Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

22 112 Nieuwe Commissievoorstellen en initiatieven van de lidstaten van de Europese Unie

Nr. 3455 **BRIEF VAN DE MINISTER VAN BUITENLANDSE ZAKEN**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 17 juni 2022

Overeenkomstig de bestaande afspraken ontvangt u hierbij 3 fiches die werden opgesteld door de werkgroep Beoordeling Nieuwe Commissie voorstellen (BNC).

Fiche: Mededeling een digitaal decennium voor kinderen en jongeren (Kamerstuk 22 112, nr. 3454)
Fiche: Verordening ter voorkoming en bestrijding van seksueel kindermisbruik
Fiche: Herziening richtlijn betreffende op afstand afsluiten van overeenkomsten inzake financiële diensten (Kamerstuk 22 112, nr. 3456)

De Minister van Buitenlandse Zaken,
W.B. Hoekstra

kst-22112-3455
ISSN 0921 - 7371
's-Gravenhage 2022

Fiche: Verordening ter voorkoming en bestrijding van seksueel kindermisbruik

1. Algemene gegevens

a) *Titel voorstel*
Voorstel voor een verordening van het Europees parlement en de Raad betreffende voorschriften ter voorkoming en bestrijding van seksueel kindermisbruik
b) *Datum ontvangst Commissiedocument*
11 mei 2022
c) *Nr. Commissiedocument*
COM(2022) 209
d) *EUR-Lex*
EUR-Lex – COM:2022:209:FIN – EN – EUR-Lex (europa.eu)
e) *Nr. impact assessment Commissie en Opinie Raad voor Regelgevingstoetsing*
SWD(2022) 209
f) *Behandelingstraject Raad*
Raad Justitie en Binnenlandse Zaken
g) *Eerstverantwoordelijk ministerie*
Ministerie van Justitie en Veiligheid
h) *Rechtsbasis*
Artikel 114 van het Verdrag betreffende de werking van de Europese Unie (VWEU)
i) *Besluitvormingsprocedure Raad*
Gekwalificeerde meerderheid
j) *Rol Europees parlement*
Medebeslissing

2. Essentie voorstel

a) Inhoud voorstel

Op 11 mei 2022 heeft de Commissie een voorstel gepubliceerd voor een verordening betreffende voorschriften ter voorkoming en bestrijding van seksueel kindermisbruik (hierna: CSA (Child Sexual Abuse)). Dit voorstel was aangekondigd in de EU-strategie voor een effectievere aanpak van CSA[1].

Parallel aan dit voorstel heeft de Commissie een nieuwe EU-strategie[2] gepubliceerd om kinderen in de online wereld te beschermen en weerbaarder te maken. U wordt hierover geïnformeerd in een separaat BNC-fiche.

De Commissie constateert dat het huidige systeem, dat gebaseerd is op vrijwillige detectie en melding door bedrijven, onvoldoende effectief is gebleken om kinderen in afdoende mate te beschermen. Bovendien zal dit niet langer meer mogelijk zijn zodra de tijdelijke oplossing[3] afloopt om vrijwillig materiaal van CSA te kunnen detecteren en melden. De

---

[1] COM(2020) 607, 24 juli 2020 en Kamerstuk 22 112, nr. 2926.
[2] COM(2022) 212, 11 mei 2022.
[3] Verordening 2021/1232/EU van het Europees parlement en de Raad van 14 juli 2021 betreffende een tijdelijke afwijking van enkele bepalingen van Richtlijn 2002/58/EG wat betreft het gebruik van technologieën door aanbieders van nummeronafhankelijke interpersoonlijke communicatiediensten voor de verwerking van persoons- en andere gegevens ter bestrijding van online CSA. De verordening heeft een beperkte duur en een beperkt toepassingsgebied, dat beperkt is tot vrijwillige activiteiten van bepaalde onlinediensten gedurende een periode van ten hoogste drie jaar, die in augustus 2024 verstrijkt.

Commissie heeft dit voorstel gepresenteerd om online CSA doeltreffender aan te pakken.

Het voorstel richt zich op twee punten. Het voorstel bestaat enerzijds uit regels die aanbieders van hostingdiensten en interpersoonlijke communicatiediensten[4] verplichten om het risico te beoordelen dat hun diensten worden gebruikt voor het verspreiden van materiaal van CSA en het benaderen van kinderen voor seksuele doeleinden (*grooming*). Ook dienen zij dit materiaal te melden aan het nieuw op te richten Europees Centrum en te verwijderen. Onder bepaalde omstandigheden kunnen bedrijven ook worden verplicht materiaal van CSA te detecteren. Anderzijds stelt de Commissie voor een Europees centrum (hierna: EU Centrum) inzake seksueel misbruik van kinderen op te richten. Het EU Centrum zal als expertise centrum fungeren om betrouwbare informatie over materiaal van CSA te verstrekken, de ontvangen meldingen van materiaal van CSA te beoordelen, relevante meldingen spoedig naar rechtshandhavingsautoriteiten door te sturen en steun aan slachtoffers te verlenen.

Het voorstel specificeert welke verplichtingen voor aanbieders van hostingdiensten en interpersoonlijke communicatiediensten moeten gaan gelden, maar er worden ook bevoegdheden toegekend aan en verplichtingen opgeworpen voor verschillende (al dan niet nog in te stellen) autoriteiten en het op te richten EU Centrum. Ten eerste moeten aanbieders van hostingdiensten en aanbieders van interpersoonlijke communicatiediensten de misbruikrisico's van hun diensten voor het verspreiden van materiaal van CSA en *grooming* beoordelen en beperken. Om dit risico te beperken moeten zij maatregelen treffen die hiertoe in verhouding staan en die onderworpen zijn aan robuuste voorwaarden en waarborgen. Lidstaten moeten ieder een coördinerende autoriteit aanwijzen die de risicobeoordeling moet gaan evalueren. Indien de coördinerende autoriteit vaststelt dat er ondanks de maatregelen sprake is van een blijvend aanzienlijk risico – en de waarschijnlijkheid en ernst van de potentiële negatieve effecten op betrokken partijen objectief en grondig zijn afgewogen, geïdentificeerd en beoordeeld – kunnen zij, op grond van case-by-case, een justitiële autoriteit of een onafhankelijke bestuursrechtelijke autoriteit verzoeken een detectiebevel uit te vaardigen voor bekend of nieuw materiaal van CSA of *grooming*. Bevelen kennen daarnaast een begin- en een eindtijd. De nationale justitiële autoriteit of onafhankelijke bestuursrechtelijke autoriteit kan mogelijke aanvullende voorwaarden stellen, zoals onafhankelijke auditing, versterkt toezicht door personen, of een verdere beperking van de tijd waarvoor het bevel geldt. Hierbij wordt rekening gehouden met de financiële en technologische capaciteiten en grootte van de dienstverlener. Een bevel behoort gericht en specifiek te zijn om eventuele negatieve effecten tot een minimum te beperken. Hierbij moet in ieder geval sprake zijn van een beperking tot een identificeerbaar deel of onderdeel van een dienst of specifieke gebruikers of groepen gebruikers. Aanbieders van hostingdiensten en aanbieders van interpersoonlijke communicatiediensten die een dergelijk detectiebevel ontvangen, mogen alleen materiaal detecteren aan de hand van indicatoren van CSA die door het EU Centrum zijn geverifieerd en verstrekt. Daarnaast worden aanbieders van hostingdiensten en aanbieders van interpersoonlijke communicatiediensten verplicht

