Ministerie van Justitie en Veiligheid

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding
Cybercrime en zeden

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Datum
30 september 2024

Onze referentie
5813750

Bijlage(n)
0

nota

Beslisnota bij Kamerbrief inzake kabinetsstandpunt EU-Verordening ter bestrijding van online seksueel kindermisbruik

1. Aanleiding

Op 9 september jl. heeft het Hongaarse voorzitterschap een compromisvoorstel gedaan ten aanzien van de EU-Verordening dat ziet op de bestrijding van online seksueel kindermisbruik ('CSAM-Verordening'). In deze brief neemt het kabinet een standpunt in over het compromisvoorstel ten behoeve van de in de EU Raad te kiezen positie in aanloop naar het bereiken van een algemene oriëntatie over de verordening, zodat de Raad die wel of niet voor de onderhandelingen kan doorsturen naar het Europees Parlement voor de zogeheten 'triloogfase'. De brief besteedt aandacht aan de verschillende aspecten die tegen elkaar moeten worden afgewogen bij het innemen van een standpunt ten aanzien van de EU-Verordening en schetst de dilemma's die daarbij rijzen. Het voorzitterschap streeft ernaar tijdens de Coreper-vergadering van 2 oktober en de JBZ-Raad van 10/11 oktober 2024 de algemene oriëntatie te bereiken. Het betreft dus geen stemmingen over de Verordening zelf.

2. Geadviseerd besluit

U wordt geadviseerd om in te stemmen met bijgaande Kamerbrief.

3. Kernpunten

- In de brief wordt aandacht besteed aan de historie van de Nederlandse positie. Op 11 mei 2022 heeft de Europese Commissie een voorstel gepubliceerd voor een verordening betreffende voorschriften ter voorkoming en bestrijding van seksueel kindermisbruik (hierna: CSA (Child Sexual Abuse). Op 17 juni 2022 is er een BNC-fiche in reactie op het voorstel naar de Kamer gestuurd.
- Het voorstel creëert nieuwe verplichtingen voor aanbieders van hostingdiensten en interpersoonlijke communicatiediensten, onder andere om het risico te beoordelen dat hun diensten worden gebruikt voor het verspreiden van materiaal van CSA en het benaderen van kinderen voor seksuele doeleinden (grooming) of om materiaal te verwijderen. Onder bepaalde omstandigheden kunnen deze bedrijven ook worden verplicht om materiaal van CSA te detecteren op hun dienst.
- Vervolgens wordt ingegaan op het compromisvoorstel. Op 9 september jl. hebben de lidstaten van het Hongaarse voorzitterschap een compromisvoorstel ontvangen. Het voorzitterschap stelt in zijn compromisvoorstel voor de scope van het detectiebevel in de Verordening – voor het eerst – te beperken tot het detecteren van bekend kinderpornografisch materiaal; detectie op nieuw CSA materiaal en *grooming* zijn als zodanig verwijderd uit de scope van de Verordening. Het beperken van deze scope is een stap die tegemoetkomt aan een van de grootste bezwaren die door Nederland gedurende het

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding
Cybercrime en zeden

Datum
30 september 2024

Onze referentie
5813750

onderhandelingsproces naar voren zijn gebracht. Nederland heeft hiervoor in Brussel haar erkentelijkheid uitgesproken, maar tegelijkertijd benoemd dat als gevolg van de recente kabinetswissel, politieke besluitvorming nog in voorbereiding is.
- Bij de vraag welke positie Nederland ten aanzien van het voorstel moet innemen is er zowel aandacht geweest voor de complexe inhoudelijke belangenafweging als voor de positie van ons land in het Europese krachtenveld.
- Nederland erkent de urgentie van de bestrijding van kinderpornografisch materiaal volledig en is voorstander van effectieve EU-regelgeving voor het tegengaan van de verspreiding van kinderpornografisch materiaal. Tegelijkertijd is het kabinet van mening dat er op dit moment onvoldoende duidelijk is over de impact van de voorgestelde maatregelen. 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.
- Het kabinet heeft daarom besloten om zich te onthouden van het innemen van een positie en dit actief kenbaar te maken. Nederland zal daarmee worden gerekend tot de landen die de algemene oriëntatie niet steunen.

