

Beantwoording SO JBZ 13-14 oktober (niet-geagendeerd)

3317-772 JBZ-Raad op 13 en 14 oktober 2022

Verslag van een schriftelijk overleg

Binnen de vaste commissie voor Justitie en Veiligheid hebben de onderstaande fracties de behoefte vragen en opmerkingen voor te leggen aan de minister van Justitie en Veiligheid en de minister voor Rechtsbescherming over de volgende stukken:

- Geannoteerde agenda van de JBZ-Raad van 13 en 14 oktober 2022 (Kamerstuk 32317, nr. 772)
- Verslag van de informele JBZ-Raad van 11-12 juli 2022 (Kamerstuk 32317, nr. 771)
- Voorstel over het aanmerken van overtredingen van EU-sanctiemaatregelen als EU-misdrijf (Kamerstuk 22112, nr. 3473)
- Fiche: Richtlijn Ontneming en confiscatie van vermogensbestanddelen (Kamerstuk 22112, nr. 3467)
- Geannoteerde agenda van de informele JBZ-Raad van 11 en 12 juli 2022 (Kamerstukken 32317, nr. 767 en 32317, nr. 770)

De op 10 oktober 2022 toegezonden vragen en opmerkingen zijn met de door de minister van Justitie en Veiligheid en de minister voor Rechtsbescherming bij brief van 21 oktober toegezonden antwoorden hieronder afgedrukt.

De voorzitter van de commissie,

Van Meenen

Adjunct-griffier van de commissie,

Nouse

Vragen en opmerkingen vanuit de fracties en reactie van de bewindspersonen

I. Vragen en opmerkingen van de leden van de VVD-fractie

De leden van de VVD-fractie hebben met belangstelling kennisgenomen van de geannoteerde agenda van de JBZ-raad van 13-14 oktober a.s.. Deze leden maken van de gelegenheid gebruik nog enkele vragen te stellen aan de ministers.

Verordening tegengaan online seksueel misbruik van kinderen

De leden van de VVD-fractie lezen dat de kaders uit het kabinetsstandpunt leidend zijn voor de Nederlandse inbreng ten aanzien van encryptie. Deze leden zijn het met de minister eens en zouden niet willen dat aan encryptie getornd wordt. Hoe ziet het Europees krachtenveld eruit gelet op het behoud van encryptie?

Antwoord

De lidstaten hebben een overwegend positieve houding ten opzichte van het voorstel van de Europese Commissie (Commissie). De lidstaten zien de noodzaak van een Europese aanpak om (online) seksueel kindermisbruik tegen te gaan. Op dit moment wordt onderhandeld over het voorstel en worden de bepalingen nauwkeurig en kritisch gezien. Daarbij wordt ook gekeken naar de effecten van het detectiebevel op end-to-end encryptie. Er zijn zowel lidstaten die van mening zijn dat end-to-end encryptie niet mag worden verzwakt als lidstaten die vinden dat end-to-end encryptie niet in de weg mag staan van de werking van de verordening. De Commissie meent dat end-to-end encryptie niet onmogelijk wordt gemaakt door het voorstel. Dit wordt momenteel grondig bestudeerd.

II. Vragen en opmerkingen van de leden van de D66-fractie

De leden van de D66-fractie hebben met belangstelling kennisgenomen van de stukken op de agenda en hebben nog enkele vragen.

Verordening tegengaan online seksueel misbruik van kinderen

De leden van de D66-fractie hebben met interesse kennisgenomen van het BNC-fiche en de technische briefing over de Verordening tot vaststelling van regels ter voorkoming en bestrijding van online seksueel misbruik van kinderen. Deze leden onderschrijven de noodzaak van een gezamenlijke aanpak om het verschrikkelijke fenomeen van online seksueel kindermisbruik aan te pakken. Zij juichen toe dat er verplichtingen komen voor aanbieders van hostingdiensten en interpersoonlijke communicatiediensten tot risicobeoordeling en risico beperkende maatregelen. Ook zien zij de meerwaarde van een EU-expertisecentrum. Zij hebben hierover nog wel enkele vragen.

Welke maatregelen worden nu al door aanbieders van hostingdiensten en interpersoonlijke communicatiediensten genomen om online kindermisbruik tegen te gaan? Worden met dit voorstel (naast verplichtingen) ook beperkingen opgelegd aan bedrijven in methodes die zij nu toepassen? Hoe kijkt de minister hier tegenaan? Biedt het voorstel volgens de minister ook voldoende mogelijkheden voor webproviders om preventieve maatregelen te nemen?

