Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2024–2025

34 843 Seksuele intimidatie en geweld

Nr. 114

LIJST VAN VRAGEN EN ANTWOORDEN

Vastgesteld 8 oktober 2024

De vaste commissie voor Justitie en Veiligheid heeft een aantal vragen voorgelegd aan de Minister van Justitie en Veiligheid over de brieven Positie Nederland ten aanzien van de CSAM-Verordening (Kamerstuk 34 843, nr. 113) en Kabinetsstandpunt inzake de CSAM verordening en de uitvoering van de moties Van Ginneken c.s. (Kamerstuk 26 643, nr. 1011) en Dekker Abdulaziz c.s. (Kamerstuk 32 317, nr. 856) (Kamerstuk 34 843, nr. 112).

De Minister heeft deze vragen beantwoord bij brief van 8 oktober 2024. Vragen en antwoorden zijn hierna afgedrukt.

De voorzitter van de commissie,
Pool

Adjunct-griffier van de commissie,
Paauwe

kst-34843-114
ISSN 0921 - 7371
's-Gravenhage 2024

1
Is er een scenario denkbaar dat Nederland voor het voorstel zal stemmen zonder dat de impact precies duidelijk is, aangezien het kabinet stelt dat er op dit moment onvoldoende duidelijk is over de impact van de voorgestelde maatregelen?

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. Nederland is niet het enige land dat op dit moment niet kan instemmen; daarom heeft het Hongaarse voorzitterschap er voor gekozen om besluitvorming over de verordening van de agenda van de JBZ-Raad te halen.

2
Laat Nederland in eigen beheer onderzoeken wat de mogelijke impact kan zijn? Zo nee, bent u bereid dit te doen?

Ja, Nederland heeft meer tijd nodig om duidelijkheid over de gevolgen van het voorgestelde detectiebevel te krijgen van experts. De zorgen van het kabinet over de bescherming van de met dit voorstel 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.

3
Klopt het dat het kabinet het van belang acht dat er een juiste balans wordt gevonden tussen het effectief bestrijden van kinderpornografisch materiaal en het beschermen van fundamentele kinderrechten, alsmede het aan de andere kant waarborgen van fundamentele grondrechten, zoals met name het beschermen van de privacy en het waarborgen van het brief- en telecommunicatiegeheim? Kunt u omschrijven wat u hier een juiste balans in vindt?

Ja dat klopt. Met deze passage bedoelde het kabinet aan te geven dat inperkingen van grondrechten moeten voldoen aan – in het kort – de eisen van noodzakelijkheid, proportionaliteit en subsidiariteit. Dat volgt uit het Europees Verdrag voor de Rechten van de Mens en de bijbehorende jurisprudentie. Bovendien vereist het Europees Handvest voor de Grondrechten dat inperkingen van grondrechten wel de wezenlijke inhoud van de grondrechten moeten eerbiedigen. Tot slot kent ook onze Grondwet specifieke vereisten. De inperkingen van grondrechten die de CSAM-verordening met zich brengt zullen dus moeten voldoen aan deze eisen. Het kabinet heeft daar zorgen over.

4
Kunt u duiden op welke manier de EU-verordening ter bestrijding van online seksueel kindermisbruik (CSAM-verordening) meerwaarde kan hebben op de bestaande Nederlandse opsporingsbevoegdheden?

De ontwerp EU-verordening stelt regels om ervoor te zorgen dat de verschillende aanbieders van tussenhandeldiensten meer verantwoordelijkheid nemen om de eigen diensten schoon te maken en houden van online materiaal van seksueel kindermisbruik. Voorbeelden van dergelijke diensten zijn hostingdiensten, online platforms en interpersoonlijke communicatiediensten. Niet alleen het detectiebevel is daarvoor relevant, maar ook de regels rond preventie en risicobeoordeling van deze diensten. Daarnaast biedt de ontwerpverordening uniforme regels ten aanzien van een aantal soorten bevelen, zoals verwijderbevelen. Het kan de Nederlandse opsporing helpen als er op Europees niveau afspraken worden gemaakt over het naleven van verwijderbevelen. Het helpt de opsporing om beter zicht te krijgen op de grootste verspreiders van online materiaal van seksueel kindermisbruik die gebruik maken van tussenhandeldiensten. De capaciteit en bevoegdheden kunnen dan gerichter worden ingezet. Verpreiders van kinderporno houden zich immers niet aan landsgrenzen en een efficiënte internationale samenwerking is essentieel voor het schoon houden van de online omgeving. Het voorgestelde EU Centrum voor de bestrijding van online seksueel kindermisbruik is de ontvanger van de rapportages van aanbieders van tussenhandeldiensen. Indien het Centrum van mening is dat een rapport over online seksueel kindermisbruik gegrond is stuurt zij dit door voor verder onderzoek naar dader en slachtoffers naar de relevante opsporingsdiensten.

5
Onder welke voorwaarden kan Nederland voor stemmen, als het voorstel na de onderhandelingen ter stemming voorgelegd wordt aan alle lidstaten? Onder welke omstandigheden zal Nederland tegen stemmen of zich onthouden van stemming?

Het Nederlandse standpunt over de verordening is op 1 oktober jl. met uw Kamer gedeeld. 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. Indien een nieuw of aangepast voorstel wordt voorgesteld, dan zal het kabinet dat opnieuw als geheel beoordelen.

6
Heeft u Offlimits betrokken bij de besluitvorming of haar kennis geraadpleegd als nationale autoriteit? Zo ja, wat was haar advies? Zo niet, waarom acht u dit niet nodig?

Nee, voor het Nederlandse standpunt van 1 oktober is Offlimits niet geraadpleegd. Wel is de afgelopen periode over de diverse compromisvoorstellen regelmatig contact geweest met de diverse stakeholders, waaronder Offlimits. Daarnaast heeft Offlimits op 18 september jl. een open brief aan het kabinet gestuurd. Offlimits geeft daarin aan het CSAM-voorstel dat nu op tafel ligt onnodig te vinden, dat het voorstel normaal experimenterend verkeer tussen jonge mensen criminaliseert en een grove inbreuk op privacy van mensen maakt.

7
Heeft u de Autoriteit online Terroristisch en Kinderpornografisch Materiaal (ATKM) betrokken bij de besluitvorming of haar kennis geraadpleegd als nationale autoriteit? Zo ja, wat was haar advies? Zo niet, waarom acht u dit niet nodig?

Nee, voor het Nederlandse standpunt van 1 oktober is de Autoriteit Terroristisch en Kinderpornografisch Materiaal (ATKM) niet geraadpleegd. Wel is de afgelopen periode over de diverse compromisvoorstellen regelmatig contact geweest met de diverse stakeholders, waaronder de ATKM. De bestuursvoorzitter van de ATKM heeft eerder publiekelijk haar zorgen geuit over het eerdere CSAM-voorstel.

8
Heeft u de zedenpolitie, in het bijzonder het Team ter bestrijding van Kinderpornografie en Kindersekstoerisme (TBKK), betrokken bij de besluitvorming of zijn kennis geraadpleegd als nationale autoriteit? Zo ja, wat was zijn advies? Zo niet, waarom acht u dit niet nodig?

Nee, voor het Nederlandse standpunt van 1 oktober is de zedenpolitie niet geraadpleegd. Wel is de afgelopen periode over de diverse compromisvoorstellen regelmatig contact geweest met de diverse stakeholders, waaronder de politie.

9
Heeft u juridisch advies ingewonnen over de gevolgen van de CSAM-verordening voor de onschuldpresumptie van alle Europeanen wiens privécommunicatie gescand zou worden? Zo ja, kunt u dit advies doen toekomen? Zo niet, kunt u dit alsnog doen en zo snel mogelijk doen toekomen?

Het doel van de CSAM-verordening is om de verspreiding van beelden van online seksueel kindermisbruik te stoppen en niet om de makers of verspreiders daarvan (strafrechtelijk) op te sporen. De onschuldpresumptie is een grondbeginsel in het strafrecht en deze verordening is zoals gezegd in beginsel geen strafrechtelijk instrument. Wel is uitgebreid gekeken naar de diverse grondrechten van gebruikers. Het voorstel is binnen de betrokken ministeries beoordeeld. Er is geen extern advies ingewonnen.

10
Welke externe technische en juridische experts heeft u geraadpleegd bij het formuleren van het kabinetsstandpunt?

Voor het formuleren van het huidige kabinetsstandpunt van 1 oktober zijn verschillende ministeries betrokken geweest, evenals de AIVD en het Nederlands Forensisch Instituut. Externe experts zijn niet geraadpleegd.

11
Wat is uw reactie op de verschillende open en gerichte brieven die u heeft ontvangen van private en publieke organisaties, met zorgen over de verordening? Heeft u deze meegenomen in uw overwegingen?

De binnengekomen brieven van private en publieke organisaties zijn mij bekend. Het betreft brieven van zowel de voor- als tegenstanders van het voorstel. Een deel van de zorgen die door

zowel voor- als tegenstanders zijn geuit, worden door het kabinet onderschreven en zijn meegewogen in de overwegingen.

12
Bent u bekend met het advies van 26 april 2023 van de Juridische Dienst van de Raad van Europa, waarin zorgen worden geuit over de proportionaliteit en technische onderbouwing van de CSAM-verordening? Wat betekent dit voor de technische en juridische houdbaarheid van het voorstel?