4. Toelichting

Het vorige kabinet heeft als standpunt ingenomen dat Nederland alleen kan instemmen met een detectiebevel indien een dergelijk bevel niet de detectie van nieuw materiaal of grooming omvat, omdat detectie van dit materiaal bij de huidige stand van de techniek niet op een proportionele manier kan worden uitgevoerd. Alleen ten aanzien van de detectie van reeds bekend materiaal kan een dergelijk bevel worden uitgevoerd op een wijze die proportioneel is (via *hashing*-technologie). Omdat het kabinet geen maatregelen ondersteunt die end-to-end-encryptie onmogelijk maken, is de enige wijze waarop dit bevel kan worden uitgevoerd bij end-to-end-versleutelde diensten via client-side scanning. Het vorige kabinet heeft uitdrukkelijk met de Kamer gecommuniceerd dit als een optie te zien.

Op basis van dit standpunt heeft JenV in eerste instantie een positieve grondhouding ingenomen ten aanzien van het Hongaarse voorstel. Het detectiebevel is in dit voorstel namelijk in grote mate beperkt, onder meer naar aanleiding van de kritiek dat eerdere voorstellen een niet-gerechtvaardigde inbreuk maakten op het recht op privacy en het brief- en telecommunicatiegeheim.

Naar aanleiding van het voorstel heeft overleg plaatsgevonden met betrokken bewindspersonen. Vorige week is naar aanleiding van een nieuw advies van de AIVD de positie ten opzichte van het compromisvoorstel opnieuw bezien.

De AIVD waarschuwt dat '*het introduceren van een scan applicatie op elke mobiele telefoon met een daarbij horende infrastructuur van beheersystemen een uiterst omvangrijk en complex systeem oplevert. Dit complexe systeem heeft daarbij toegang tot een grote hoeveelheid mobiele devices en de persoonlijke gegevens daarop. Dit resulteert uiteindelijk in een situatie waarvan de AIVD de risico's voor de digitale weerbaarheid te groot acht*.'

De verordening schrijft geen specifieke methode voor om detectie uit te voeren; een dienstverlener kan, indien een bevel wordt gegeven, zelf de manier kiezen waarop op CSA materiaal binnen de verleende dienst wordt gedetecteerd. Indien een detectiebevel wordt opgelegd aan een dienstverlener die gebruik maakt van end-to-end encryptie is de inschatting van de AIVD dat detectie van kinderpornografisch materiaal middels client-side scanning een te groot veiligheidsrisico voor de digitale weerbaarheid van Nederland met zich meebrengt.

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding
Cybercrime en zeden

Datum
30 september 2024

Onze referentie
5813750

Het advies beschrijft tevens alternatieve mogelijkheden ("de enige zinnige manier"), waarbij het scannen van gegevens op een wijze kan plaatsvinden die de strikte definitie van end-to-end-encryptie loslaat. Daarbij wordt verwezen naar de wijze waarop dit is vormgegeven bij aanbieders van openbare telecommunicatienetwerken (deze hebben een verplichting aftapbaar te zijn en de informatie zonder eigen encryptie aan te leveren). Deze mogelijkheid is verder niet uitgewerkt en is niet in lijn met de motie-Van Raan[1].

Het advies van de AIVD en de opmerkingen over alternatieven behoeven nadere bestudering. Gezien de korte tijd is een zorgvuldige afweging hierover niet mogelijk, mede gezien de brede afstemming die dit zou vereisen. Wel is duidelijk dat de veiligheidsrisico's die door de AIVD worden genoemd ten aanzien van client side scanning, maken dat het maar zeer de vraag is of de grondrechteninbreuk kan worden gerechtvaardigd, omdat voor wat betreft die methode geen sprake is van een proportioneel middel. Deze zorgen zijn mondeling met u besproken voorafgaand aan de MR.