De leden van de D66-fractie delen de zorgen van de minister dat een deel van de maatregelen in het voorstel de veiligheid van het internetverkeer juist zou kunnen schaden. Zij onderschrijven de inzet van de minister om geen maatregelen te steunen die end-to-end-encryptie onmogelijk maken. Kan de minister toelichten hoe zij zich in de JBZ-Raad zal inspannen om te waarborgen dat er niet aan end-to-end-encryptie gesleuteld wordt? Welke lidstaten delen deze zorgen? Gaat Nederland samen met hen optrekken om oplossingsrichtingen aan te dragen?

Antwoord

In december 2020 is de Europese code voor elektronische communicatie van toepassing geworden. Per die datum omvat het begrip communicatiedienst ook nummeronafhankelijke interpersoonlijke communicatiediensten. Sindsdien vallen ook nummeronafhankelijke interpersoonlijke communicatiediensten onder het bereik van de e-privacyrichtlijn.¹ Onder de e-privacyrichtlijn is het voor bedrijven niet mogelijk om op vrijwillige basis materiaal van online seksueel kindermisbruik te detecteren. Om ervoor te zorgen dat bedrijven op vrijwillige basis konden blijven zoeken naar materiaal van online seksueel kindermisbruik is met Verordening 2021/1232 op dit punt voorzien in een tijdelijke afwijking van de e-privacyrichtlijn.² Op dit moment kunnen bedrijven dus nog wel vrijwillige maatregelen nemen in de aanpak van online seksueel kindermisbruik. Bedrijven kunnen bijvoorbeeld gebruik maken van een hashdatabase om bekend materiaal van de seksueel kindermisbruik te detecteren.

De tijdelijke Verordening 2021/1232 vervalt na 3 augustus 2024. Op dat moment is het voor deze aanbieders niet meer mogelijk om op vrijwillige basis te detecteren. De thans voorgestelde verordening van de Commissie ter voorkoming en bestrijding van seksueel misbruik van kinderen moet de tijdelijke Verordening 2021/1232 opvolgen. De voorgestelde verordening biedt geen grondslag voor vrijwillige detectie door aanbieders van interpersoonlijke communicatiediensten. De voorgestelde verordening biedt wel een rechtsgrondslag voor het uitvoeren van een detectiebevel door een rechterlijke autoriteit of onafhankelijke administratieve autoriteit, waarmee aanbieders verplicht worden om materiaal van seksueel kindermisbruik te detecteren. Op grond van de voorgestelde verordening kan alleen na een zorgvuldig proces een detectiebevel worden opgelegd wanneer het noodzakelijk, evenredig en met de nodige waarborgen omkleed is.

In de besprekingen in de JBZ-Raad over de voorgestelde verordening zal Nederland het standpunt uitdragen dat het een voorstel dat end-to-end encryptie onmogelijk maakt niet kan steunen. Nederland sluit zich op dit punt aan bij lidstaten met een gelijklopende opvatting.

PNR-richtlijn

De leden van de D66-fractie hebben kennisgenomen van het recente arrest van het Europees Hof over de PNR-richtlijn, waarin de condities voor het gebruik van de PNR-richtlijn op vluchten binnen de EU zijn aangescherpt. Kan de minister toelichten welke implicaties dit arrest heeft voor de implementatie van de PNR-richtlijn in Nederland?

Antwoord

Het Hof heeft geoordeeld dat de richtlijn in het licht van het EU-Grondrechtenhandvest

¹ Richtlijn 2002/58/EG van het Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie), PbEU, L. 201/37.

² Verordening 2021/1232 betreffende een tijdelijke afwijking van sommige bepalingen van Richtlijn 2002/58/EG ten aanzien van het gebruik van technologieën door aanbieders van nummeronafhankelijke interpersoonlijke communicatiediensten voor de verwerking van persoonsgegevens en andere gegevens ten behoeve van de bestrijding van online seksueel misbruik van kinderen, PbEU 2021, L274.