Ja, daar ben ik mee bekend. Nederland is een van de lidstaten die (veelvuldig) om dit advies van de Juridische Dienst van de Raad van de Europese Unie (JDR) heeft gevraagd. Het advies onderschrijft dat een detectiebevel voor onbekend materiaal en *grooming* op dit moment met de huidige beschikbare technologie, kort samengevat, niet proportioneel kan zijn. Dit was mede reden voor Nederland om niet te kunnen instemmen met een detectiebevel voor onbekend materiaal en *grooming*. Voor bekend materiaal kan uit het advies van de JDR worden geconcludeerd dat er onder scherpe voorwaarden wel mogelijkheden zijn om dit materiaal te detecteren. De belangrijkste zorg van de JDR zat met name in de gerichtheid van het detectiebevel van het voorstel zoals dit voorlag in 2023. Dit voorstel is later vele malen gewijzigd, waarbij tevens zorgen omtrent de gerichtheid deels zijn geadresseerd. Zoals ook gecommuniceerd aan uw Kamer blijft het kabinet kritisch over de gerichtheid van het voorstel.

13
Is bij u bekend of er een recenter advies is uitgebracht door de Juridische Dienst van de Raad van Europa? Zo ja, heeft dit dezelfde strekking als dat van vorig jaar?

Nee, er is geen recenter advies uitgebracht. De JDR heeft recenter wel uitgesproken dat hun zorgen niet zijn weggenomen door latere compromisvoorstellen.

14
Kunt u een overzicht geven van alle momenten waarop u met collega-bewindspersonen, al dan niet op ambtelijk niveau, contact heeft gehad over de besluitvorming met betrekking tot de CSAM-verordening? Welke bewindspersonen en departementen betrof dit?

Voor de besluitvorming met betrekking tot de CSAM-verordening is de afgelopen periode meerdere malen contact geweest op ambtelijk niveau en binnen het kabinet. Hierbij zijn naast mijn ministerie met name de ministeries van Binnenlandse Zaken en Koninkrijksrelaties, Economische Zaken en Buitenlandse Zaken betrokken geweest. Uiteindelijk heeft dat geleid tot gezamenlijke besluitvorming van het kabinet.

15
Heeft het Hongaarse voorzitterschap direct contact met u of uw collega-bewindspersonen gezocht aangaande de CSAM-verordening? Zo ja, wat was de strekking van dit contact?

Er is op ministerieel niveau geen direct contact geweest met Hongarije. Het Hongaarse voorzitterschap heeft, zoals gebruikelijk in de rol van het Voorzitterschap, contact gehad met vertegenwoordigingen van alle lidstaten in Brussel, waaronder die van Nederland.

16
Heeft u zelf direct contact gehad of gezocht met het Hongaarse voorzitterschap tijdens de formulering van uw standpunt over de CSAM-verordening? Zo ja, wat was de strekking van dit contact?

Nee.

17
Met welke lidstaten heeft u contact gehad tijdens het formuleren van uw standpunt over de CSAM-verordening? Op welke momenten is dit contact gelegd?

De Permanente Vertegenwoordiging van Nederland in Brussel heeft zoals gewoonlijk het krachtenveld bijgehouden en daarvoor contact gehad met vertegenwoordigingen van andere lidstaten. Dit contact is er de afgelopen twee jaar geregeld en op verschillende momenten tijdens de onderhandelingen geweest. Daarnaast is er op ministerieel niveau met de bewindspersoon van een andere lidstaat gesproken over dit voorstel. Over de inhoud van dat gesprek en de positie van die lidstaat kan vanwege de vertrouwelijkheid niets worden gemeld.

18
Kunt u onderbouwen waarom het verplichten van client side scanning op versleutelde privécommunicatie wat u betreft wel/niet een wettelijke verzwakking of omzeiling van end-to-endencryptie betekent? Wat betekent dit voor het grondrecht op het (digitale) briefgeheim?

Binnen het EU-voorstel voor de CSAM-verordening staat een bepaling die het mogelijk maakt om, als laatste redmiddel en als alle andere middelen onvoldoende resultaat hebben opgeleverd, een detectiebevel tegen een aanbieder van een tussenhandeldienst of interpersoonlijke communicatiedienst op te leggen. Nederland heeft op dit punt altijd gehandeld binnen het kader van de in 2022 aangenomen motie-Van Raan (Kamerstuk 26 643, nr. 885), die inhoudt dat Nederland geen voorstellen ondersteunt die end-to-end encryptie onmogelijk maken. Ook stelde het kabinet vast dat client-side scanning ten aanzien van berichtendiensten die gebruik maken van end-to-end encryptie de enige technische manier is om, binnen die diensten, het detectiebevel uit te voeren op een wijze die end-to-end encryptie niet onmogelijk maakt. Dit standpunt en de onderbouwing is met uw Kamer gedeeld.[1]

De doelstelling van artikel 13 Grondwet betreft het beschermen van de vertrouwelijkheid van communicatie van burgers. De bescherming van artikel 13 Grondwet is niet absoluut; beperking van dit recht is mogelijk in de gevallen bij de wet bepaald met machtiging van de rechter of, in het belang van de nationale veiligheid, door of met machtiging van hen die daartoe bij de wet zijn aangewezen. Daarnaast moet ook worden voldaan aan de eisen die worden gesteld in het Europees Verdrag voor de Rechten van de Mens en de bijbehorende jurisprudentie. De bescherming van artikel 13 Grondwet geldt met en zonder encryptie: ook als de inhoud van communicatie niet versleuteld is, mag die niet zomaar worden bekeken. Encryptie is een technische manier om de inhoud van de communicatie te beschermen tegen inzage door anderen, naast andere manieren

[1] Kamerstuk 26 643, nr. 1069

om daartegen te beschermen. Artikel 13 van de Grondwet schrijft niet voor of en op welke wijze private partijen hun communicatie dienen te beschermen. Dat een beveiligingsmethode eventueel gekraakt kan worden doet aan de Grondwettelijke bescherming niet af.[2]

19
Is het inbouwen van een laagdrempelige meldknop voor ongewenst gedrag op chat- en communicatiediensten een effectieve maatregel? Is deze opgenomen in de CSAM-verordening?

Een laagdrempelige meldknop is inderdaad onderdeel van de voorgestelde CSAM verordening en terug te vinden in artikel 12 lid 3. Deze maatregel kan helpen ongewenst gedrag tegen te gaan. De effectiviteit is op dit moment nog niet volledig te beoordelen. Daarnaast is op 17 februari 2024 voor de Europese Unie de Digital Services Act in werking getreden. De DSA verplicht aanbieders van tussenhandeldiensten om een gebruiksvriendelijke meldprocedure in te richten voor hun gebruikers, zodat illegale inhoud op een eenvoudige manier bij de dienst gemeld kan worden.

20
Hoe apprecieert u de strafrechtelijke gevolgen die kunnen voortvloeien uit de geautomatiseerde meldingen van client side scanning? Is deze automatische besluitvorming met grote gevolgen bij een onterechte verdachtmaking in lijn met het kabinetsbeleid?

In het voorstel is geen sprake van automatische besluitvorming en het voorstel ziet ook niet op strafrechtelijke besluitvorming. In het geval een aanbieder van een tussenhandeldienst een detectiebevel ontvangt, en hij voor dat detecteren een technologie als client side scanning zal gebruiken, is hij verplicht om over dit proces en de technologie een regelmatige menselijke toets in te richten om fouten te voorkomen. Na beoordeling van een melding wordt een rapport opgemaakt en naar het op te richten EU Centrum ter bestrijding van online seksueel kindermisbruik gestuurd. Het Centrum zal de rapportage bekijken en bepalen of de notificatie gegrond is. Indien er sprake is van een gegronde notificatie zal de rapportage doorgestuurd worden naar nationale opsporingsdiensten en/of Europol, die vervolgens verder onderzoek kunnen doen naar daders en slachtoffers van het beeldmateriaal.

21
Wat is uw standpunt over de gevolgen van ongerichte client side scanning op versleutelde privécommunicatie? Kunt u met juridisch precedent onderbouwen hoe dit niet leidt tot een ongerichte en buitenproportionele inbreuk van het (digitale) briefgeheim?

Het Europese Hof heeft in een aantal zaken benadrukt dat overheidsvoorschriften voldoende gericht moeten zijn om wanneer deze een aantasting van grondrechten met zich meebrengen. Er is geen juridisch precedent dat uitsluitsel geeft over het gebruik van client-side scanning op de manier zoals voorzien in het huidige EU-voorstel. Een dergelijke zaak zou moeten worden beoordeeld op proportionaliteit, subsidiariteit en

[2] Deze grondgedachte is door de tijd heen in feite hetzelfde gebleven, zie o.a. Kamerstukken II, 1997–1998, 25 443, nr. 5.

noodzakelijkheid van de maatregel ten aanzien van het beoogde doel, alsmede de strikte waarborgen waaronder de maatregel zou kunnen worden ingezet.
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.

22
Met hoeveel zekerheid kunt u zeggen dat de CSAM-verordening, indien aangenomen in huidige vorm, zal leiden tot minder verspreiding en zichtbaarheid van kinderpornografische beelden?

