32317 JBZ-Raad

34843 Seksuele intimidatie en geweld

Nr. 906 Brief van de minister van Justitie en Veiligheid

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 29 november 2024

Tijdens het debat over de JBZ-Raad, op 9 oktober jl., is met uw Kamer gesproken over de Verordening ter bestrijding van online seksueel kindermisbruik, ook wel de ‘CSAM-Verordening’ genoemd, waarvan het zogeheten ‘detectiebevel’ een veelbesproken onderdeel is. In deze brief informeert het kabinet uw Kamer nader over de stand van zaken met betrekking tot deze Verordening naar aanleiding van de motie-Kathmann c.s., die op 9 oktober is ingediend en op dezelfde datum door uw Kamer werd aangenomen.[1]

Het Hongaarse voorzitterschap streeft nog steeds naar het bereiken van een algemene oriëntatie over deze Verordening. Om die reden is het de verwachting dat het voorstel voor zal liggen tijdens de JBZ-raad van 12 en 13 december. Tot dusver is vanuit het Voorzitterschap geen nieuw voorstel gedaan en het is niet de verwachting dat dit nog zal gebeuren. Verder lijkt het op dit moment niet aannemelijk dat de blokkerende minderheid voor het huidige voorstel wordt opgeheven. De positie van Nederland ten aanzien van dat voorstel is dan ook ongewijzigd: bij het inbrengen van het huidige compromisvoorstel zal Nederland zich onthouden van het innemen van een positie en dit actief kenbaar maken. Nederland wordt hiermee gerekend tot de groep landen die de algemene oriëntatie niet steunt.

Zoals ook vermeld in de brief van 1 oktober jl. geldt voor het kabinet als
uitgangspunt dat in het voorstel tot een Verordening een juiste balans wordt gevonden tussen het effectief bestrijden van kinderpornografisch materiaal en het daarmee beschermen van fundamentele kinderrechten, het zorgen voor een veilige digitale omgeving voor gebruikers, en het aan de andere kant waarborgen van fundamentele grondrechten, ook die van kinderen, zoals het beschermen van de privacy en het waarborgen van het brief- en telecommunicatiegeheim.[2] Ook moet telkens worden bezien of het

[1] Kamerstuk 32 317, nr. 891.
[2] Kamerstuk 34 843, nr. 113.

voorstel onbedoelde risico’s voor de cyberveiligheid en de digitale weerbaarheid van Nederland meebrengt.

De afgelopen tijd is met verschillende organisaties en experts gesproken over het voorstel. Het kabinet hecht er daarbij aan zich, zoals eerder op dit dossier is gedaan, breed te laten informeren door uiteenlopende organisaties en experts. Om die reden zijn in de afgelopen maand veel gesprekken gevoerd. De organisaties die zijn gesproken betreffen academici, veiligheidsdiensten, de Autoriteit online Terroristisch en Kinderpornografisch Materiaal (ATKM), de politie, het openbaar ministerie, Offlimits, het Bureau van de Nationaal Rapporteur Mensenhandel en Seksueel Geweld tegen Kinderen, het Nederlands Forensisch Instituut (NFI) en ngo’s, waaronder Amnesty International Nederland, Bits of Freedom, Cybervelig Nederland, NLdigital, Defence for Children en Terre des Hommes.

In deze brief worden de Nederlandse uitgangspunten voor de onderhandelingen in Brussel benoemd en nader toegelicht, met bijzondere aandacht voor het detectiebevel. Hiermee wordt invulling gegeven aan de motie-Kathmann c.s. Hierbij constateert het kabinet dat technische ontwikkelingen constant in beweging zijn. Het is mogelijk dat nieuwe technologische ontwikkelingen of andere relevante inzichten aanleiding kunnen geven om bestaande standpunten opnieuw te bekijken. Indien dergelijke technieken of omstandigheden zich voordoen, zal het kabinet deze nader onderzoeken.

Deze brief bevat geen aanzet voor een alternatief Europees voorstel, zoals verzocht door de motie-Kathmann. Het is binnen het huidige Europese krachtenveld niet opportuun voor Nederland om dit te bewerkstelligen.