overeind blijft. Volgens het Hof vereisen de grondrechten dat de bevoegdheden waarin de PNR-richtlijn voorziet slechts worden uitgeoefend voor zover dat strikt noodzakelijk is. Het Hof heeft zich daarbij ook uitgesproken over de toepassing van de richtlijn op vluchten binnen de EU. Deze uitspraak van het Hof wordt momenteel door lidstaten bestudeerd op de consequenties voor de operatie van de verschillende passagiersinformatie-eenheden en de onderliggende nationale wetgeving. Het kabinet acht het van cruciaal belang de gevolgen van de uitspraak van het Hof gezamenlijk vanuit Europees perspectief te adresseren zodat een sterke informatiepositie van de verschillende lidstaten in de strijd tegen terrorisme en ernstige criminaliteit kan worden gehandhaafd en het zorgvuldig samengestelde systeem van privacywaarborgen dat de PNR-richtlijn omvat kan worden gegarandeerd. Per brief van 30 juni jl. heeft de minister van Justitie en Veiligheid toegezegd zich daar de komende periode in Europa actief voor in te zetten.³ Sinds de uitspraak benadrukt Nederland in Brussel op verschillende niveaus de urgentie en het belang van een EU-brede aanpak, waarbij de uitspraak van het Hof als uitgangspunt wordt genomen. In samenwerking met andere lidstaten, het Voorzitterschap en de Commissie wordt bezien welke oplossingsrichtingen hier recht aan doen.

IV. Vragen en opmerkingen van de leden van de SP-fractie

Verordening ter voorkoming en bestrijding van seksueel kindermisbruik

De leden van de SP-fractie hebben bij het vorige schriftelijke overleg over de JBZ-Raad uitgebreid stilgestaan bij de plannen voor de aanpak en het voorkomen van seksueel kindermisbruik en online kinderlokken. Vorige week vond tevens een technische briefing plaats over dit onderwerp. De leden van de SP-fractie hebben hier nog vragen over.

De leden van de SP-fractie willen vooraf benadrukken dat zij zich al jaren lang druk maken over de online verspreiding van materiaal van seksueel kindermisbruik. Het Expertisebureau Online Kindermisbruik (EOKM) speelt daarvoor in Nederland een belangrijke rol. Deze leden hebben in het verleden daarom meerdere keren voorgesteld om het EOKM beter te financieren en beter opvolging te geven aan verwijderingsverzoeken van het EOKM. Ook hebben zij diverse keren aandacht gevraagd over de verantwoordelijkheid van online aanbieders. Toch zijn er nog veel vragen over het voorliggende voorstel. Het EOKM noemt deze plannen bijvoorbeeld niet proportioneel

Ook het BNC-fiche van de regering is vrij kritisch. Zo lazen de leden van de SP-fractie dat de minister zorgen heeft over aspecten die een grote inbreuk lijken te maken op het recht op privéleven, het recht op gegevensbescherming en het communicatiegeheim van burgers. Daarnaast geeft de minister aan kritisch te zijn op het onderdeel van het detectiebevel en het opheffen van anonimiteit op het internet. Uit het verslag over de JBZ-bijeenkomst van juli jl.? blijken deze zorgen echter niet. Kan de minister nog eens toelichten wat Nederland nu precies heeft ingebracht? En met welke ambitie? Is dat in gezamenlijkheid met andere landen? Deze leden willen dat de kritiek uit Den Haag ook in Brussel goed over het voetlicht wordt gebracht.

De leden van de SP-fractie hebben nog diverse vragen over de inhoud. Zo werd tijdens de technische briefing aangegeven door de politie dat er geen capaciteit is om alle meldingen op te volgen. Hoe kijkt de minister hiernaar? Is deze verordening een dode letter?

³ Kamerstukken II, vergaderjaar 2021-2022, Kamerstuk 29754, nr. 644, d.d. 30 juni 2022.

Daarnaast is er veel onduidelijk over het detectiebevel. Wanneer de nationale autoriteit zorgen heeft over het aanbieden van materiaal kunnen diensten worden verplicht om de inhoud te scannen. De EC schrijft echter geen technologie voor. Bestaat hiervoor eigenlijk wel de juiste technologie? Welke foutmarge is daarbij acceptabel? Kan de minister toezeggen dat er altijd een check door een persoon verricht gaat worden wanneer materiaal verwijderd wordt?

In voorbereiding op de vorige JBZ-Raad schreef de minister dat diensten data gaan verzamelen over de identiteit van gebruikers. Dit is risicovol. Kan de minister dat verder toelichten? Kan de minister, wellicht aan de hand van een voorbeeld, uiteenzetten wat precies de plannen zijn?

De leden van de SP-fractie willen ook graag stilstaan bij ontsleuteling. Wanneer kan de Kamer de antwoorden op al haar vragen tegemoet zien? Wat wordt ermee bedoeld dat Nederland de voorstellen op ontsleuteling niet steunt? Hoe gaat Nederland andere lidstaten van het belang van end-to-end-encryptie overtuigen?