De maatregelen die benoemd zijn in de CSAM-verordening zullen hoogstwaarschijnlijk veel bijdragen aan de aanpak van online beeldmateriaal van seksueel kindermisbruik. Aanbieders van tussenhandeldiensten dienen risico-analyses uit te voeren en mitigerende maatregelen te nemen om hun diensten weerbaarder te maken tegen de verspreiding van beeldmateriaal en de dienst schoon en veilig te houden voor gebruikers. De verordening biedt ook de mogelijkheden aan nationale autoriteiten in alle landen van de Unie om verwijderbevelen uit te vaardigen om het materiaal offline te laten halen. Een detectiebevel zal waarschijnlijk ook bijdragen aan de bestrijding van online materiaal van seksueel kindermisbruik, maar het is voor het kabinet nog te onduidelijk of dit op een manier kan waarbij geen buitenproportionele inbreuk wordt gemaakt op grondrechten als privacy en het briefgeheim, en de digitale weerbaarheid niet in het geding komt. Tenslotte is de verwachting dat het EU centrum zal bijdragen aan het vergroten van kennis over de mate van verspreiding van materiaal van online seksueel kindermisbruik en zal het de Europese samenwerking op het gebied van bestrijding verbeteren.

23
Wordt kinderpornografisch beeldmateriaal grotendeels gedeeld en gezien in versleutelde privéchats, of op gesloten en openbare groepen op socialemediaplatforms? Kunt u dit onderbouwen met cijfers? Acht u de verplichtingen in de CSAM-verordening proportioneel, gezien deze verdeling?

Het is per definitie lastig om een volledig beeld te hebben van besloten groepen en wat voor beeldmateriaal daar in wordt gedeeld omdat daar geen toegang toe is. Volgens verschillende wetenschappelijke onderzoeken, zoals het WODC-onderzoek «De rol van encryptie in de opsporing: Belemmeringen en mogelijkheden» uit 2023, wordt het gebruik van encrypte communicatie-apps zoals Signal en Telegram populairder onder daders van kindermisbruik. Ook Europol bevestigt het gebruik van peer-to peer communicatiekanalen zoals Facebook Messenger voor het delen van CSAM.
In 2019 uitte het National Center for Missing and Exploited Children (NCMEC) voor het eerst zijn grote zorgen over de groeiende impact van encryptie bij de aanpak van seksueel kindermisbruik. De organisatie schat in dat als end-to-end versleuteling wordt geïmplementeerd zonder oplossingen om kinderen te beschermen, ze meer dan de helft minder meldingen zal ontvangen. Dat betekent niet dat minder materiaal online aanwezig is, maar het biedt daders de mogelijkheid om hun

criminele activiteiten beter te verbergen.[3] In het rapport van meldingen over 2022 staan meer dan twintig miljoen meldingen over Facebook, vijf miljoen meldingen die over Instagram zijn binnengekomen, ruim 2 miljoen meldingen over Google en één miljoen meldingen van online materiaal van seksueel kindermisbruik die over WhatsApp werden gedeeld.[4] Vergeleken met de meldingen over 2020 zijn een miljoen meer meldingen binnengekomen over een interpersoonlijke communicatiedienst die gebruik maakt van end-to-end encryptie.[5]

24
Kunt u onderbouwen waarom u in eerste instantie van plan was om zich stil te onthouden bij de standpuntbepaling in de JBZ-Raad, zoals beschreven in de beslisnota?

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).
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. In die fase is naar aanleiding van een nieuw advies van de AIVD de positie ten opzichte van het compromisvoorstel opnieuw bezien.
Na meerdere besprekingen in het kabinet zijn de overwegingen over het belang van de bestrijding van online seksueel kindermisbruik, grondrechten en de digitale weerbaarheid 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.

25
Welke overwegingen zijn doorslaggevend geweest in het veranderen van deze positie? Kunt u toelichten waarom de bezwaren niet hebben geleid tot een ondubbelzinnige negatieve beoordeling van de CSAM-verordening?

---

[3] https://www.missingkids.org/content/dam/missingkids/pdfs/End-to-End%20Encryption%20Media%20Kit.pdf
[4] 2022 CyberTipline Reports by ESP (missingkids.org)
[5] Child sexual abuse material and end-to-end encryption on social media platforms: An overview, Teunissen & Napier, 2022 en National Center for Missing and Exploited Children (NCMEC) (2020). 2020 CyberTipline reports by electronic service providers (ESP). Verkregen via: https://www.missingkids.org/content/dam/missingkids/pdfs/2020-reports-by-esp.pdf

Zie hiervoor mijn brief van 1 oktober jl. aan uw Kamer en het antwoord op vraag 24.

26
Wat is wat u betreft een acceptabele foutmarge voor de systematiek die bekend materiaal moet opsporen via client side scanning? Kunt u deze foutmarge uiteenzetten op het gemiddelde dagelijkse berichten- en fotoverkeer in Europa?

De foutmarge waarmee bestaand materiaal van seksueel kindermisbruik door middel van hashing kan worden gedetecteerd met gebruik van client-side scanning is buitengewoon laag. Het kabinet heeft hierover geen strikte ondergrens bepaald. Wel kan worden gewezen op cijfers en documentatie gepubliceerd over software die door veel bedrijven en overheden dagelijks wordt gebruikt om beeldmateriaal van seksueel kindermisbruik te onderkennen.[6] Het kabinet merkt hierbij overigens op dat de foutmarge op zichzelf niet bepaalt of detectie al dan niet proportioneel is.

27
Welke departementen zijn betrokken geweest bij het formuleren van het kabinetsstandpunt over de CSAM-verordening? Kunt u op hoofdlijnen beschrijven wat elk departement afzonderlijk aan u heeft geadviseerd?

Bij het formuleren van het kabinetsstandpunt zijn met name de ministeries van Justitie en Veiligheid, Binnenlandse Zaken en Koninkrijksrelaties, Economische Zaken en Buitenlandse Zaken betrokken geweest. Het besluit dat ten grondslag ligt aan het standpunt is namens het kabinet genomen; hier zijn alle ambtelijke adviezen in meegewogen.

28
Houdt de CSAM-verordening voldoende rekening met de signalen vanuit de zedenpolitie, dat extra meldingen niet zullen leiden tot een snellere of effectievere bestrijding van onlinekindermisbruik, omdat de capaciteit niet op orde is?

Zolang de reikwijdte van de verordening nog niet definitief is, is het lastig te bepalen wat de exacte consequenties kunnen zijn voor de uitvoering bij de politie. Meldingen die volgen uit een detectiebevel van een nationale autoriteit zullen doorgeleid worden aan het voorgestelde Europees centrum. Het is aan de lidstaten om te bepalen welke nationale autoriteiten bij dit proces een rol krijgen. Overigens zouden de maatregelen in de voorgestelde verordening het gebruik van diensten voor de verspreiding van materiaal van online seksueel kindermisbruik niet alleen tegengaan door de mogelijkheid een detectiebevel af te geven. Diensten die een hoog risico hebben voor de verspreiding van dergelijk materiaal te worden gebruikt, zouden eerst risicomitigerende maatregelen moeten nemen. Daarmee zou het gebruik van die diensten voor de verspreiding van dergelijk

[6] Zie CSAM Impact assessment, p. 71, waarin verwezen wordt naar een verklaring uit 2019 van de maker van deze software tegenover het Amerikaans Huis van Afgevaardigde. Laatstgenoemde gaf aan dat de foutmarge van de desbetreffende software 1 op 50 miljard betreft. Zie ook case study van de International Telecommunications UnionL https://www.itu.int/en/cop/case-studies/Documents/ICMEC_PhotoDNA.PDF; Guidelines for industry on Child Online Protection (itu.int)en Guidelines for policy-makers on Child Online Protection ${field:Subtitle report} (itu.int).

materiaal lastiger of onmogelijk worden gemaakt. Pas als deze maatregelen onvoldoende effectief blijken, zou onder voorwaarden een detectiebevel aan de orde kunnen komen.

29
Zijn de zedenteams van de nationale politie-eenheden uit andere lidstaten voldoende geëquipeerd om adequaat te reageren op de toestroom van meldingen die volgen vanuit automatische detecties, inachtnemende dat de Nederlandse politie ook aangeeft dit onuitvoerbaar te vinden?

Er is geen sprake van automatische detectie. Ik kan niet oordelen over de capaciteit van politie-eenheden uit andere lidstaten.

30
Hoe hoog acht u het risico dat de CSAM-verordening een waterbedeffect creëert, waardoor misbruikers en verdachten zich zullen verplaatsen naar ongereguleerde platforms? Wat betekent het wegbewegen van deze misbruikers en verdachten voor de proportionaliteit van de verplichtingen op wél gereguleerde platforms?

In het algemeen zullen criminelen die voor hun criminele activiteiten gebruik maken van een bepaalde dienst, op zoek gaan naar andere mogelijkheden indien die diensten lastiger of risicovoller worden om te gebruiken. In het geval van deze verordening is dat naar verwachting niet anders. Dat is echter in beginsel geen reden af te zien van het opwerpen van barrières tegen crimineel handelen. Wel is het zo dat deze verordening een zo breed mogelijk scala aan typen diensten van de informatiemaatschappij omvat, van online platformen tot interpersoonlijke communicatiediensten. Platformen die zich houden aan de verplichtingen van de CSAM-verordening zullen regelmatig risico-analyses uit moeten voeren en preventieve maatregelen nemen om hun diensten schoon te houden van online kindermisbruik. De preventieve en mitigerende maatregelen die aanbieders nemen corresponderen met de risico's die worden gesignaleerd en het is daarmee de verwachting dat die proportioneel zullen zijn.