1. Uitgangspunten

Op voorhand geldt dat Nederland het doel van de Verordening onverminderd blijft steunen. Zoals opgenomen in het regeerprogramma zet het kabinet in op nieuwe en effectievere EU-regelgeving ter voorkoming en bestrijding van seksueel misbruik van kinderen. Een Unierechtelijke aanpak van online seksueel kindermisbruik is noodzakelijk om effectief op te kunnen treden tegen de online verspreiding van dit materiaal. Dat een Verordening nodig is, staat voor Nederland niet ter discussie. Een punt van discussie zit vooral in de vraag hoe die aanpak in de Verordening moet worden vormgegeven en, meer specifiek, of en zo ja, onder welke voorwaarden een verplichtend detectiebevel daarvan onderdeel moet uitmaken.

De zorgen over het detectiebevel vallen met name uiteen in twee delen: zorgen over de privacy-inbreuken en zorgen over de digitale veiligheid.

Voor wat betreft privacy-inbreuken zal Nederland geen voorstellen ondersteunen die verplichte detectie in de privécommunicatie van alle burgers inhouden, conform het verzoek aan de regering dat is neergelegd in de voornoemde motie-Kathmann c.s. Het kabinet benadrukt dat in het laatste voorstel van het voorzitterschap het doel was het detectiebevel zo veel mogelijk te beperken tot detectie in hoog risico-diensten en onderdelen van bepaalde diensten. Tegelijkertijd is de uitkomst dat het voorgestelde compromis leidt tot zorgen omtrent zowel fundamentele rechten als digitale veiligheid. Het kabinet acht het voorgestelde compromis niet in lijn met de strekking van de motie-Kathmann c.s. en zal soortgelijke voorstellen, indien die aan de orde komen, daarom niet steunen.

Verder geldt dat geen voorstellen worden ondersteund die een verplichting inhouden tot de detectie van onbekend kinderpornografisch materiaal en grooming. De argumenten die daarvoor redengevend zijn, zijn met uw Kamer gedeeld bij brief van 8 mei 2023.[3] Naar het oordeel van Nederland is een van de redenen hiervoor dat geen technologie beschikbaar is die detectie van onbekend materiaal en grooming vorm kan geven op een wijze die proportioneel en gerechtvaardigd is. Gezien het grote aantal personen dat in de huidige voorstellen met detectie te maken kunnen krijgen, gaat een hogere foutmarge gepaard met een privacy-inbreuk die naar het oordeel van het kabinet te groot is.

De zorgen met betrekking tot end-to-end-encryptie en client side scanning betreffen ook de digitale veiligheid. Het kabinet zal geen voorstellen ondersteunen die de verplichting inhouden om detectie te laten plaatsvinden door middel van client-side scanning of die, bij de huidige stand van de technologie, uitsluitend op die wijze kunnen worden uitgevoerd. Zoals uw Kamer weet, stelt de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) dat inzet van client-side scanning binnen de context van het detectiebevel een te groot risico met zich meebrengt voor de digitale weerbaarheid. Het kabinet heeft dit advies nader bestudeerd en besproken met andere organisaties en experts. Daarbij is met name bezien of het aanscherpen van de criteria waaronder een detectiebevel kan worden uitgevaardigd, bijvoorbeeld door die toe te spitsen op individuen, de bezwaren ten aanzien van client-side scanning zouden doen opheffen. De conclusie is op dit moment dat dit niet het geval is en dat nadere bestudering van dit probleem veel tijd zal kosten. Een belangrijk aspect van de problematiek rondom

[3] Kamerstuk 26 643, nr. 1022.

digitale weerbaarheid is het feit dat, hoe gericht een bevel tegen een hoog risico-dienst ook zal zijn, de uitvoering daarvan in vrijwel alle gevallen vereist dat op het apparaat van een groot aantal gebruikers de toepassing (lees: de app) van de betreffende hoog risico-dienst aangepast wordt, zodat client-side scanning binnen deze toepassing mogelijk wordt gemaakt. Hiermee wordt het risico voor de digitale weerbaarheid te groot. Indien de gerichtheid van het bevel zodanig wordt toegespitst dat dit zich richt tegen individuen en niet tegen groepen, dan gaat dit het doel (én de gekozen wettelijke grondslag) voor deze Verordening – een bestuursrechtelijke aanpak van grote hoeveelheden kinderpornografisch materiaal – voorbij. Tegen die achtergrond zal het kabinet met de informatie die nu voorhanden is, geen voorstellen over verplichte detectie ondersteunen die in de praktijk uitsluitend kunnen worden uitgevoerd door middel van client-side scanning.