In eerste instantie bent u geadviseerd om geen positie in te nemen over de algemene oriëntatie en deze derhalve niet te blokkeren, en daarbij te benoemen dat voor Nederland in de verdere onderhandelingen nog een aantal zorgen weggenomen moeten worden.

Na meerdere besprekingen in het kabinet zijn alle bovenstaande overwegingen in acht genomen. Hierbij is zowel aandacht geweest voor de complexe inhoudelijke belangenafweging als voor de positie van ons land in het Europese krachtenveld. Zorgen 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. Daarom is in het kabinet besloten om zich te onthouden van het innemen van een positie en dit actief kenbaar te maken. Nederland zal daarmee worden gerekend tot de landen die de algemene oriëntatie niet steunen.

4.1. Politieke context

Regeerprogramma 2024
In het regeerprogramma 2024 staat het volgende opgenomen over dit onderwerp: "De aanpak van seksueel kindermisbruik wordt binnen de bestaande financiële kaders geïntensiveerd. Daarom is het onverminderd voortzetten van de aanpak een prioriteit voor dit kabinet en wordt bezien of er extra stappen gezet kunnen worden. Daarbij is er aandacht voor de veranderende belevingswereld van kinderen en jongeren, die zich voor een groot deel online afspeelt. We zetten daarom in op nieuwe en effectievere EU-regelgeving ter voorkoming en bestrijding van seksueel misbruik van kinderen. Ook continueren we de strafrechtelijke en bestuursrechtelijke aanpak, onder meer via de Autoriteit online Terroristisch en Kinderpornografisch Materiaal (ATKM)."

Schriftelijke Kamervragen NSC en GL-PvDA
Op 6 september jl. hebben de leden Six Dijkstra (Nieuw Sociaal Contract) en Kathmann (GroenLinks-PvdA) u schriftelijke Kamervragen gestuurd naar aanleiding van het Hongaarse voorstel. Beantwoording van deze vragen kan worden geconcipieerd nadat een kabinetsstandpunt is bepaald.

Verzoek Vaste Commissie Digitale Zaken
De Vaste Commissie voor Digitale Zaken van de Tweede Kamer heeft tijdens de procedurevergadering van 11 september jl. het kabinet verzocht om binnen drie werkdagen een brief te sturen over het kabinetsstandpunt over de CSAM-

[1] Kamerstukken II 2021/22, 26643, nr. 885.

Verordening. Omdat dit standpunt nog bereikt moest worden, is de Kamer alleen procesmatig geïnformeerd. De brief is verstuurd op 16 september jl.

Verzoek Vaste commissie Justitie en Veiligheid
De vaste commissie voor Justitie en Veiligheid heeft u op 26 september jl. verzocht de Kamer actief te informeren over de besluitvorming inzake de CSAM-verordening. De commissie verzoekt u tevens om bij het doen toekomen van het kabinetsstandpunt inzake de CSAM-verordening aan de Kamer, de (ambtelijke) adviezen toe te voegen. Momenteel wordt bezien welke ambtelijke adviezen, voor zover niet staatsgeheim, met de Tweede Kamer kunnen worden gedeeld.

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding
Cybercrime en zeden

Datum
30 september 2024

Onze referentie
5813750

4.2. Krachtenveld
Met betrekking tot de positie in het krachtenveld van de Europese Unie geldt dat er een grote groep lidstaten is die dit voorstel kan steunen en tot een algemene oriëntatie wil komen. Tegelijk bestaat ook een kleine groep kritische lidstaten die het huidige voorstel nog niet kan steunen. Zou er nu geen algemene oriëntatie kunnen worden bereikt, dan zal het voorzitterschap moeten werken aan een nieuw voorstel. Komt er wel een algemene oriëntatie, dan is het de verwachting dat naar de huidige omstandigheden het voorstel naar het Europees Parlement kan worden doorgestuurd. Pas na afloop van deze onderhandelingsfase wordt over de Verordening gestemd.

5. Informatie die niet openbaar gemaakt kan worden

5.1. Toelichting
De persoonsgegevens van de ambtenaren zijn niet openbaar ter bescherming van de persoonlijke levenssfeer.