31
Kunt u een duidelijke appreciatie geven van artikel 77 van de CSAM-verordening, waarin wordt gesteld dat een verplichting voor technologie om te scannen op onbekend materiaal en grooming elke drie jaar onderzocht en heroverwogen moet worden? Raakt dit artikel aan de harde grens van Nederland om deze scans niet mogelijk te maken?

Het standpunt van het vorige kabinet waarbij het scannen op onbekend materiaal en grooming als disproportioneel werd gezien, blijft ook voor dit kabinet staan. Het staat vast dat detectie van dit materiaal bij de huidige stand van de techniek niet op een proportionele manier kan worden uitgevoerd. In het laatste voorstel van het Hongaarse voorzitterschap is in artikel 85 voor de Commissie een verplichting opgenomen om na drie jaar een rapport op te maken met overwegingen over de noodzaak en (technische) haalbaarheid van detectie op onbekend materiaal en grooming,. Dit is echter alleen een rapportageverplichting en kan niet leiden tot een automatisch besluit om over te gaan tot detectiebevelen voor dit materiaal. Hier zal de Commissie een apart wetsvoorstel voor moeten maken.

32

Met welke zekerheid kunt u zeggen dat het mogelijk maken van client side scanning op versleutelde privécommunicatie op termijn niet zal leiden tot het uitbreiden naar andere soorten materiaal?

Andere doeleinden zijn geen onderdeel van dit voorstel en zijn niet aan de orde. Daarnaast kan meer algemeen worden benoemd dat een voorstel tot aanpassing van een Verordening zeer langdurig traject betreft dat voorzien is van alle democratische waarborgen die gebruikelijk zijn bij de totstandkoming van wetgeving. Gedurende een dergelijk traject kunnen, net zoals dit het geval was bij de totstandkoming van het huidige voorstel, nationale regeringen en uw Kamer uitgebreid invloed uitoefenen op de besluitvorming.

33
Heeft u een risicobeoordeling gemaakt van de strategische afhankelijkheden die onze nationale autoriteiten zouden krijgen van grote onlineplatforms bij het invoeren van de CSAM-verordening? Welke mogelijke risico's en onduidelijkheden bestaan er, wetende dat veel van deze bedrijven onder het recht van de Verenigde Staten vallen?

Nee, deze beoordeling is niet als zodanig gemaakt. Indien een aanbieder van diensten van de informatiemaatschappij actief wil zijn op de Europese markt maar zijn hoofdvestiging niet in de EU heeft, moet deze op grond van artikel 24 van de CSA-verordening een wettelijk vertegenwoordiger binnen de Europese Unie aanwijzen. Dat betekent ook dat het online platform zich aan de Europese regelgeving, waaronder mogelijk de CSAM-verordening, dient te houden.

34
Wat is het standpunt van de Verenigde Staten over de CSAM-verordening, waardoor zijn nationale techsector mogelijk wordt gehouden aan juridische verplichtingen die in strijd zijn met Amerikaanse wetgeving?

Er is mij geen standpunt van de Verenigde Staten over de CSAM-verordening bekend.

35
Wat heeft u doen besluiten om toch niet akkoord te gaan met het compromisvoorstel, gezien u in uw brief van 16 september 2024 aangaf dat het Hongaars voorzitterschap is gekomen met een compromisvoorstel dat tegemoetkomt aan de bezwaren van Nederland inzake het detectiebevel? In welke opzichten voldoet het compromisvoorstel dan nog steeds niet aan de eisen die uw kabinet stelt?

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).
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 telecommunica-

tiegeheim. Naar aanleiding van het voorstel heeft overleg plaatsgevonden met betrokken bewindspersonen. In die fase is naar aanleiding van een nieuw advies van de AIVD de positie ten opzichte van het compromisvoorstel opnieuw bezien.
Na meerdere besprekingen in het kabinet zijn de overwegingen over het belang van de bestrijding van online seksueel kindermisbruik, grondrechten en de digitale weerbaarheid 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.

36
Klopt het dat het kabinet heeft besloten om zich te onthouden van het innemen van een positie en dit actief kenbaar te maken? Sluit u daarmee ook niet uit dat wanneer dit voorstel niet verder wordt aangepast, Nederland niet gaat instemmen met het voorstel?

Ja, dit klopt. Ik verwijs hierbij naar mijn brief van 1 oktober jl.

37
Wat moet er volgens u nog veranderen aan het voorstel om te overwegen dit wel te kunnen steunen?

Op dit moment zie ik geen wijzigingen die ervoor zorgen dat het standpunt heroverwogen zal worden. Het kabinet houdt zich aan de motie-Van Raan die oproept end-to-end-encryptie niet onmogelijk te maken. De technologie die vervolgens detectie van online beeldmateriaal van seksueel kindermisbruik toch mogelijk kan maken is client side scanning. Uw Kamer heeft eerder aangegeven via de motie-Van Ginneken (Kamerstuk 26 643, nr. 1011) dat ook voorstellen die dit mogelijk maken niet gesteund zouden moeten worden. Het kabinet onderkent dat hier omwille van de digitale weerbaarheid ook risico's aan verbonden zijn. Dat betekent dat er voor het voorstel voor een detectiebevel voor het vinden van beeldmateriaal van online seksueel kindermisbruik in de praktijk te weinig ruimte overblijft. Indien wijzigingen zullen worden voorgesteld zullen we dat binnen het kabinet opnieuw overwegen.

38
Zijn er tussen 16 september 2024 en 1 oktober 2024 ambtelijke adviezen gegeven die aanleiding hebben gegeven om te komen tot het besluit om te onthouden van het innemen van een positie? Zo ja, kunt u deze delen met de Tweede Kamer?

Voor de besluitvorming met betrekking tot de CSAM-verordening is de afgelopen periode meerdere malen contact geweest op ambtelijk niveau en met mijn collega bewindspersonenbinnen het kabinet. Op ambtelijk niveau heeft ook regelmatig afstemming plaatsgevonden. Hierbij zijn naast mijn ministerie met name de ministeries van Binnenlandse Zaken en Koninkrijksrelaties, Economische Zaken en Buitenlandse Zaken betrokken geweest. Uiteindelijk heeft dat geleid tot gezamenlijke besluitvorming van

het kabinet. Bij de brief van 1 oktober is de bijbehorende beslisnota meegezonden.

39
Waarom heeft u gekozen om zich te onthouden van een positie, en niet besloten om voor of tegen het voorstel te stemmen?

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. Hierbij is zowel aandacht geweest voor de complexe inhoudelijke belangenafweging als voor de positie van ons land in het Europese krachtenveld.

40
Welke maatregelen treft u zelf om de verspreiding van kinderporno tegen te gaan? Wordt gewacht op een voorstel uit Europa of gaat u zelf met een voorstel aan de gang?

In Nederland worden er al vele maatregelen genomen om verspreiding van beeldmateriaal van online seksueel kindermisbruik tegen te gaan. Het meest recente voorbeeld hiervan is de oprichting van de Autoriteit online Terroristisch en Kinderpornografisch Materiaal (ATKM). De bevoegdheden van de ATKM zijn geregeld in de Wet bestuursrechtelijke aanpak kinderpornografisch materiaal die per 1 juli 2024 in werking is getreden.

41
Heeft u vertrouwen erin dat grote techbedrijven de verplichtingen uit de CSAM-verordening ordentelijk zullen uitvoeren? Waaruit blijkt dit?

Ja, daar heb ik vertrouwen in. De Nederlandse ervaring met het nakomen van wet- en regelgeving door de sector laat zien dat de grote techbedrijven goed meewerken als het gaat om het bestrijden van online materiaal van seksueel kindermisbruik. Daarnaast treft de sector ook zelf maatregelen om de verspreiding van dit materiaal tegen te gaan.

42
Kunt u aangeven welke alternatieven het betreft waar in de beslisnota is aangegeven dat het advies van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) «tevens alternatieve mogelijkheden beschrijft»?

In het advies van de AIVD is desgevraagd ingegaan op mogelijke alternatieven. De AIVD gaf hierbij aan dat er op dit moment geen voor de hand liggende alternatieven bestaan die aan alle behoeftes kunnen voldoen. De AIVD heeft daarbij aangegeven dat dit een langere termijninspanning vereist waar naar juridische en technische standaardisatie dient te worden gekeken.

43

Kan het in de beslisnota genoemde advies van de AIVD openbaar worden gemaakt?

De beslisnota bij het kabinetsstandpunt is meegestuurd naar uw Kamer. Daarin is de hoofdlijn en conclusie van het advies van de AIVD opgenomen.

44
Is het mogelijk om met technische middelen uit te sluiten dat een detectiebevel in de toekomst voor andere soorten informatie dan materiaal van seksueel misbruik van kinderen en jongeren wordt gebruikt?

Zoals aangegeven in het antwoord op vraag 32 zijn andere doeleinden geen onderdeel van dit voorstel en niet aan de orde.

45
Wat is de rationale achter artikel 7(8)(d) dat stelt dat de detectie niet van toepassing is op accounts die door de Staat worden gebruikt voor nationale veiligheidsdoeleinden, handhaving van de openbare orde of militaire doeleinden?

Deze accounts worden in het voorstel uitgesloten omwille van zorgen rond de cyberveiligheid en de digitale weerbaarheid van een lidstaat die detectie door een private partij op een account van de betreffende overheid mee kan brengen.

46
Hoe zou Europa onder de CSAM-verordening toezicht kunnen houden op grote onlineplatforms die buiten Europese wet- en regelgeving vallen?