[4] Volgens de verordening vallen hieronder voor het publiek beschikbare diensten op het gebied van interpersoonlijke communicatie, zoals berichtendiensten en e-maildiensten via het web. Aangezien sommige diensten, als neveneffect, rechtstreekse interpersoonlijke en interactieve uitwisseling van informatie mogelijk maken, vallen diensten zoals chatten en soortgelijke functies als onderdeel van spelletjes, het delen van beelden en het hosten van video's ook onder deze verordening.

materiaal van CSA te melden aan het EU Centrum zodra zij dit aantreffen. Bovendien wordt het voor aanbieders van hostingdiensten verplicht om materiaal binnen 24 uur te verwijderen. De coördinerende autoriteit krijgt de bevoegdheid om de aangewezen justitiële autoriteit of onafhankelijk bestuursrechtelijke autoriteit van een lidstaat te verzoeken een verwijderingsbevel aan de provider uit te vaardigen. Aanbieders van internettoegang zullen ook worden verplicht de toegang tot beelden en video's uit te schakelen die niet kunnen worden verwijderd, bijvoorbeeld omdat ze worden gehost in niet-coöperatieve jurisdicties buiten de EU. Tot slot wordt er voorgesteld app stores te verplichten ervoor te zorgen dat kinderen geen apps kunnen downloaden die hen kunnen blootstellen aan een hoog risico op *grooming*.

Daarnaast stelt de Commissie voor een nieuw EU Centrum ter voorkoming en bestrijding van CSA op te richten in Den Haag om optimaal gebruik te kunnen maken van de samenwerking met Europol. Het EU Centrum zal aanbieders van hostingdiensten en aanbieders van interpersoonlijke communicatiediensten ondersteunen bij het voldoen aan de nieuwe verplichtingen om risicobeoordelingen uit te voeren, materiaal van CSA op te sporen, te melden en te verwijderen en de toegang daartoe onmogelijk te maken. Daarnaast biedt het EU Centrum ondersteuning door databases met indicatoren van CSA aan te reiken ten behoeve van de detectie en door de meldingen van deze diensten in ontvangst te nemen. Het EU Centrum zal tevens ondersteuning bieden aan nationale rechtshandhavingsautoriteiten en Europol door meldingen van aanbieders van hostingdiensten en aanbieders van interpersoonlijke communicatiediensten te controleren op juistheid en door te sturen naar de juiste rechtshandhavingsautoriteit. Verder zal het EU Centrum voor lidstaten fungeren als kenniscentrum voor uitwisseling van *best practices* betreffende preventie en slachtofferhulp, om zo een empirisch onderbouwde aanpak te bevorderen. Voorts zal het EU Centrum slachtoffers van misbruik ondersteunen door hen te helpen het materiaal te (laten) verwijderen waarop hun misbruik staat afgebeeld.

b) Impact assessment Commissie

In de impact assessment wordt geconcludeerd dat kinderen in toenemende mate worden blootgesteld aan online risico's en schade, en dat materiaal van CSA zich in steeds grotere hoeveelheden online verspreidt. Hiervoor zijn drie oorzaken geïdentificeerd. Ten eerste, hoewel sommige dienstverleners vrijwillig actie ondernemen om materiaal van CSA online op te sporen, is dit onvoldoende effectief gebleken. Ten tweede, inefficiënties in de publiek-private samenwerking tussen onlinedienst verleners, maatschappelijke organisaties en overheidsinstanties belemmeren een doeltreffende bestrijding van CSA. Sommige lidstaten zijn reeds overgegaan tot het maken van nationale regelgeving om online CSA tegen te gaan, waardoor fragmentatie op de interne markt ontstaat. Ten derde, de inspanningen van de lidstaten om CSA te voorkomen en slachtoffers bij te staan zijn beperkt, verschillend, onvoldoende gecoördineerd en niet duidelijk doeltreffend.

De algemene doelstelling van het voorstel is om de werking van de interne markt te verbeteren door duidelijke, uniforme en proportionele EU-regels in te voeren ter voorkoming en bestrijding van CSA, met name door de rol en de verantwoordelijkheden van aanbieders van onlinediensten te verduidelijken. Met de voorkeursoptie wordt verwacht dat het initiatief de versnippering van de interne markt zal tegengaan en de rechtszekerheid zal verbeteren, de identificatie, bescherming en ondersteuning van slachtoffers van CSA zal verbeteren, de doeltreffendheid van preventie zal verbeteren en opsporingsonderzoeken zal vergemakkelijken.

De voorkeursoptie zal gevolgen hebben voor de fundamentele rechten van alle gebruikers van de betrokken diensten. Hierbij gaat het met name om het recht op privacy, het recht op de bescherming van persoonsgegevens, het recht op vrijheid van meningsuiting, vertrouwelijkheid van communicatie en het recht op vrijheid van informatie. De wetgeving moet waarborgen bevatten die rekening houden met de mate van inbreuk op de persoonlijke levenssfeer, afhankelijk van de aard van de online diensten, teneinde een proportioneel evenwicht te bereiken tussen de verschillende grondrechten, waaronder ook de rechten van het kind, en het vermogen om CSA beter tegen te gaan.

3. Nederlandse positie ten aanzien van het voorstel

a) Essentie Nederlands beleid op dit terrein

In 2018 is het nationale programma aanpak online CSA gestart. Deze nationale aanpak geschiedt langs een drietal lijnen: preventieve acties ter voorkoming van online CSA, een betere opsporing en vervolging en het internet schonen op basis van afspraken in publiek-privaat samenwerkingsverband met als sluitstuk bestuursrechtelijk handhaving door een onafhankelijke autoriteit waarvoor binnenkort een wetsvoorstel bij de Tweede Kamer zal worden ingediend.

Het kabinet zet in op het voorkomen van CSA. Het beleid richt zich op zowel potentiële slachtoffers als daders. Hierin is de voorlichting van ouders en kinderen een belangrijk element. Daarnaast wordt er ingezet op de screening van justitiële antecedenten bij iedereen die professioneel of als vrijwilliger wil werken met minderjarigen. Daarnaast richt de aanpak zich op het versterken van de strafrechtelijke aanpak. Daarbij wordt ook de internationale samenwerking op dit gebied verstevigd.