De ambitie om de verspreiding van materiaal van seksueel kindermisbruik tegen te gaan wordt vanzelfsprekend gedeeld. Er is echter nog onvoldoende helder over de waarborgen en de gevolgen van het voorstel. De leden van de SP-fractie spreken de hoop uit dat dat de bovenstaande punten opgehelderd kunnen worden voordat een deal wordt bereikt op dit voorstel.

Antwoord

In de JBZ-Raad heeft Nederland het belang onderstreept van het beschermen van kinderen en het kunnen optreden tegen seksueel kindermisbruik. In sommige gevallen kan dit echter een inbreuk vormen op bepaalde grondrechten. Dit kan alleen als de maatregel strikt noodzakelijk en proportioneel is en is voorzien van de juiste waarborgen. De Commissie heeft enkele voorbeelden genoemd van mogelijkheden waarmee materiaal dat seksueel kindermisbruik bevat kan worden gedetecteerd. Via het BNC-fiche is uw Kamer geïnformeerd dat nog onduidelijkheid bestaat over de gevolgen van deze voorstellen voor de versleuteling van berichten, de inbreuk op de privacy en het brief- en telecommunicatiegeheim. Daarom neemt het kabinet een vragende maar kritische houding aan. In de onderhandelingen over de voorgestelde verordening zal duidelijk worden gemaakt dat Nederland voorstellen die end-to-end encryptie onmogelijk maken niet steunt, conform hetgeen met uw Kamer gecommuniceerd over de uitvoering van de door uw Kamer aangenomen motie-Van Raan c.s. Daarbij zal, samen met lidstaten met een gelijklopende opvatting, worden gezocht naar oplossingen die recht doen aan de wens om op een proportionele en effectieve manier online seksueel kindermisbruik aan te pakken. De verschillende mogelijkheden zullen inhoudelijk zorgvuldig worden beoordeeld.

Het voorstel richt zich in eerste instantie op administratieve handhaving en de aanbieders van hostingdiensten en interpersoonlijke communicatiediensten. De Coördinerende Autoriteit krijgt de bevoegdheid om een gerechtelijke autoriteit of een onafhankelijke administratieve autoriteit te verzoeken een bevel uit te vaardigen om een aanbieder van hostingdiensten te verplichten materiaal van seksueel kindermisbruik op zijn diensten te verwijderen of ontoegankelijk te maken. De politie is in dit proces nog niet betrokken. Als aanbieders van hostingdiensten of interpersoonlijke communicatiediensten kennis hebben gekregen van mogelijk online seksueel kindermisbruik op of via hun diensten worden zij verplicht om dit te melden aan het EU-centrum. Om het risico van foutieve detectie en het aantal meldingen tot een minimum te beperken zal het EU-centrum meldingen van potentieel seksueel kindermisbruik verifiëren voordat dit wordt gedeeld met rechtshandavingsinstanties en Europol, op dat moment komt de politie in beeld.

Er zijn diverse technologieën beschikbaar die nauwkeurig worden bestudeerd in het licht van deze verordening. Een voorbeeld van een technologie die nu al in Nederland wordt

gebruikt voor vrijwillige detectie is via een hashdatabase. Bij bestudering van de technologieën wordt ook gekeken naar de foutmarge. In de technische briefing is reeds aangegeven dat de foutmarge van een specifieke technologie afhankelijk is van de instellingen waarbij de verwachting is dat bij een kleiner foutmarge minder materiaal wordt gedetecteerd en vice versa.

Aanbieders van hostingdiensten of interpersoonlijke communicatiediensten moeten controles om het misbruikrisico van hun diensten te beoordelen op anonieme basis laten plaatsvinden. Er kunnen alleen stappen worden ondernomen om gebruikers te identificeren indien mogelijk materiaal van seksueel kindermisbruik wordt geconstateerd. De gebruikte technologie zou dus geen andere informatie kunnen verzamelen dan wat strikt noodzakelijk is om het misbruik op te sporen. Aanbieders van hostingdiensten of interpersoonlijke communicatiediensten moeten tevens alle noodzakelijke maatregelen nemen om ervoor te zorgen dat persoonsgegevens uitsluitend worden gebruikt voor het opsporen van de verspreiding van bekend of nieuw materiaal van seksueel kindermisbruik of de benadering van kinderen voor seksuele doeleinden.