Deze verordening is van toepassing op aanbieders van tussenhandeldiensten die dergelijke diensten in de Europese Unie aanbieden, ongeacht de locatie van hun hoofdvestiging. De CSAM-verordening bevat geen instrumenten voor aanbieders die alleen buiten de EU actief zijn.

47
Hoe moet het gerichtheidsprincipe uit overweging 23 worden uitgelegd? Kan een detectiebevel voor publiek toegankelijke interpersoonlijke communicatiediensten ook ingezet worden tegen een select aantal personen? Zo ja, wat zou de overweging zijn om het al dan niet breder in te zetten?

Het detectiebevel kan worden uitgevaardigd aan aanbieders van hoog risico-diensten wanneer er bewijs bestaat van een aanzienlijk en aanwezig of voorzienbaar risico dat de dienst of onderdelen of componenten van de dienst worden gebruikt voor het doel van de verspreiding van bekend online materiaal van online kindermisbruik. De overweging is bedoeld om de coördinerende autoriteiten ertoe aan te zetten om hun verzoek tot een detectiebevel zo gericht mogelijk te maken, bijvoorbeeld gericht op specifieke besloten groepen of onderdelen van diensten. Zonder gerichtheid kan een detectiebevel niet proportioneel zijn ten opzichte van de grondrechten die daarbij worden geschonden. Dit wordt ook door de JDR in haar advies van 2023 onderschreven. Overwegingen hebben geen bindend karakter. Deze overweging verzet zich daarom niet tegen het breder inzetten van het detectiebevel. De bepalingen in de verordening

vereisten alleen een beperking tot een dienst, of onderdelen of componenten van een dienst.

48
Welke methoden zouden in de praktijk toegepast kunnen worden binnen de twee voorwaarden uit het voorstel, namelijk dat het technologieneutraal is opgesteld maar zich beperkt tot bekend materiaal?

Het vorige kabinet heeft aangegeven de motie-Van Raan uit te voeren waardoor een derde voorwaarde is toegevoegd, namelijk dat end-to-end encryptie niet onmogelijk mag worden gemaakt. In de praktijk betekent dat dat client side scanning als methode toegepast moet kunnen worden. Overigens is het volgens het voorstel aan de dienstverlener om te bepalen welke methode wordt gebruikt voor de uitvoering van een detectiebevel.

49
Heeft de AIVD aangegeven onder welke omstandigheden een dergelijk voorstel wel veilig zou kunnen plaatsvinden?

Nee, het is op dit moment onvoldoende duidelijk wat de impact van de voorgestelde maatregelen is. 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.

50
Hoe hanteert u de definitie van «end-to-end»? En meer specifiek, wat is het begin en wat is het einde van communicatie?

Zeer kort samengevat is end-to-end encryptie een beveiligingsmethode om berichten te versleutelen tijdens verzending. End-to-end encryptie begint wanneer de verzender een bericht verstuurt (op de «verzenden» knop drukt) en eindigt wanneer het bericht wordt ontvangen en ontsleuteld op het apparaat van de ontvanger.

51
Zijn er afspraken gemaakt over de rolverdeling van verschillende opsporingsorganisaties over hoe grensoverschrijdend te werk te gaan bij het behandelen van meldingen? Hoe maken deze afspraken deel uit van de verordening?

Nee. In eerste instantie is de CSAM-verordening niet primair gericht op opsporing in strafrechtelijke zin. Het proces rond de CSAM-verordening bevindt zich in de fase richting een algemene oriëntatie binnen de Raad, en is daarmee nog niet afgerond. Het is op dit moment te vroeg om dergelijke afspraken te kunnen maken.

52
Onder welke voorwaarden zou u overwegen om zich ondubbelzinnig tégen de CSAM-verordening te keren? Wat is daarin doorslaggevend?

Het huidige kabinetsstandpunt is geformuleerd aan de hand van het recente compromisvoorstel van het Hongaars voorzitterschap. Dit betreft de huidige situatie. Op dit moment zie ik geen wijzigingen die ervoor zorgen dat het standpunt heroverwogen zal worden. Indien wijzigingen zullen worden voorgesteld zullen we dat binnen het kabinet opnieuw afwegen.

53
Welke fundamentele mensenrechten komen onder druk te staat met massasurveillancetools als deze verordening?

De CSAM-verordening beoogt geen massasurveillance. Ten aanzien van de inhoud van de verordening geldt dat het kabinet zorgen heeft over inperkingen van de grondrechten en de mate waarin die voldoen aan de eisen van – in het kort – noodzakelijkheid, proportionaliteit en subsidiariteit (zie ook vraag 3). Het gaat met name om het beschermen van de privacy en de vertrouwelijkheid van communicatie. Deze rechten gelden vanzelfsprekend ook voor kinderen. Zoals hiervoor gesteld is ook de onschuldpresumptie meegewogen. Tot slot speelt ook de vrije meningsuiting een rol. Ook is bezien of het voorstel onbedoelde risico's voor de cyberveiligheid en de digitale weerbaarheid van Nederland meebrengt.

54
Welke diensten hebben toegang tot de hits die de systemen detecteren en in welke mate?

Wanneer de andere maatregelen uit de Verordening zijn uitgeput en als uiterste redmiddel een detectiebevel wordt uitgevaardigd tegen een bepaalde dienst, dan moet het desbetreffende bedrijf scannen op bekend strafbaar kinderpornografisch beeldmateriaal. (foto's en video's) en URL's. Een detectiebevel wordt door de Coordinerende Autoriteit uitgevaardigd na rechtelijke machtiging. Beeldmateriaal wordt bij het uitvoeren van een detectiebevel automatisch vergeleken met beeldmateriaal waarvan is vastgesteld dat dit materiaal van seksueel kindermisbruik betreft. Bij een match stuurt het bedrijf het materiaal door naar het voorziene Europees centrum ter bestrijding van online seksueel kindermisbruik. Het bedrijf ziet er op toe dat hetgeen wordt doorgestuurd naar het Europees centrum beeldmateriaal van online seksueel kindermisbruik betreft. Vervolgens beoordeelt het Europees centrum het materiaal opnieuw. Als het Europees centrum ook van mening is dat het gaat om strafbaar beeldmateriaal, dan wordt dit materiaal doorgestuurd naar de relevante autoriteiten.

55
Wat zijn de gevolgen van deze verordening voor tieners als zij privéfoto's naar elkaar sturen? Worden zij aangemerkt als zijnde in het bezit van kinderpornografisch materiaal?

Die kans is bij detectie van bekend kinderpornografisch materiaal vrijwel nihil en zal naar verwachting vrijwel of in het geheel niet voorkomen. Zoals aangegeven in de beantwoording van de vorige vraag kan, na uitvaardigen van een detectiebevel beeldmateriaal jegens een dienstverlener, beeldmateriaal automatisch worden gematched tegen beeldmateriaal waarvan is vastgesteld dat dit materiaal van seksueel kindermisbruik betreft. Het gaat daarbij dus niet ook om beeldmateriaal van tieners die privéfoto's aan elkaar sturen, omdat dit geen materiaal is waarvan is vastgesteld dat het seksueel kindermisbruik betreft. Bij een «match» moet het bedrijf het materiaal doorsturen naar het Europees centrum, waarbij het bedrijf er erop toeziet dat hetgeen wordt doorgestuurd daadwerkelijk bekend materiaal van seksueel kindermisbruik betreft. Vervolgens beoordeelt het Europees centrum het materiaal opnieuw. Als het Europees centrum ook van mening is

dat het gaat om strafbaar beeldmateriaal, dan wordt dit materiaal doorgestuurd naar de relevante autoriteiten.

56
Hoe groot is het probleem van kinderpornografisch materiaal in Nederland?

Vanuit Nederland wordt disproportioneel veel online kinderpornografisch materiaal via het internet ter beschikking gesteld. Mede vanwege de goede digitale infrastructuur is Nederland een aantrekkelijk land voor datacentra en hostingproviders. Dit maakt dat Nederland, in vergelijking met andere Europese landen, een grote hoeveelheid kinderpornografisch materiaal op haar servers heeft staan. Onder andere in de jaarverslagen van Offlimits en InHope wordt jaarlijks gerapporteerd over de hoeveelheid kinderpornografisch materiaal dat in Nederland wordt gehost. In 2023 heeft Offlimits 255.454 meldingen verwerkt van online kinderpornografisch materiaal waarvan 63% in Nederland werd gehost. Binnen het internationale netwerk van InHope zijn er in 2023 totaal 785.322 meldingen verwerkt van kinderpornografisch materiaal. Hiervan werd 20% in Nederland gehost. Binnen Europa werd 61% van al het online kinderpornografisch materiaal in Nederland gehost.

57
Welke maatregelen zijn er genomen op het gebied van cybersecurity om ervoor te zorgen dat de grote mate van privacy te allen tijde beschermd is?

Het EU-voorstel schept strenge verplichtingen voor bedrijven om eventuele cybersecurity risico's te identificeren, analyseren, beoordelen (Artikel 3) – en vervolgens alles te doen om deze mogelijke risico's te mitigeren (Artikel 4) en minimaliseren. Zoals elders in de beantwoording geschetst zijn digitale veiligheid en weerbaarheid voor het kabinet belangrijke overwegingen die geadresseerd moeten worden bij de standpuntbepaling over deze verordening.