Gezien zijn hoogstaande ICT infrastructuur worden in Nederland gevestigde hostingbedrijven, helaas, vaak misbruikt voor het opslaan en distribueren van materiaal van CSA. Om die reden loopt Nederland voorop in de aanpak van online CSA materiaal. Het kabinet zet bij het opschonen van internet van materiaal van CSA in op effectieve zelfregulering, waarbij goedwillende aanbieders van hostingdiensten samenwerken met nationale meldpunten om materiaal van CSA op accurate wijze ontoegankelijk te maken. Vanuit het programma »aanpak online seksueel kindermisbruik» is er zowel op Europees als nationaal niveau ingezet op de verantwoordelijkheid van de sector om hun platformen en servers schoon te houden van materiaal van CSA. De sector zelf heeft zich gecommitteerd aan robuuste afspraken met betrekking tot het melden en verwijderen van materiaal van CSA (notice and take down – NTD) waarbij materiaal van CSA binnen 24 uur na een melding verwijderd dient te zijn. De Technische Universiteit Delft heeft speciale monitoringsoftware ontwikkeld waarmee meldingen van materiaal van CSA van het Nederlandse Expertisebureau Online Kindermisbruik (hierna: EOKM) kunnen worden gevolgd. Deze tool kan nauwkeurig nagaan welke dienst materiaal van CSA host, waar het is opgeslagen, hoe lang het na een melding online beschikbaar is en hoeveel materiaal van CSA er online circuleert. Uit de monitor[5] is gebleken dat 84% van de meldingen van materiaal van CSA die door het EOKM worden verstuurd, door de bedrijven binnen 24 uur worden opgevolgd met de verwijdering van de inhoud. Hieruit blijkt dat de sector nauw samenwerkt met het EOKM en de overheid om materiaal van CSA aan te pakken en dat de zelfregulering van de sector doeltreffend blijkt te zijn.

[5] Kamerstuk 31 015, nr. 203, bijlage.

Voor de aanpak van bedrijven die niet meewerken en niet adequaat reageren op een melding van materiaal van CSA wordt binnenkort een wetsvoorstel bij de Tweede Kamer ingediend voor een bestuursrechtelijke aanpak voor online materiaal van CSA. Hiermee wordt voorgesteld dat niet meewerkende bedrijven een bindende aanwijzing krijgen van – de momenteel in oprichting – Autoriteit online Terroristisch en Kinderpornografisch Materiaal (hierna: ATKM). Als een bedrijf niet adequaat reageert op de bindende instructie om materiaal van zijn diensten te verwijderen, kan door de ATKM een last onder dwangsom of bestuurlijke boete worden opgelegd. Het kabinet bepleit dat bedrijven die te maken krijgen met materiaal van CSA bovendien een inspanningsplicht zouden moeten krijgen: een inspanningsplicht om niet alleen reactief, maar ook proactief op te treden tegen de verspreiding van materiaal van CSA. De keuze van de te nemen passende en proportionele proactieve maatregelen zou in eerste instantie aan de bedrijven moeten worden overgelaten; de overheid zal slechts de resultaten monitoren. Elementen zoals de omvang van het bedrijf, de financiële draagkracht van het bedrijf en de mate van blootstelling aan het materiaal zouden een rol moeten spelen bij het bepalen van de maatregelen die redelijkerwijs van een bedrijf kunnen worden verwacht.

b) Beoordeling + inzet ten aanzien van dit voorstel

Het kabinet is voorstander van een Europese aanpak en onderstreept het belang hiervan in de strijd tegen online CSA. Aangezien het internet zich niet houdt aan landsgrenzen, is Europese samenwerking een essentieel onderdeel van de aanpak om dit probleem tegen te gaan. Om die reden verwelkomt het kabinet de algemene doelstelling van het voorstel. Het invoeren van duidelijke en uniforme EU-regels kan ervoor zorgen dat er efficiënter wordt samengewerkt in het voorkomen en bestrijden van CSA.

Het kabinet steunt het uitgangspunt uit het voorstel dat zowel Europese overheden als aanbieders van internetdiensten een verantwoordelijkheid hebben bij het voorkomen en bestrijden van CSA. Tegelijkertijd heeft het kabinet zorgen over een aantal aspecten van het voorstel omdat hiermee niet alleen een grote inbreuk lijkt te worden gemaakt op het recht op privéleven, het recht op gegevensbescherming en het communicatiegeheim van burgers, maar ook omdat hiermee de veiligheid van het internet(verkeer) kan worden geschaad. Deze zorgen richten zich specifiek op de verplichtingen die in het leven worden geroepen voor aanbieders van hostingdiensten en interpersoonlijke communicatiediensten om de inhoud te scannen en in specifieke gevallen mogelijk communicatie te ontsleutelen. Het kabinet zet zich ervoor in dat materiaal van CSA effectief kan worden bestreden, maar dat de inperking van grondrechten alleen plaatsvindt wanneer deze strikt noodzakelijk proportioneel en omkleed met waarborgen is. Hieronder zal meer in detail worden ingegaan op de waardering van de verschillende voorgestelde verplichtingen voor aanbieders van hostingdiensten en interpersoonlijke communicatiediensten.

Het kabinet is positief over het voorstel voor wat betreft het door aanbieders van hostingdiensten en interpersoonlijke communicatiediensten in beeld laten brengen van de misbruikrisico's van hun diensten middels een risicobeoordeling onder voorwaarden dat vertrouwelijkheid van communicatie niet in het geding komt. Het kabinet steunt in algemene zin ook een vorm van een zorgplicht, waarbij aanbieders van internetdiensten met veel meldingen een inspanningsplicht krijgen om niet alleen reactief, maar ook proactief de verspreiding van materiaal van CSA tegen te gaan. Het kabinet vindt het hierbij echter belangrijk dat uitvoerbaarheid in acht wordt genomen en de keuze van de te nemen passende en

proportionele maatregelen in eerste instantie aan de aanbieders van internetdiensten wordt overgelaten. Het kabinet is tevens positief over de in het voorstel opgenomen verplichting voor aanbieders van hostingdiensten en interpersoonlijke communicatiediensten om materiaal van CSA, zodra het ontdekt en gemeld, is binnen 24 uur te verwijderen. Het kabinet vindt het hierbij echter van belang dat lidstaten zelf de bestuursrechtelijke handhaving kunnen vormgeven. Hiertoe lijkt het voorstel van de Europese Commissie voldoende ruimte te bieden. Voorts zal het kabinet ervoor waken dat het voorstel niet leidt tot algemene monitoring en dat er goede waarborgen bestaan om te voorkomen dat materiaal onterecht als CSA wordt aangemerkt, zeker wanneer hierbij automatische besluitvorming wordt toegepast. De kans op fout negatieven is hierbij aanwezig, wat risico's met zich mee brengt voor de gebruiker.