Naar aanleiding van het advies van de AIVD is nader onderzoek nodig om te bezien of er alternatieven mogelijkheden zijn die technisch en juridisch voldoende waarborgen bieden voor de veiligheid en de privacy van burgers. Hierbij constateert het kabinet dat het technische veld voortdurend in beweging is. Nieuwe technologische ontwikkelingen of andere relevante inzichten kunnen aanleiding geven om bestaande standpunten opnieuw te bekijken. Indien dergelijke technieken of omstandigheden zich voordoen, zal het kabinet deze nader onderzoeken en de Kamer hierover informeren. Vooralsnog bestaat te weinig zekerheid om te kunnen concluderen dat een voldoende veilige manier beschikbaar is om vorm te geven aan alternatieve mogelijkheden. Het onmogelijk maken van end-to-end encryptie is niet aan de orde. Het kabinet komt daarmee tot de conclusie dat het thans geen ruimte ziet om in te stemmen met voorstellen die tot detectie verplichten in end-to-end versleutelde omgevingen door middel van client-side scanning. Eventuele alternatieve oplossingen vergen nader onderzoek.

2. Verdere aandachtspunten en ontwikkelingen

De vraag die daarmee rest, is of het kabinet ruimte ziet voor het ondersteunen van voorstellen inhoudende de verplichte detectie in andere omgevingen, namelijk in niet-versleutelde communicatiediensten of op hosting servers. Op dit moment is bekend dat internetbedrijven (vrijwillig) detectie in deze omgevingen reeds toepassen en dat dit effectief leidt tot het melden van materiaal en het verwijderen daarvan. De vraag die aan de orde is, is of bedrijven hier dan ook toe moeten worden verplicht en zo ja, onder welke voorwaarden. Deze vraag wordt momenteel door het kabinet nader bestudeerd.

Ten aanzien van de verplichte detectie in berichtendiensten die geen gebruik maken van end-to-endencryptie geldt dat het kabinet minimaal wenst dat de criteria waaronder het bevel tot detectie kan worden uitgevaardigd meer worden toegespitst op specifieke, afgebakende groepen en voldoende grondrechtelijke en veiligheidswaarborgen bieden. Het kabinet is tegelijk van mening dat een op individuen toegespitst detectiebevel moeilijk werkbaar is, te beperkt en bovendien te zeer overlapt met strafvorderlijke bevoegdheden – waarvan in dit geval nadrukkelijk geen sprake is. Op basis van de nadere informatie die de komende tijd wordt ingewonnen, maakt het kabinet de afweging of deze vorm van verplichte detectie mogelijk is op een manier waarmee de gemaakte grondrechteninbreuk kan worden gerechtvaardigd alsmede of dit voldoende waarborgen biedt op het terrein van cyberveiligheid en digitale weerbaarheid.

3. Conclusie

Op grond van het bovenstaande concludeert het kabinet dat de voorstellen voor verplichte detectie op dit moment niet ondersteund kunnen worden of nadere bestudering vergen. De zorgen van het kabinet over de bescherming van in het geding zijnde fundamentele grondrechten, met name op het gebied van de privacy en het brief- en telecommunicatiegeheim, en de veiligheid van het digitale domein zijn op dit moment onvoldoende weggenomen. De techniek is in ontwikkeling en er is nog weinig studie naar gedaan. Met het oog op de noodzakelijke zorgvuldigheid is meer tijd nodig om het Nederlandse standpunt op dit aspect nader te concretiseren en in te vullen.

De minister van Justitie en Veiligheid,
D.M. van Weel