58
Hoeveel fte's zijn er nodig om alle hits te controleren?

Het is op dit moment niet mogelijk om een inschatting te maken van het aantal benodigde ftes nu onvoldoende duidelijk is hoeveel hits er zullen zijn. Zolang de reikwijdte van de verordening nog niet definitief is, is het lastig te bepalen wat de consequenties kunnen zijn voor de uitvoering.

59
Hoeveel gaat de uitvoering van de verordening de EU en Nederland kosten? Kunt u een gedetailleerd overzicht verstrekken voor alle Europese landen en het totaal?

De verwachte financiële consequenties van de verordening zijn bij het formuleren van het vorige kabinetsstandpunt in het BNC fiche uiteengezet. Ik verwijs daarom naar paragraaf 5 van dit fiche.

60

Hoe kan voorkomen worden dat lijsten met gegevens van potentiële of van nog niet bevestigde bezitters van mogelijk kinderpornografisch materiaal op straat komen te liggen?

Er bestaan geen lijsten van onbevestigd kinderpornografisch materiaal. In het geval een aanbieder van een tussenhandeldienst een detectiebevel ontvangt, en hij voor dat detecteren een technologie als client side scanning zal gebruiken, is hij verplicht om over dit proces en de technologie een regelmatige menselijke toets in te richten om fouten te voorkomen. Voorts bevat de verordening meerdere regels rond de behandeling van persoonsgegevens en een gedegen gegevensbescherming.

61
Hoe kunnen goedbedoelde berichten van ouders of verzorgers eruit gefilterd worden en niet aangemerkt worden als zijnde strijdig met deze verordening?

Het Hongaars voorstel beperkt de reikwijdte van het detectiebevel tot enkel bekend materiaal. De beschreven situatie ziet op onbekend materiaal of grooming, dat geen onderdeel meer uitmaakt van de reikwijdte van het detetiebevel zoals voorgesteld door het Hongaarse voorzitterschap.

62
Welk beslag gaat het serieus opsporen van de hits leggen op de capaciteit bij de diensten die hiermee belast worden?

Vooropgesteld moet worden dat geen sprake is van opsporen in de strafrechtelijke zin. Omdat het op dit moment onvoldoende duidelijk is wat de omvang van de te beoordelen hits zal zijn, is het niet mogelijk om een inschatting te maken van de benodigde capaciteit voor de betrokken diensten. Ook geldt dat, zolang de reikwijdte van de verordening nog niet definitief is, het lastig is om te bepalen wat de consequenties kunnen zijn voor de uitvoering.

63
Hoe wordt de schade ongedaan gemaakt wanneer iemand aantoonbaar onschuldig is en binnen welke termijn, gezien je bij eenmaal een «hit» (ongeacht de ingezette middelen om tot die hit te komen), in het systeem belandt als «verdacht van kinderporno» en je in verschillende databases komt? Is de «verdachtmaking» omkeerbaar? Wat zijn de maatschappelijke gevolgen indien dat niet het geval blijkt?

Het uitgangspunt is dat de uitvoering van deze verordening niet mag leiden tot onterechte verdachtmakingen. Op dit moment zijn wij nog in het proces tot een mogelijke algemene oriëntatie. De precieze inhoud van de verordening is daarmee nog niet bekend. Wel staan in het voorstel mogelijkheden opgenomen voor gebruikers van een tussenhandeldienst om bezwaar te maken. Indien de tussenhandeldienst een detectiebevel voor zijn/haar dienst heeft ontvangen dient hij/zij al haar gebruikers hiervan op de hoogte te stellen en hebben deze gebruikers het recht om hier bezwaar tegen te maken. Op het moment dat er via een detectiebevel ook daadwerkelijk materiaal van online seksueel kindermisbruik wordt aangetroffen, dan vindt daar eerst nog een menselijke toets op plaats om vast te stellen dat het inderdaad gaat om bekend materiaal. Vervolgens wordt er een rapport opgesteld dat naar het EU-Centrum zal worden gestuurd. Ook de gebruiker van

de dienst waarbij het materiaal is aangetroffen zal hier een notificatie over ontvangen. Bezwaar staat ook op dit punt open voor de gebruiker indien deze van mening is dat hij/zij onschuldig is of het oneens is met de kwalificatie van het materiaal.

64
In hoeverre en in welke mate wordt er op dit moment beroep gedaan op technologiebedrijven in het detecteren en verwijderen van materiaal over seksueel misbruik en uitbuiting van kinderen?

In Nederland wordt voor wat betreft verwijdering van kinderpornografisch materiaal al een geruime tijd ingezet op effectieve zelfregulering. Zo is er een generieke vrijwillige gedragscode ontworpen, gericht op dienstverleners die in Nederland een tussenhandeldienst aanbieden. Deze gedragscode bevat een procedure voor het omgaan met meldingen van onrechtmatig of strafbaar materiaal op het internet, waaronder kinderpornografisch materiaal. Met een publiek-private samenwerking is deze zelfregulering verder versterkt. Zo hebben bovengenoemde partijen, na overleg met de Minister van Justitie en Veiligheid, op 13 november 2018 voor de aanpak van kinderpornografisch materiaal een addendum aan deze gedragscode toegevoegd, gericht op het verwijderen van kinderpornografisch materiaal. Hierin is de rol van Offlimits als onafhankelijke stichting en als betrouwbare melder versterkt, en wordt ingezet op het vrijwillig verwijderen van dit type materiaal binnen een termijn van 24 uur.

65
Door wie wordt het beroep op en de ontwikkeling van de AI-systemen betaald? In welke mate betaalt de EU dit?

De in het kader van deze verordening te gebruiken systemen worden niet separaat voor het doel van deze verordening ontwikkeld. Wel bevat de verordening een bepaling (Artikel 50) om bestaande detectietechnologie te beoordelen op betrouwbaarheid en proportionaliteit.

66
In hoeverre is AI in zulke mate ontwikkeld om zulke gevoelige data te verwerken?

Op dit moment geldt dat de huidige technologieën, voor wat betreft de detectie van onbekend materiaal en grooming, onvoldoende betrouwbaar zijn en tot een hoog aantal vals-positieven leiden. Zij zijn daarmee niet geschikt voor het verwerken van deze gegevens.

67
Betekent dit voorstel een einde van het Nederlandse briefgeheim?

Nee. Het kabinet heeft – zoals in de brief van 1 oktober en in de antwoorden hierboven uiteengezet – zorgen over de bescherming van de grondrechten, waaronder het briefgeheim. Dat recht is weliswaar niet absoluut, maar inperkingen van het briefgeheim moeten aan eisen voldoen. In Nederland gelden sterke waarborgen bij eventuele inbreuken op eerbiediging van het brief- en telecommunicatiegeheim, neergelegd in artikel 13 van de Grondwet. Zo is beperking van dit recht enkel mogelijk in de gevallen bij de wet bepaald met machtiging van de rechter. Voorts gelden artikel 8 EVRM en artikel 7 EU-Handvest: beper-

kingen zijn mogelijk indien voorzien bij wet, een legitiem doel wordt gediend en voldaan is aan de noodzakelijkheid- en evenredigheidsvereiste. Binnen dit grond- en mensenrechtelijk kader zal moeten worden bezien of er mogelijkheden zijn om tot regels te komen voor een effectieve bestrijding van seksueel kindermisbruik. Nederland zal niet instemmen met een voorstel dat in strijd is met artikel 13 van de Grondwet.

68
Hoelang hebben bedrijven op dit moment om materiaal te verwijderen?

Op grond van de vrijwillige Notice-and-Take-Down-procedure moet kinderpornografisch materiaal binnen 24 uur na een melding door Offlimits zijn verwijderd. Bij een aanwijzing op grond van de Wet bestuursrechtelijke aanpak online kinderpornografisch materiaal wordt een termijn gesteld waarbinnen het online kinderpornografisch materiaal ontoegankelijk moet zijn gemaakt. De lengte van die termijn is afhankelijk van de omstandigheden van het geval. Het vereist een afweging tussen het belang van tijdige verwijdering en de technische en praktische maatregelen die redelijkerwijs van de aanbieder van een communicatiedienst kunnen worden gevergd. Gelet op het veelal evidente karakter van kinderpornografisch materiaal zal de in de aanwijzing opgenomen termijn in de regel een korte zijn.

69
Kunt u een uiteenzetting geven wat er voor bedrijven in de opsporing gaat veranderen als deze wetgeving gaat gelden?

Vooropgesteld moet worden dat bij bedrijven geen sprake is van opsporing in de strafrechtelijke zin. Zolang de reikwijdte van de verordening nog niet definitief is, is het lastig te bepalen wat de consequenties kunnen zijn voor de uitvoering.

70
Welke termijn wordt er gekoppeld aan de CSAM-verordening om het materiaal met betrekking tot seksueel misbruik te verwijderen?

De bevoegde autoriteit in elke lidstaat kan een verwijderbevel uitvaardigen. De ontvanger van het verwijderbevel voert dit zo snel mogelijk, en in ieder geval binnen 24 uur na de ontvangst ervan uit.

71
Welke onderdelen van de CSAM-verordening zullen mogelijkerwijs door jurisprudentie ingevuld/aangepast worden?

Nu de inhoud van de verordening nog niet definitief vast staat, is het lastig om daar een beeld van te geven.

72
Welke vergoedingsmaatregelen worden er (mogelijkerwijs) getroffen voor slachtoffers van false-positives?

Hierover is nog niet gesproken, waardoor ik hierover op het moment geen duidelijkheid kan verschaffen. Zolang de reikwijdte van de verordening nog niet definitief is, is het lastig te bepalen hoe dit er precies gaat uitzien. Zoals geschetst in de beantwoording op vraag 63 zijn er op verschillende momenten in het

proces mogelijkheden voor gebruikers van tussenhandeldiensten om bezwaar te maken.