Een ander onderdeel van het voorstel van de Commissie is een verplichting voor aanbieders van hostingdiensten en interpersoonlijke communicatiediensten om materiaal van CSA en *grooming* op hun servers op te sporen en te melden, nadat zij een detectiebevel hebben ontvangen. Bij detecteren van materiaal van CSA en *grooming* stelt het kabinet als uitgangspunt dat een inbreuk op privacy, veiligheid en het communicatiegeheim alleen plaats mag vinden in gevallen waarin dit strikt noodzakelijk, proportioneel en omkleed met waarborgen is.

Op basis van de voorliggende tekst van het voorstel ontbreekt een duidelijk beeld van wat realistisch is in de beperking van een detectiebevel in de tijd, deel of onderdeel van een dienst of specifieke personen of groepen personen. Het detectiebevel strekt in ieder geval verder dan wat verplicht is onder het bestaande recht omdat ook interpersoonlijke communicatiediensten verplicht zouden worden communicatie van hun gebruikers in te zien en te monitoren. In het voorstel ontbreken de technische details waardoor het onduidelijk is wat de effecten op encryptie zijn en welke verschillende vormen een detectiebevel kan aannemen. Dat kan leiden tot verzwakking van encryptie. Dit geldt ook voor diensten die nu end-to-end encryptie toepassen. Het kabinet heeft daarom wel kritische vragen naar aanleiding van het voorstel als het gaat om het detectiebevel. Dit ziet vooral op hoe een dergelijk bevel past binnen een proportionele en efficiënte aanpak om de opslag en verspreiding van materiaal van CSA tegen te gaan en het effect op de veiligheid van communicatie en andere data. Het kabinet zal zich ervoor inzetten om beter inzicht te krijgen over de verhouding met de grondrechten en de zorgen omtrent de risico's voor de bescherming van de verschillende grondrechten te adresseren. De kaders uit het kabinetsstandpunt over encryptie zijn leidend voor de Nederlandse inbreng en zullen conform dat standpunt en de afwegingen die daaraan ten grondslag liggen worden uitgedragen[6]. Gelet op de effectiviteit van de Nederlandse aanpak van materiaal van CSA waarbij géén verplichte detectie (en daaruit mogelijk voortvloeiende ontsleuteling en/of het ongericht scannen van inhoud) plaatsvindt, verwacht het kabinet in EU ook met minder vergaande maatregelen stappen te kunnen zetten in de bestrijding van materiaal van CSA.

Het kabinet is in beginsel wél voorstander van effectieve zelfregulering, waarbij goedwillende bedrijven samenwerken met meldpunten om materiaal van CSA op accurate wijze ontoegankelijk te maken. Ook blijft het kabinet voorstander van het uitbreiden van de huidige werkwijze

[6] Kabinetsstandpunt 2016 is dat het «op dit moment niet wenselijk is om beperkende wettelijke maatregelen te nemen ten aanzien van de ontwikkeling, de beschikbaarheid en het gebruik van encryptie binnen Nederland. In de internationale context zal Nederland deze conclusie en de afwegingen die daaraan ten grondslag liggen uitdragen.» Kamerstuk 26 643, nr. 383.

waarbij middels hashdatabases onmiskenbaar materiaal van CSA kan worden verwijderd van diensten. Een specifiek aandachtspunt voor het kabinet zijn de voorstellen op het gebied van *grooming*. De opsporing van *grooming* ligt gevoeliger, omdat het hierbij gaat om tekst waarbij de inhoud afhankelijk is van interpretatie en dus een grijs gebied kent. In Nederland is het detecteren van *grooming* exclusief belegd bij opsporingsinstanties. Het kabinet wil dit zo houden. Een wettelijk vastgelegde rol voor bedrijven om *grooming* zelf op te sporen, zoals voorgesteld door de Commissie, past niet bij dit uitgangspunt. Daarnaast is het kabinet kritisch wat betreft het gebruik door interpersoonlijke communicatiediensten van language identifiers als indicatoren om grooming op te sporen. Dergelijke software kan worden misbruikt voor andere doeleinden.

Verder worden in het voorstel aanbieders van hostingdiensten en interpersoonlijke communicatiediensten verplicht de toegang tot beelden en video's uit te schakelen die niet kunnen worden verwijderd. Het ontoegankelijk maken van gegevens op het internet raakt aan de vrijheid van meningsuiting. Het kabinet acht het van belang dat er duidelijke afspraken en waarborgen zijn om willekeurige inbreuk op de vrijheid van meningsuiting te voorkomen en in effectieve rechtsbescherming te voorzien wanneer content verwijderd wordt of ontoegankelijk wordt gemaakt.

In het voorstel wordt tevens gesproken over het rapporteren van de identiteit, of identiteit-gerelateerde data, aan het EU Centrum. Het kabinet staat kritisch tegenover een systeem waarbij anonimiteit op het internet niet langer mogelijk is en private partijen data verzamelen over de identiteit van hun gebruikers. Dit brengt risico's met zich mee.

Het voornemen tot oprichting van een EU Centrum beziet het kabinet positief. Een EU centrum zou een centrale rol kunnen spelen in een gezamenlijke aanpak van de verspreiding van materiaal van CSA. Volgens het kabinet ligt de meerwaarde van een EU Centrum zowel in de uitwisseling van *best practices* tussen de lidstaten en aanbieders van internetdiensten op het gebied van preventie, slachtofferhulp en het verwijderen van materiaal CSA van het internet, als in het aanjagen van innovatie en het doen van onderzoek naar nieuwere fenomenen, zoals *live-streaming*. Ook zou het EU Centrum een rol kunnen spelen bij ondersteunen van derde landen met het verhogen van hun weerbaarheid tegen online CSA, zodat ook internationaal aansluiting is in de aanpak van CSA.

Voor wat betreft het beheer door het EU Centrum van een database met indicatoren om aanbieders van hostingdiensten en interpersoonlijke communicatiediensten te ondersteunen bij het verwijderen van materiaal van CSA ziet het kabinet mogelijkheden voor het gebruik van hashdatabases van bekend materiaal. Voor wat betreft het detecteren van nieuw materiaal benadrukt het kabinet te allen tijde te willen voorkomen dat medewerkers van aanbieders van hostingdiensten en interpersoonlijke communicatiediensten worden geconfronteerd met materiaal van CSA.

