dergelijke maatregelen is steeds respect voor fundamentele rechten, data-protectiewetgeving en behoud van cybersecurity. Ook wordt scherp gekeken of het middel proportioneel is ten aanzien van het doel dat wordt nagestreefd. Zo acht het kabinet het niet proportioneel wanneer dit middel wordt ingezet om tekstberichten te scannen, maar wel indien enkel wordt gescand op bestaand beeldmateriaal. Dat wil zeggen, materiaal waarvan reeds is vastgesteld dat dit materiaal betreft van seksueel kindermisbruik, en waarvan het bezit dus strafbaar is. Omdat bij het gebruik van *client-side scanning* het communicatiegeheim moet worden gewaarborgd, beziet het kabinet verder zeer kritisch welke nadere waarborgen aan het bevel moeten worden verbonden, met name ten aanzien van de vraag wat er met gedetecteerde informatie moet gebeuren.

Vraag 9
Is het kabinet van mening dat de mogelijkheid om berichtendiensten te scannen op materiaal van kindermisbruik zwaarder moet wegen dan een dreigend vertrek van WhatsApp en Signal uit Nederland, wanneer blijkt dat het breken van encryptie een effectieve manier is om online kindermisbruik tegen te gaan?

Antwoord 9
Nederland steunt geen Europese voorstellen die end-to-end encryptie onmogelijk maken, in lijn met de door uw Kamer aangenomen motie-Van Raan c.s. De strijd tegen online seksueel kindermisbruik blijft desalniettemin van essentieel belang, zeker gelet op de grote rol van Nederland als het gaat om het hosten van online materiaal van seksueel kindermisbruik.[10] Ik voel daarom een grote verantwoordelijkheid voor het vormgeven van een effectieve bestrijding van seksueel kindermisbruik, binnen het kader van de motie-Van Raan c.s., waarbij alle grondrechten worden geëerbiedigd. Zoals onder de vragen 4 en 8 weergegeven, lijkt *client-side scanning* de enige manier waarop de maatregelen in de verordening ten aanzien van interpersoonlijke communicatiediensten kunnen worden uitgevoerd zonder end-to-end encryptie onmogelijk te maken. Het is daarbij belangrijk dat berichtendiensten – zoals Whatsapp of Signal – niet buiten de reikwijdte van de verordening vallen.

[9] Verslag van een schriftelijk overleg over uitvoering van de motie van het lid Van Raan c.s. over end-to-end encryptie in stand houden (Kamerstuk 26 643, nr. 885) (Kamerstuk 26 643, nr. 908).

[10] Zie o.a. de jaarlijkse rapporten van INHOPE (www.inhope.org) en de Internet Watch Foundation (www.iwf.org.uk).