73
In hoeverre houdt de verordening rekening met de desastreuze gevolgen van de backdoor in software om deze verordening na te leven om dit materiaal op te sporen?

Het is aan de betrokken dienstverlener om te bepalen met welke methode een detectiebevel zal worden uitgevoerd. 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.

74
Hoeveel wordt er verwacht kwijt te zijn aan mogelijke schadevergoedingen voor slachtoffers van false-positives, indien daar sprake van is?

Hierover is nog niet gesproken, waardoor ik hierover op het moment geen duidelijkheid kan verschaffen. Zolang de reikwijdte van de verordening nog niet definitief is, is het lastig te bepalen hoe dit er precies gaat uitzien. Zoals geschetst in de beantwoording op vraag 63 zijn er op verschillende momenten in het proces mogelijkheden voor gebruikers van tussenhandeldiensten om bezwaar te maken.

75
Aan de hand van welke gegevens wordt bepaald of iemand wel of niet onder de verordening valt, denk daarbij aan IP-adres, profielinstellingen, EU-telefoonnummers et cetera?

De verordening geldt voor alle verleners van diensten binnen de EU die onder de reikwijdte van de verordening vallen. Deze diensten staan opgenomen in artikel 2 van de verordening. De verplichtingen in de verordening betreffen met name hostingdiensten en interpersoonlijke communicatiediensten.

76
Is er rekening gehouden met de rol van een VPN in het omzeilen van de strafbaarstelling volgens deze Europese verordening?

De CSAM-verordening ziet op diensten en niet op individuele gebruikers. De verordening bevat derhalve geen strafbaarstelling voor individuele gebruikers. Wel bevat de verordening sanctiebepalingen voor dienstverleners die zich niet houden aan bepaalde onderdelen van de verordening. Afhankelijk van de exacte wijze van dienstverlening kan worden bepaald of de verplichtingen en eventuele handhavingsmogelijkheden in de verordening daarop van toepassing zijn.

77
Hoe verhoudt de CSAM-verordening zich tot bestaand bestuursrechtelijk beleid van Nederland om kinderpornografisch materiaal tegen te gaan?

Voor wat betreft het bestuursrechtelijk beleid zet het kabinet bij het opschonen van het internet van materiaal van seksueel kindermisbruik in op effectieve zelfregulering binnen de sector. In aanvulling hierop maakt de Wet bestuursrechtelijke aanpak

online kinderpornografisch materiaal het mogelijk om een binnen Nederland gevestigde dienstverlener (hosting service provider of communicatiedienst) die kinderpornografisch materiaal opslaat of doorgeeft een bindende aanwijzing te geven. De aanwijzing attendeert de dienstverlener op de aanwezigheid van het materiaal en houdt het bevel in dit materiaal binnen een korte termijn ontoegankelijk te maken. Naleving van de aanwijzing kan worden afgedwongen met een last onder dwangsom of een bestuurlijke boete. Met de CSAM-verordening wordt op Europees niveau aanvullende regelgeving voor bedrijven voorgesteld om, bijvoorbeeld door risicomitigerende maatregelen, hun diensten schoon te houden van kinderpornografisch materiaal. De CSAM-verordening kent meer bevoegdheden en is van toepassing op de gehele EU.

78
Hoe verhoudt de CSAM-verordening zich tot bestaand strafrechtelijk beleid van Nederland om kinderpornografisch materiaal tegen te gaan?

De CSAM-verordening richt zich op bedrijven als hostingdiensten, interpersoonlijke communicatiediensten, appstores en internet-toegangdiensten. De strafrechtelijke aanpak in Nederland richt zich op identificatie van slachtoffers teneinde acute misbruik- en/of uitbuitingsituaties spoedig te kunnen stoppen en de daders daarvan op te sporen en vervolgen. De prioriteit van deze strafrechtelijke aanpak is geborgd in de opname van online seksueel kindermisbruik als thema in de Veiligheidsagenda 2023–2026.

79
Hoe verhoudt de CSAM-verordening zich tot de Digitaledienstenverordening?

De CSAM-verordening kan worden gezien als een zogenaamde *lex specialis* van de Digitaledienstenverordening (DSA). De DSA stelt algemene regels aan diensten van de informatiemaatschappij over o.a. moderatie van inhoud en aanbevelingsalgoritmen. De CSAM-verordening voorziet in verder uitgewerkte regels omtrent een specifiek type illegale inhoud te weten online materiaal van seksueel kindermisbruik. Daarmee gaan de regels van de CSAM-verordening voor op de regels van de DSA.

80
Hoe verhoudt de CSAM-verordening zich tot het EU-centrum ter voorkoming en bestrijding van seksueel misbruik van kinderen?

Onderdeel van de CSAM-verordening is de oprichting van een Europees centrum inzake seksueel misbruik van kinderen. Op basis van de verordening worden bevoegdheden aan dit centrum toegekend. Zo zal het centrum als kennis- en expertise centrum fungeren om, onder meer, betrouwbare informatie over materiaal van CSA te verstrekken en steun aan slachtoffers te verlenen.

81
Welke voorstellen ter verbetering van het compromisvoorstel zijn er noodzakelijk om toch in te kunnen stemmen met het voorstel?

Het huidige kabinetsstandpunt is geformuleerd aan de hand van het recente compromisvoorstel van het Hongaars voorzitterschap. Dit betreft de huidige situatie. Op dit moment zie ik geen

wijzigingen die ervoor zorgen dat het standpunt heroverwogen zal worden. Indien wijzigingen zullen worden voorgesteld zullen we dat binnen het kabinet opnieuw afwegen.

82
Wat is uw inzet nu Nederland gerekend wordt tot de tegenstanders van het compromisvoorstel? Is het nog mogelijk om in de triloogfase het voorstel aan te passen?

Op dit moment zal er bij de beandeling van de CSAM-verordening bij de JBZ-Raad geen sprake zijn van besluitvorming. Dat geeft Nederland meer tijd om naar de belangenafweging rond het voorstel te kijken. 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. Op dit moment heeft de Raad nog geen algemene oriëntatie aangenomen. Dat betekent dat het starten van de triloogfase op dit moment niet aan de orde is. De discussie in de triloogfase wordt in beginsel gevoerd tussen het Europees Parlement en Raad van de Europese Unie. Nederland zal, waar mogelijk, haar zorgen omtrent het voorstel in deze fase naar voren brengen.

83
Wat is de precieze aanleiding voor het wijzigen van het standpunt van het kabinet, gelet op het beperken van de reikwijdte van het voorstel dat aan veel Nederlandse bezwaren tegemoetkomt?

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).
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.
Na meerdere besprekingen in het kabinet zijn de overwegingen over het belang van de bestrijding van online seksueel kindermis-

bruik, grondrechten en de digitale weerbaarheid 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.

84
Geeft u zich er rekenschap van dat met onthouding er geen verordening komt en de bestrijding van kinderporno lastiger wordt?

Het formuleren van het huidige kabinetsstandpunt was geen eenvoudige opgave. Hierbij is zowel aandacht geweest voor de complexe inhoudelijke belangenafweging, weergegeven onder vraag 82, als voor de positie van ons land in het Europese krachtenveld. Het is Nederland bekend wat de gevolgen van het kabinetsstandpunt kunnen zijn voor wat betreft het verdere proces in Brussel.

85
Waar ligt voor u de grens wat betreft privacy-inmenging van verdachten teneinde de verspreiding van kinderporno tegen te gaan?

Het is ten eerste belangrijk om aan te geven dat het bij deze verordening niet gaat om strafrechtelijke opsporing. De maatregelen ter bestrijding van online materiaal van seksueel kindermisbruik moeten proportioneel zijn. Er zal altijd een afweging moeten worden gemaakt tussen de mate van verdenking die bestaat tegen iemand die dit materiaal mogelijk verspreidt en de privacy van die persoon.

86
Wat is de definitie van een «detectiebevel» zoals dat voor ligt in het laatste voorstel vanuit het Hongaars voorzitterschap?

In het voorstel vanuit het Hongaars voorzitterschap is geen definitie van het detectiebevel opgenomen.

87
Wie geeft in het voorstel een detectiebevel af?

De coördinerende autoriteit van een lidstaat kan een gerechtelijke autoriteit of onafhankelijke administratieve autoriteit verzoeken een detectiebevel af te geven. Lidstaten kunnen er ook voor kiezen de coördinerende autoriteit dit bevel te laten uitvaardigen, met machtiging van een gerechtelijke of onafhankelijke administratieve autoriteit.

88
Kan worden geschetst welke stappen er in het voorstel staan die eerst moeten worden genomen alvorens een detectiebevel kan worden afgegeven, gezien hierover in de brief wordt gesproken als een «last resort»?