Daarnaast zal het EU Centrum, volgens het voorstel, ondersteuning bieden aan nationale rechtshandhavingsautoriteiten en aan Europol door meldingen van aanbieders van internetdiensten op juistheid te controleren en door te sturen naar de juiste nationale rechtshandhavingsautoriteit. Het kabinet is nog benieuwd hoe de Commissie nationale meldpunten hierbij wil betrekken. Het kabinet acht het van groot belang dat opsporingsdiensten niet worden overspoeld door een groot aantal meldingen van bekend materiaal van CSA, zodat de opsporingsdiensten zich kunnen richten op het aanpakken van de daadwerkelijke daders en

kinderen te ontzetten uit acute misbruiksituaties. Het kabinet steunt het voorstel van de Commissie om het EU Centrum op te richten en om het te huisvesten bij, haar partner, Europol. Het kabinet houdt daarbij rekening met andere Nederlandse kandidaturen voor EU-agentschappen en neemt in ogenschouw dat de Commissie met het voorstel afwijkt van de gebruikelijke procedure bij de toekenning van vestigingslocaties van EU-agentschappen. De nabijheid van Europol heeft voor het EU Centrum onder andere voordelen voor de voorziene nauwe samenwerking, veilige informatie-uitwisseling en gedeeld gebruik van veilige infrastructuur, ook in samenwerking met de private sector.

Het kabinet ondersteunt het in het voorstel opgenomen voorstel tot het aanwijzen van een nationale coördinerende autoriteit in elke lidstaat die verantwoordelijk is voor de toepassing en handhaving van de verordening. Het kabinet heeft echter vragen omtrent de judiciële of onafhankelijke administratieve autoriteit die toestemming moet geven voor het uitvaardigen van een detectie- of verwijderingsbevel. De nationale coördinerende autoriteit moet volgens het voorstel bij een rechter of onafhankelijk administratieve autoriteit vragen om het uitvaardigen van dergelijke bevelen. Een dergelijke systematiek past niet goed in het Nederlandse bestuursrecht, maar past beter in het strafrecht. De vraag rijst waarom gekozen is voor een systematiek die afwijkt van de verordening terroristische content online (TOI), mede gelet op de uitvoerbaarheid van de onderhavige verordening. De inzet van het kabinet zal zijn om qua systematiek zo veel als mogelijk aan te sluiten bij de TOI-verordening. De nationale coördinerende autoriteiten zou volgens het kabinet het mandaat moeten hebben om een boete of dwangsom op te leggen aan aanbieders van hostingdiensten en interpersoonlijke communicatiediensten die geen adequate maatregelen nemen of niet meewerken aan de bestrijding van materiaal van CSA. Het kabinet onderschrijft het belang van onafhankelijke nationale autoriteiten, die niet hiërarchisch ondergeschikt zijn aan een politieke ambtsdrager, zodat een onafhankelijk oordeel gewaarborgd is en de mogelijkheid van overheidscensuur wordt voorkomen.

c) Eerste inschatting van krachtenveld

De verwachting is dat andere lidstaten een overwegend positieve houding zullen hebben ten opzichte van het voorstel. Met name het belang van de verantwoordelijkheid van aanbieders van online diensten, publiek-private samenwerking, het snel verwijderen van materiaal van CSA en het uitwisselen van *best practices* wordt breed gedeeld onder de EU-lidstaten. Tegelijkertijd is de verwachting dat lidstaten kritisch zullen zijn op het voorstel voor wat betreft de inbreuk op het recht gegevensbescherming, het recht op privacy en de vertrouwelijkheid en beveiliging van elektronische communicatie. Het Europees parlement acht bestrijding van CSA een belangrijk thema en zet zich hier actief voor in, maar zal gelijktijdig ook kritisch zijn op de onderdelen van het voorstel die toezien op het monitoren en verwijderen van content.

4. Beoordeling bevoegdheid, subsidiariteit en proportionaliteit

a) Bevoegdheid

Het oordeel van het kabinet over de bevoegdheid is positief. De voorgestelde rechtsgrondslag voor de verordening is artikel 114, VWEU. Dit artikel voorziet in de bevoegdheid voor de EU tot de vaststelling van maatregelen om de instelling en de werking van de interne markt te waarborgen. Het kabinet kan zich vinden in de keuze voor deze rechtsgrondslag, aangezien deze verordening behalve het tegengaan van de

verspreiding van materiaal van CSA ook tot doel heeft de digitale interne markt te verbeteren. Op het terrein van de interne markt is sprake van een gedeelde bevoegdheid tussen de EU en de lidstaten (artikel 4, tweede lid, onder a, VWEU).

b) Subsidiariteit

Het oordeel van het kabinet over de subsidiariteit is positief. De verordening heeft zowel tot doel om de werking van de interne markt te verbeteren door duidelijke, uniforme en proportionele EU-regels in te voeren ter voorkoming en bestrijding van CSA als tot doel om een doeltreffende bestrijding van online CSA mogelijk te maken met inachtneming van de grondrechten van alle betrokken partijen onder het EU-recht. Gezien de grensoverschrijdende dimensie van het internet en de verspreiding van materiaal van CSA kan deze doelstelling het beste op het niveau van de EU worden bereikt.

Gezien de grensoverschrijdende aard van online dienstverleners zou het uitblijven van EU-maatregelen ruimte laten voor nationale verschillen. Sommige lidstaten zijn reeds overgegaan tot het maken van nationale regelgeving om online CSA tegen te gaan. Deze nationale verschillen kunnen ervoor zorgen dat online dienstverleners hoge uitvoeringslasten hebben, omdat ze aan uiteenlopende pakketten nationale regels moeten voldoen en kunnen leiden tot ongelijke voorwaarden voor aanbieders in de hele EU, alsook tot mogelijke lacunes in de wetgeving als gevolge van deze nationale verschillen. Het voorstel beoogt daarom bestaande nationale verschillen weg te nemen en te voorkomen dat er in de toekomst nieuwe belemmeringen zouden kunnen ontstaan doordat lidstaten ieder afzonderlijk nationale regelgeving over dit onderwerp tot stand brengen. Deze mate van harmonisatie is op individueel lidstatenniveau niet te bereiken. Om deze redenen is optreden op het niveau van de EU gerechtvaardigd.

c) Proportionaliteit

Het oordeel van het kabinet is positief met een kanttekening. De verordening heeft zowel tot doel om de werking van de interne markt te verbeteren door duidelijke, uniforme en proportionele EU-regels in te voeren ter voorkoming en bestrijding van CSA als tot doel om een doeltreffende bestrijding van online CSA mogelijk te maken met inachtneming van de grondrechten van alle betrokken partijen onder het EU-recht.

