Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2018–2019

Aanhangsel van de Handelingen

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

1353

Vragen van het lid **Van Nispen** (SP) aan de Staatssecretaris van Economische Zaken en Klimaat en de Ministers van Justitie en Veiligheid en voor Rechtsbescherming over *de mogelijk negatieve effecten van de e-privacyrichtlijn op het werk van het Expertisebureau Online Kindermisbruik (EOKM)* (ingezonden 5 december 2018).

Antwoord van Staatssecretaris **Keijzer** (Economische Zaken en Klimaat), mede namens de Minister van Justitie en Veiligheid (ontvangen 30 januari 2019).

Vraag 1
Heeft u kennisgenomen van de brandbrief van (internationale) kinderbeschermingsorganisaties waarin gewezen wordt op een mogelijk nadelig effect van de e-privacyrichtlijn in de mogelijkheden om bijvoorbeeld kinderporno op te sporen? [1]

Antwoord 1
Ja.

Vraag 2
Kunt u garanderen dat de e-privacyrichtlijn, meer specifiek artikel vijf van de richtlijn, niet zal verhinderen dat het EOKM, of andere private partijen, zonder toestemming van de eindgebruiker het netwerkverkeer voorafgaande aan de upload kunnen scannen op kinderporno? Zo nee, bent u bereid tezamen naar een oplossing voor dit probleem te zoeken?

Antwoord 2
Op dit moment worden uploads niet preventief gescand op de aanwezigheid van kinderpornografische content, met als doel verwijdering van deze strafbare content. Zowel in de geldende als toekomstige e-privacyregels is het communicatiegeheim verankerd. Dit betekent dat aanbieders van telecommunicatiediensten in beginsel niet in het telecommunicatieverkeer mogen kijken dat zij verzorgen. Het gaat hier om een belangrijk grondrecht. Zo mag een partij die internettoegang aanbiedt (zoals KPN of Ziggo) bij het uploaden van beeldmateriaal, in beginsel niet bekijken wat er wordt geupload. De reikwijdte van het communicatiegeheim is echter beperkt tot de fase waarin het

[1] http://www.chis.org.uk/2018/12/01/child-protection-organizations-across-europe-and-the-world-express-grave-concerns, 01-12-2018

ah-tk-20182019-1353
ISSN 0921 - 7398
's-Gravenhage 2019

elektronisch transport wordt verzorgd. Toegepast op het zojuist genoemde voorbeeld betekent dit dat zodra het beeldmateriaal op de server van hostingpartij (de partij die er voor zorgt dat de betreffende inhoud op internet te vinden is) is aangekomen niet langer de e-privacyregels van toepassing zijn maar de regels van de Algemene verordening gegevensbescherming. Dat betekent op zijn beurt weer dat het de hosting partij is toegestaan met behulp van de zogenoemde hashdatabase strafbare kinderpornografische content van zijn server te verwijderen.

Vraag 3
Kunt u garanderen dat het EOKM ook na inwerkingtreding van de e-privacyrichtlijn gebruik zal kunnen maken van haar zogenoemde «hashdatabase» in haar strijd om kinderporno op het internet op te sporen? Zo nee, waarom niet en bent u bereid hier alsnog maatregelen voor te nemen?

Antwoord 3
Ja, zie het antwoord op vraag 2
Zoals aangegeven in het antwoord op vraag 2 zijn de e-privacyregels niet langer van toepassing op het moment dat kinderpornografisch beeldmateriaal is aangekomen op de server van de hostingpartij. Dit betekent dat de inzet van de hashdatabase niet in gevaar is. Tot slot wijs ik er op dat zowel de huidige e-privacyrichtlijn als het voorstel voor een e-privacyverordening voorzien in de mogelijkheid om bij nationale wetgeving te voorzien in uitzonderingen op het communicatiegeheim ten behoeve van het voorkomen van strafbare feiten mits dit nodig, passend en proportioneel is. Voor wat betreft de aanpak van kinderpornografische inhoud overweeg ik samen met de Minister van Justitie en Veiligheid deze optie te verkennen wanneer het aantal meldingen niet daalt als gevolg van de aangekondigde acties in het kader van de «Hernieuwde aanpak online kindermisbruik» (Kamerstuk 31 015, nr. 135).