Wanneer de andere maatregelen uit de Verordening zijn uitgeput en als uiterste redmiddel een detectiebevel wordt uitgevaardigd

tegen een bepaalde dienst, dan moet het desbetreffende bedrijf scannen op bekend strafbaar kinderpornografisch beeldmateriaal. Een detectiebevel wordt door de Coordinerende Autoriteit uitgevaardigd na rechtelijke machtiging of machtiging van een andere onafhankelijke autoriteit. Beeldmateriaal wordt bij het uitvoeren van een detectiebevel automatisch vergeleken met beeldmateriaal waarvan is vastgesteld dat dit materiaal van seksueel kindermisbruik betreft. Bij een match stuurt het bedrijf het materiaal door naar het voorziene Europees centrum ter bestrijding van online seksueel kindermisbruik. Het bedrijf ziet er op toe dat hetgeen wordt doorgestuurd naar het Europees centrum beeldmateriaal van online seksueel kindermisbruik betreft. Vervolgens beoordeelt het Europees centrum het materiaal opnieuw. Als het Europees centrum ook van mening is dat het gaat om strafbaar beeldmateriaal, dan wordt dit materiaal doorgestuurd naar de relevante autoriteiten.

89
Wat is de definitie van «internetbedrijf» zoals verwoord in de brief?

De term «internetbedrijf» is een verzamelnaam voor hostingdiensten, interpersoonlijke communicatiediensten, appstores en internettoegangdiensten.

90
Welke risicomitigerende maatregelen moeten bedrijven nemen en waarom wordt er niet bij voorbaat op gestuurd dat bedrijven risicomitigerende maatregelen treffen tegen de verspreiding van kinderpornografisch materiaal? Wie geeft opdracht tot deze risicomitigerende maatregelen? Is dit statisch, eenmalig of een continu proces?

In artikel 4 van de CSAM-verordening staat opgenomen welke risicomitigerende maatregelen, ten minste, dienen te worden genomen door tussenhandeldiensten. Het is niet verplicht om al deze maatregelen te nemen. Onder de maatregelen vallen, onder meer, het versterken van interne processen en het initiëren of aanpassen van functionaliteiten die gebruikers in staat stellen CSAM te melden. De verordening is juist zo opgezet dat het treffen van risico mitigerende maatregelen vooraf gaat aan meer verplichtende maatregelen zoals het detectiebevel. Het proces van risicobeoordeling, waaruit kan blijken dat meer risicobeperkende maatregelen zouden moeten worden ingevoerd, is een continu proces.

91
Komt er één coördinerende autoriteit van alle lidstaten en ontleent deze autoriteit haar bevoegdheden aan de CSAM-verordening?

Onderdeel van de CSAM-verordening is de oprichting van een Europees Centrum inzake seksueel misbruik van kinderen. Op basis van de verordening worden bevoegdheden aan dit centrum toegekend. Voorts verlangt de verordening dat de lidstaten op nationaal niveau elk een coördinerende autoriteit aanwijzen die verantwoordelijk is voor de toepassing en handhaving van de verordening. Het Europees centrum zorgt voor de totstandkoming en het onderhoud van een of meer betrouwbare en beveiligde informatie-uitwisselingssystemen ter ondersteuning van de communicatie tussen de coördinerende autoriteiten, de Commissie, het Europees centrum, andere betrokken agentschappen van de Unie en de aanbieders van relevante tussenhan-

deldiensten zoals hostingdiensten, online platformen en interpersoonlijke communicatiediensten.

92
Klopt het dat het detectiebevel alleen zou gaan over bestaand kinderpornografisch materiaal?

Dat klopt. In het Hongaarse compromisvoorstel wordt het detectiebevel beperkt tot alleen bekend materiaal.

93
Wat gebeurt er feitelijk in het laatste voorstel als er een detectiebevel wordt gegeven? Wat gebeurt er als een scan bestaand kinderpornografisch materiaal aantreft? Wie handelt verwijtbaar: de dienst, de verzender of de ontvanger? Wat zijn de openstaande rechtsmiddelen voor deze partij?

Wanneer de andere maatregelen uit de Verordening zijn uitgeput en als uiterste redmiddel een detectiebevel wordt uitgevaardigd tegen een bepaalde dienst, dan moet het desbetreffende bedrijf scannen op bekend strafbaar kinderpornografisch beeldmateriaal. Een detectiebevel wordt door de Coordinerende Autoriteit uitgevaardigd na rechtelijke machtiging of machtiging van een andere onafhankelijke autoriteit. Beeldmateriaal wordt bij het uitvoeren van een detectiebevel automatisch vergeleken met beeldmateriaal waarvan is vastgesteld dat dit materiaal van seksueel kindermisbruik betreft. Bij een match stuurt het bedrijf het materiaal door naar het voorziene Europees centrum ter bestrijding van online seksueel kindermisbruik. Het bedrijf ziet er op toe dat hetgeen wordt doorgestuurd naar het Europees centrum beeldmateriaal van online seksueel kindermisbruik betreft. Vervolgens beoordeelt het Europees centrum het materiaal opnieuw. Als het Europees centrum ook van mening is dat het gaat om strafbaar beeldmateriaal, dan wordt dit materiaal doorgestuurd naar de relevante autoriteiten.

94
Aan welke bezwaren van Nederland is tegemoetgekomen en welke bezwaren of bedenkingen staan er nu nog open?

Het voorstel van het Hongaars voorzitterschap bevat onderdelen die tegemoetkomen aan bezwaren die gedurende de onderhandelingen door Nederland naar voren zijn gebracht ten aanzien van de reikwijdte van het zogeheten «detectiebevel». Zo heeft het vorige kabinet gemeld dat een detectiebevel zich zou dienen te beperken tot bestaand materiaal. In het Hongaarse compromisvoorstel wordt hieraan tegemoet gekomen. Het is echter nog te onduidelijk hoe er uitvoering aan een detectiebevel zou kunnen worden gegeven zonder daarbij de digitale weerbaarheid aan te tasten en proportioneel te zijn ten opzichte van grondrechten.

95
Wat zijn «specifieke diensten waarvan het risico hoog is dat zij worden misbruikt voor de verspreiding van kinderpornografisch materiaal»? Is daar een definitie van?

Nee. De mate van risico van een dienst zal blijken uit de verplichte risicoanalyse die de dienstverlener uitvoert. De Europese Commissie heeft ook de mogelijkheid om hierover gedelegeerde handelingen aan te nemen.

96
Kan er – zonder staatsgeheime informatie prijs te geven – meer inzicht worden gegeven in de strekking van de adviezen van de AIVD over het meest recente voorstel?

De hoofdlijn en conclusie van het advies is opgenomen in de beslisnota bij de Kamerbrief van 1 oktober jl. De AIVD is desgevraagd ingegaan op de technische werking van client side scanning. Daarbij is ingegaan op de adviesvragen omtrent de technische werking en mogelijke alternatieve technische mogelijkheden. Tevens verwees de AIVD naar een advies van de Cyber Security Raad (CSR).[7]

97
Waarom heeft de AIVD pas nu advies uitgebracht?

Naar aanleiding van het nieuwe compromisvoorstel is de AIVD benaderd dvoor advies. De AIVD benadrukt regelmatig het risico dat statelijke actoren misbruik kunnen maken van bepaalde technologieën.

98
Welke andere partijen hebben advies uitgebracht? Was dit advies ten tijde van het BNC-fiche of bij deze aangepaste algemene oriëntatie?

Er is eerder advies uitgebracht door de Juridische Dienst van de Raad en door de European Data Protection Board (EDPB) en European Data Protection Supervisor (EDPS). Er is ook advies uitgebracht door de Juridische Dienst van de Commissie. Deze adviezen zijn allen uitgebracht na het opstellen van het BNC-fiche.

99
Is de input van de AIVD gewogen bij de inzet van Nederland toen het BNC-fiche over de CSAM-verordening naar de Kamer is gestuurd?

De input van de AIVD is niet meegewogen bij de inzet van Nederland in de BNC-fase. Het advies was toen nog niet bekend en kon daarom niet worden betrokken.

100
Wat wordt er bedoeld met alternatieve mogelijkheden voor client side scanning, waarbij het scannen van gegevens op een wijze kan plaatsvinden die de strikte definitie van end-to-endencryptie loslaat?

De detectie van materiaal van seksueel kindermisbruik kan in beginsel plaatsvinden op het apparaat (client side) of tijdens het transport van het bericht waar dit in is verwerkt. Bij end-to-end-encrypted diensten is detectie van dit materiaal tijdens het transport niet mogelijk. Bij end-to-end encryptie is immers de communicatie van eindpunt-naar-eindpunt beveiligd en gedurende het transport niet leesbaar.
Indien niet voor client side scanning wordt gekozen, is detectie tijdens transport van het bericht – in welke vorm dan ook – de enige andere keuze.

---

[7] https://www.cybersecurityraad.nl/binaries/cybersecurityraad/documenten/adviezen/2022/08/25/csr-adviesbrief-in-relatie-tot-encryptie---minister-van-justitie-en-veiligheid/20220823+CSR+Adviesbrief+in+relatie+tot+encryptie+-+Minister+van+Justitie+en+Veiligheid+DEF.pdf

101
Wat is de meest recente informatie over de standpunten van de landen inzake deze algemene oriëntatie? Hoe verliep het overleg in Coreper?

Over de positie van specifieke lidstaten kan in het kader van de vertrouwelijkheid niets worden gezegd. Wel is duidelijk 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. Omdat het krachtenveld nog zo gefragmenteerd is heeft het Hongaarse voorzitterschap besloten om in de komende JBZ-Raad geen algemene oriëntatie vast te stellen. Er zal alleen een stand van zaken worden gegeven.

102
Wat zijn de verwachtingen van Nederland wat er met het voorstel zal gebeuren onder het aankomende Poolse voorzitterschap?

Het is aan het Poolse voorzitterschap om invulling te geven aan het verdere proces rond deze verordening.