Het voorgestelde optreden is geschikt om de doelstelling te bereiken en gaat ook deels niet verder dan noodzakelijk. Het kabinet steunt het uitgangspunt van het voorstel dat zowel Europese overheden als aanbieders van hostingdiensten een verantwoordelijkheid hebben bij het voorkomen en bestrijden van CSA. Het kabinet steunt in algemene zin ook een vorm van een zorgplicht, waarbij aanbieders van internetdiensten met veel meldingen een inspanningsplicht krijgen om niet alleen reactief, maar ook proactief de verspreiding van materiaal van CSA tegen te gaan. Het kabinet is tevens positief over de in het voorstel opgenomen verplichting voor aanbieders van hostingdiensten en interpersoonlijke communicatiediensten om materiaal van CSA, zodra het ontdekt en gemeld, is binnen 24 uur te verwijderen. Het voornemen tot oprichting van een EU Centrum beziet het kabinet positief. Een EU Centrum zou een centrale rol kunnen spelen in een gezamenlijke aanpak van de verspreiding van materiaal van CSA. Een aandachtspunt van het kabinet is de gekozen systematiek van de toepassing en handhaving door een nationale coördinerende autoriteit en de toestemming die nodig is voor

een detectie- of verwijderingsbevel van een judiciële of onafhankelijke administratieve autoriteit. Het kabinet acht deze niet geschikt voor toepassing in alle nationale rechtsstelsels en zal dan ook in de onderhandelingen inzetten op het wijzigen van dit onderdeel van het voorstel.

Het kabinet plaatst een kanttekening ten aanzien van de noodzakelijkheid van de verstrekkende verplichtingen die in het leven worden geroepen voor aanbieders van hostingdiensten en interpersoonlijke communicatiediensten om inhoud te scannen – en waar nodig de communicatie te ontsleutelen – en het melden, en zal dit kritisch volgen. Deze verplichtingen kunnen een grote inbreuk opleveren op het recht op privéleven, het recht op gegevensbescherming, het recht op vrijheid van meningsuiting, het communicatiegeheim van burgers, en hiermee kan de veiligheid van het internet(verkeer) worden geschaad. Uit het voorstel blijkt nog onvoldoende wat de technische effecten op de vormgeving van encryptie zijn en op de verschillende vormen die een detectiebevel kan aannemen. Het detectiebevel in de vorm zoals nu opgenomen in het voorstel staat niet meer in verhouding tot het te bereiken doel en gaat verder dan noodzakelijk, omdat ook interpersoonlijke communicatiediensten verplicht zouden worden communicatie van hun gebruikers in te zien en te monitoren. Het kabinet zal zich ervoor inzetten om beter inzicht te krijgen over de verhouding met de grondrechten en de zorgen omtrent de risico's voor de bescherming van de verschillende grondrechten te adresseren. Daarnaast acht het kabinet het van groot belang dat opsporingsdiensten niet worden overspoeld door een groot aantal meldingen van bekend materiaal van CSA. Het kabinet zal het belang hiervan bij de Commissie benadrukken.

5. Financiële consequenties, gevolgen voor regeldruk, concurrentiekracht en geopolitieke aspecten

a) Consequenties EU-begroting

De gevolgen van het voorstel voor de begroting zullen worden gedekt door de toewijzingen die in het meerjarig financieel kader (MFK) 2021–27 zijn voorzien in het kader van de financiële toewijzingen van het Fonds voor interne veiligheid. Het EU Centrum – als onafhankelijke entiteit gehuisvest bij Europol – wordt gefinancierd uit de EU-begroting, geraamd op eenmalige kosten van 5 miljoen euro en jaarlijkse kosten van 25,7 miljoen euro. Nederland is van mening dat de middelen gevonden dienen te worden binnen de in de Raad afgesproken financiële kaders van de EU-begroting 2021–2027 en dat deze moeten passen bij een prudente ontwikkeling van de jaarbegroting. Daarnaast moet de ontwikkeling van de administratieve uitgaven in lijn zijn met de ER-conclusies van juli 2020 over het MFK-akkoord.

b) Financiële consequenties (incl. personele) voor rijksoverheid en/ of medeoverheden

De jaarlijkse geschatte kosten van optie E worden voor overheidsinstanties ingeschat op 5,43 miljoen eenmalig en 825,57 miljoen structureel (zie tabel p.177/178, SWD(2022) 209 final, annex 3). Deze bedragen kunnen niet per land binnen de EU worden gespecificeerd. Ze zijn ook mede afhankelijk van wat al in een lidstaat op dit gebied wordt uitgevoerd en hoe dit – al dan niet – aansluit op de nieuwe regelgeving vanuit dit voorstel. Het is op basis van het huidige voorstel niet mogelijk voor de uitvoerende organisaties Politie en OM om de financiële consequenties te ramen. Dat komt ook omdat de set aan regels die het voorstel behelst nog ter discussie staat. Om die reden moet op dit punt dus een voorbehoud worden gemaakt. De onzekerheid wat betreft de kosten maakt ook een

opgave van de mogelijke dekking ervan in dit stadium nog niet mogelijk. In geval het EU Centrum in Den Haag zal worden gevestigd dan zal dat worden meegenomen in de huisvestigingsbehoefte van Europol. Indien er sprake is van budgettaire gevolgen voor Nederland, dan zullen deze worden ingepast op de begroting van de beleidsverantwoordelijke departementen, conform de regels van de budgetdiscipline.

c) Financiële consequenties en gevolgen voor regeldruk voor bedrijfsleven en burger

De jaarlijkse geschatte kosten van optie E worden voor serviceproviders ingeschat op 1.595,3 miljoen eenmalig en 1.463,3 miljoen structureel (zie tabel p.177/178, SWD(2022) 209 final, annex 3). Het gaat dan om kosten voor serviceproviders om maatregelen te nemen om online kindermisbruik op te sporen, te melden en te verwijderen, evenals de kosten om elke melding te verwerken. Bij de inschatting van de kosten is geen inschatting per lidstaat gemaakt. Het is dus lastig in te schatten hoe hoog de kosten uit zullen komen voor serviceproviders die in Nederland gevestigd zijn.

Uit de impact assessment blijkt dat MKB-bedrijven ook serviceproviders behoren die worden getroffen door de maatregelen die worden voorgesteld. Echter de Commissie geeft aan dat bijna 95% van de online meldingen van seksueel misbruik van kinderen door dienstverleners wordt gedaan door één grote aanbieder (Facebook), terwijl slechts 5 aanbieders verantwoordelijk zijn voor 99% van dergelijke meldingen. Hieruit blijkt dat het MKB slechts een klein deel van de huidige rapportages voor zijn rekening neemt. Volgens schattingen door de Commissie zouden ten minste 10.000 Europese dienstverleners waarop het voorstel betrekking heeft, MKB-bedrijven kunnen zijn. Hoewel het MKB slechts verantwoordelijk is voor een klein deel van de meldingen, lopen hun diensten een bijzonder risico om misbruikt te worden voor online seksueel kindermisbruik, aangezien ze vaak niet over de capaciteit beschikken om geschoold personeel in te huren of geavanceerde technologie in te zetten om dergelijke illegale inhoud op hun diensten te bestrijden. Voor het MKB gelden dus dezelfde verplichtingen als voor grotere aanbieders.

d) Gevolgen voor concurrentiekracht en geopolitieke aspecten

In de verordening zullen voor MKB[7] dezelfde verplichtingen gelden als voor grotere aanbieders. Volgens de impact assessment zijn de MKB bijzonder kwetsbaar voor uitbuiting van illegale activiteiten, waaronder CSA, niet in het minst omdat zij doorgaans over beperkte capaciteit beschikken om ultramoderne technologische oplossingen voor het opsporen van materiaal van CSA in te zetten of over gespecialiseerd personeel. Ook al beschikken ondernemingen misschien niet over dezelfde middelen om technologieën voor het opsporen van CSAM in hun producten te integreren, toch weegt dit negatieve effect volgens de Commissie niet op tegen het feit dat uitsluiting van deze verplichting een veilige ruimte zou creëren voor CSA en dus het doel van het voorstel zou ondermijnen.

De toepassing van technologieën voor de opsporing van CSA kan nieuwe hinderpalen opwerpen en een belasting vormen voor het MKB. Hoewel het EU Centrum technologieën kosteloos ter beschikking van MKB zou stellen, zou de continue werking van die technologieën ook tot hogere kosten kunnen leiden. Het MKB zou ook meer personele middelen moeten

[7] Ondernemingen met niet meer dan 250 personeelsleden, een omzet van 50 miljoen EUR en een jaarlijks balanstotaal van 43 miljoen EUR.

inzetten om CSA online op te sporen, te rapporteren en te verwijderen, onder meer door te reageren op follow-upverzoeken van rechtshandhavingsinstanties. De extra kosten zouden ertoe kunnen leiden dat het MKB minder middelen ter beschikking heeft voor onderzoek en innovatie, waardoor zijn concurrentienadeel ten opzichte van grote ondernemingen zou toenemen.

Het gezamenlijk optreden van Europese Unie tegen het hosten en verspreiden van materiaal van CSA kan tot gevolg hebben dat dergelijk materiaal verschuift naar aanbieders van hostingdiensten of interpersoonlijke communicatiediensten die buiten de Europese Unie zijn gevestigd. De oprichting van een EU Centrum zou een rol kunnen spelen bij ondersteunen van derde landen met het verhogen van hun weerbaarheid tegen online CSA.

6. Implicaties juridisch

a) Consequenties voor nationale en decentrale regelgeving en/of sanctionering beleid (inclusief toepassing van de lex silencio positivo)

Een verordening in de zin van artikel 288 VWEU is verbindend in al haar onderdelen en rechtstreeks toepasselijk in elke lidstaat. Op een aantal onderdelen is ter niettemin Nederlandse besluitvorming en wetgeving nodig. De nationale uitvoering van deze verordening vergt naar alle waarschijnlijkheid wetgeving in formele zin. De precieze inhoud en uitwerking daarvan is nog niet bekend. In inhoudelijk opzicht moet in ieder geval een nationale coördinerende autoriteit of autoriteiten worden opgericht, of aangewezen. Daarbij moet in ieder geval aandacht zijn voor de toedeling van de noodzakelijke bevoegdheden, waaronder een systeem van toezicht en handhaving en de bijbehorende rechtsbescherming. Tevens moet een judiciële of onafhankelijke autoriteit worden aangewezen die verzoeken tot het uitvaardigen van de verschillende soorten bevelen behandeld. Ook de verhouding van het voorstel tot artikel 7 van de Grondwet verdient bijzondere aandacht.

b) Gedelegeerde en/of uitvoeringshandelingen, incl. NL-beoordeling daarvan

Het voorstel bevat in artikel 3 een grondslag voor de Commissie om een gedelegeerde handeling vast te stellen, overeenkomstig artikel 290 VWEU. Overeenkomstig artikel 86 van het voorstel, krijgt de Commissie de bevoegdheid om de verordening aan te vullen met de nodige gedetailleerde regels voor de vaststelling en betaling van de kosten van de risicobeoordeling en de toepassing van de vrijstelling voor micro-, kleine en middelgrote ondernemingen. Het kabinet acht toekenning van deze bevoegdheden mogelijk, omdat het de vaststelling van een niet-essentieel onderdeel van de verordening betreft. Het betreft een aanvulling op de wetgevingshandeling, vandaar dat delegatie voor de hand ligt. Het kabinet vindt het bovendien wenselijk om deze bevoegdheden aan de Commissie toe te kennen om de wetgevingsprocedure niet te belasten en vanwege de flexibiliteit. Het kabinet kan zich vinden in de voorgestelde werkwijze.

In artikel 8 van de verordening krijgt de Commissie de bevoegdheid, overeenkomstig artikel 86, gedelegeerde handelingen vast te stellen tot wijziging van de bijlagen I en II inzake het detectiebevel, indien dat nodig is om de sjablonen te verbeteren met het oog op relevante technologische ontwikkelingen of opgedane praktijkervaring. Het voorstel kent de Commissie in artikel 13 verder de bevoegdheid toe om, overeenkomstig artikel 86, gedelegeerde handelingen vast te stellen om bijlage III inzake rapporteren van meldingen te wijzigen teneinde het sjabloon te verbe-

teren wanneer dat nodig is in het licht van relevante technologische ontwikkelingen of opgedane praktijkervaring. Het voorstel kent de Commissie in artikel 14 tevens de bevoegdheid toe om, overeenkomstig artikel 86, gedelegeerde handelingen vast te stellen tot wijziging van de bijlagen IV, V en VI inzake het verwijderbevel, indien dat nodig is om de sjablonen te verbeteren in het licht van relevante technologische ontwikkelingen of opgedane praktijkervaring. Het voorstel kent de Commissie in artikel 17 ook de bevoegdheid toe om, overeenkomstig artikel 86, gedelegeerde handelingen vast te stellen tot wijziging van de bijlagen VII en VIII inzake het bevel tot blokkeren, indien dat nodig is om de sjablonen te verbeteren met het oog op relevante technologische ontwikkelingen of opgedane praktijkervaring. Het kabinet acht toekenning van de bevoegdheid om gedelegeerde handelingen vast te stellen tot wijziging van de bijlagen I t/m VIII (artikel 8, 13, 14 en 17) mogelijk omdat het de vaststelling van niet-essentiële onderdelen van de verordening betreft. Dit geldt echter voor zover hier geen inbreuk wordt gemaakt op grondrechten. Het kabinet zal hierover opheldering vragen tijdens de onderhandelingen. Het kabinet acht toekenning van deze bevoegdheden wenselijk vanwege flexibiliteit en niet belasten gewone wetgevingsproces en kan zich vinden in de keuze voor delegatie, aangezien het een wijziging van de (bijlagen bij de) verordening betreft.

In artikel 47 van de verordening krijgt de Commissie de bevoegdheid, overeenkomstig artikel 86, gedelegeerde handelingen vast te stellen om deze verordening aan te vullen met de nodige gedetailleerde voorschriften onder andere betreffende de opzet van de databases van indicatoren, de verwerking van de meldingen door coördinerende instanties ten behoeve van het aanvullen van de databases, de inhoud van databases, toegang tot de databases en de controles en audits van de databases. Het kabinet twijfelt of de toekenning van deze bevoegdheid mogelijk is, omdat het de vaststelling van essentiële onderdelen van de verordening lijkt te betreffen. Het aanvullen van de verordening met de nodige gedetailleerde voorschriften inzake databases kan inbreuk maken op het recht op gegevensbescherming, het recht op privacy en de beveiliging van elektronische communicatie. Hierbij moet een belangrijke politieke beoordeling worden gemaakt of deze inmenging strikt noodzakelijk en proportioneel is en dit kan niet worden overgelaten aan die Commissie middels een gedelegeerde handeling. Het kabinet zal hier tijdens de onderhandelingen opheldering over vragen.

In artikel 84 van de verordening krijgt de Commissie de bevoegdheid, overeenkomstig artikel 86, gedelegeerde handelingen vast te stellen om deze verordening aan te vullen met de nodige sjablonen en gedetailleerde regels voor de jaarrapportage van relevante aanbieders van onlinediensten betreffende de vorm, de precieze inhoud en andere details van de rapporten en het rapportageproces overeenkomstig de punten 1, 2 en 3. Het kabinet acht toekenning van deze bevoegdheid mogelijk, omdat het de vaststelling van niet-essentiële onderdelen van de verordening betreft. Het kabinet acht toekenning van deze bevoegdheden wenselijk vanwege flexibiliteit en niet belasten gewone wetgevingsproces en kan zich vinden in de keuze voor delegatie, aangezien het een wijziging van de (bijlagen bij de) verordening betreft.

Het voorstel kent de Commissie in artikel 39 van het voorstel, overeenkomstig artikel 291 VWEU en Verordening (EU) nr. 182/2011 de bevoegdheid toe om een uitvoeringshandeling vast te stellen ter bepaling van de praktische en operationele regelingen voor de werking van de in lid 2 bedoelde informatie-uitwisselingssystemen en hun interoperabiliteit met andere relevante systemen. Het EU centrum zorgt voor de totstandbrenging en het onderhoud van een of meer betrouwbare en beveiligde

informatie-uitwisselingssystemen ter ondersteuning van de communicatie tussen de coördinerende autoriteiten, de Commissie, het EU Centrum, andere betrokken agentschappen van de Unie en de aanbieders van relevante diensten van de informatiemaatschappij. Deze uitvoeringshandelingen worden vastgesteld volgens de in artikel 87 van de verordening bedoelde raadplegingsprocedure zoals bedoeld in artikel 4 van Verordening (EU) nr. 182/2011. Het kabinet acht de toekenning van deze bevoegdheid mogelijk, omdat het de vaststelling van niet-essentieel onderdeel van de verordening betreft en tevens wenselijk om het gewone wetgevingsproces daarmee niet te belasten. De keuze voor uitvoering is passend, omdat door deze handelingen wordt gewaarborgd dat de verordening volgens eenvormige voorwaarden wordt uitgevoerd. Wel acht het kabinet de onderzoekprocedure als bedoeld in artikel 5 passender, gezien de toegang tot systemen en interoperabiliteit daarvan aanzienlijke implicaties kunnen hebben en zal tijdens de onderhandelingen inzetten op het gebruik van de onderzoeksprocedure.

c) Voorgestelde inwerkingtreding

De verordening is beoogd in werking te treden op de twintigste dag na die van de bekendmaking ervan in het Publicatieblad van de Europese Unie. De verordening wordt van toepassing 6 maanden na deze datum. Gelet op de gevolgen van deze Verordening voor zowel de Nederlandse overheid als de praktijk is deze termijn te kort, zeker nu uitvoering van deze verordening formele wetgeving vergt. Het kabinet acht deze termijn dan ook niet haalbaar en zet in op een termijn van ten minste 24 maanden.

d) Wenselijkheid evaluatie-/horizonbepaling

Het voorstel bepaalt dat de Commissie uiterlijk vijf jaar na de inwerkingtreding van de verordening, een evaluatie zal verrichten en bij het Europees parlement en de Raad een verslag indient. Op basis van de bevindingen van het verslag, met name over de vraag of de verordening leemten vertoont die in de praktijk relevant zijn, en rekening houdend met de technologische ontwikkelingen, zal de Commissie beoordelen of het toepassingsgebied van de verordening moet worden aangepast. Indien nodig zal de Commissie voorstellen indienen om de verordening aan te passen. Vervolgens zal om de zes jaar een evaluatie plaatsvinden.

e) Constitutionele toets

Een aantal verplichtingen uit het voorstel veroorzaakt een (potentieel grote) inbreuk op de grondrechten van de gebruikers van aanbieders van hostingdiensten en interpersoonlijke intercommunicatiediensten, waaronder het recht op privacy, het recht op de bescherming van persoonsgegevens, het recht op vrijheid van meningsuiting en het recht op vrijheid van informatie. Het gaat in het bijzonder om de verplichting voor aanbieders om materiaal van CSA en *grooming* op hun servers te detecteren en te melden, nadat zij een detectiebevel hebben ontvangen, en daarnaast om de verplichting tot het rapporteren van de identiteit, of identiteit-gerelateerde data, aan het EU Centrum, en de verplichting tot het uitschakelen van beelden en video's die niet kunnen worden verwijderd. Voor het kabinet is het van belang om, mede gelet op de technische gevolgen van het voorstel en de risico's die daarmee gepaard gaan, goed zicht te krijgen op de verhouding van het voorstel tot de verschillende grondrechten. De inbreuken op grondrechten moeten in verhouding staan tot het te bereiken doel en niet verder gaan dan noodzakelijk. Daarbij moeten waarborgen worden geboden die rekening houden met de mate van inbreuk op grondrechten, afhankelijk van de aard van de online diensten, zodat een proportioneel evenwicht wordt

bereikt tussen de verschillende grondrechten, waaronder ook de rechten van het kind, en het vermogen om CSA beter tegen te gaan. Op basis van het huidige voorstel acht het kabinet het van belang dat deze waarborgen worden verstevigd.

7. Implicaties voor uitvoering en/of handhaving

De uitvoeringsgevolgen zullen nader in kaart moeten worden gebracht. De voorstellen zullen naar verwachting wijzigingen van werkprocessen inhouden en extra capaciteit vergen van de betrokken diensten. De implicaties voor de uitvoering zijn afhankelijk van de keuze voor de toepassing van de maatregelen. Voor de uitvoerende organisaties kunnen de consequenties omvangrijk zijn, derhalve zet Nederland zich in voor een ruime implementatietermijn.

8. Implicaties voor ontwikkelingslanden

Geen implicaties voor ontwikkelingslanden.