Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2018–2019

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

Nr. 2706 **BRIEF VAN DE MINISTER VAN BUITENLANDSE ZAKEN**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 19 oktober 2018

Overeenkomstig de bestaande afspraken ontvangt u hierbij 10 fiches, die werden opgesteld door de werkgroep Beoordeling Nieuwe Commissievoorstellen (BNC).

Fiche: Verordening tot oprichting van het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging en het netwerk van nationale coördinatiecentra (Kamerstuk 22 112, nr. 2705)
Fiche: Verordening ter voorkoming van de verspreiding van online terroristische inhoud
Fiche: Mededeling voorstel uitbreiding bevoegdheden EOM (Kamerstuk 22 112, nr. 2707)
Fiche: Pakket vrije en eerlijke verkiezingen (Kamerstuk 22 112, nr. 2708)
Fiche: Richtlijn betreffende het einde van de omschakeling tussen winter- en zomertijd (Kamerstuk 22 112, nr. 2709)
Fiche: Mededeling Versterking van het Uniekader voor prudentieel en antiwitwastoezicht voor financiële instellingen (Kamerstuk 22 112, nr. 2710)
Fiche: Gewijzigd voorstel tot aanpassing van de verordeningen m.b.t. de Europese Toezichthoudende Autoriteiten en tot wijziging van de vierde anti-witwasrichtlijn (Kamerstuk 22 112, nr. 2711)
Fiche: Mededeling nieuwe Afrikaans-Europese alliantie voor duurzame investeringen en banen (Kamerstuk 22 112, nr. 2712)
Fiche: Mededeling Naar een doeltreffendere financiële architectuur voor investeringen buiten de EU (Kamerstuk 22 112, nr. 2713)
Fiche: Mededeling over efficiëntere besluitvorming in het GBVB (Kamerstuk 22 112, nr. 2714)

De Minister van Buitenlandse Zaken,
S.A. Blok

kst-22112-2706
ISSN 0921 - 7371
's-Gravenhage 2018

Fiche: Verordening ter voorkoming van de verspreiding van online terroristische inhoud

1. Algemene gegevens

a) *Titel voorstel*
Voorstel voor een verordening van het Europees Parlement en de Raad ter voorkoming van de verspreiding van terroristische online-inhoud
b) *Datum ontvangst Commissiedocument*
12 september 2018
c) *Nr. Commissiedocument*
COM/2018/640 final
d) *EUR-Lex*
https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52018PC0640&qid=1537273285749
e) *Nr. impact assessment Commissie en Opinie Raad voor Regelgevingstoetsing*
SEC (2018) 397
f) *Behandelingstraject Raad*
Raad Justitie en Binnenlandse Zaken
g) *Eerstverantwoordelijk ministerie*
Ministerie van Justitie en Veiligheid
h) *Rechtsbasis*
Art. 114 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

De aanhoudende aanwezigheid van terroristische inhoud op het internet vormt een ernstige bedreiging voor burgers en voor de samenleving in het algemeen. Dit wordt nog verergerd door de snelheid waarmee die inhoud zich over de diverse platforms verspreidt. Dit blijkt ook uit de wijze waarop terroristen misbruik hebben gemaakt van het internet tijdens verscheidene terroristische aanslagen binnen de Europese Unie. De maatregelen die tot nu toe zijn genomen om de verspreiding van terroristische inhoud tegen te gaan, zijn grotendeels vrijwillig van aard. De vrijwillige samenwerking brengt echter ook beperkingen met zich mee. Zo zijn niet alle aanbieders van hostingdiensten bij het EU-Internetforum betrokken en volstaan de schaal en het tempo van de vooruitgang bij de aanbieders van hosting diensten niet om dit probleem adequaat aan te pakken. De Commissie is er derhalve van overtuigd dat wetgeving nodig is om de nog altijd significante dreiging die van terroristische inhoud op het internet uitgaat, effectief te bestrijden. Het doel van de verordening is dat alle internetplatforms en alle nationale autoriteiten zich inzetten voor de bescherming van Europese burgers online, te verhinderen dat terroristische uitingen op internet kunnen worden verspreid, te komen tot een geharmoniseerde rechtskader dat de verlening van onlinediensten in de hele digitale eengemaakte markt faciliteert en te verzekeren dat voor alle aanbieders van hostingdiensten die hun diensten op de Europese Unie richten een gelijk speelveld behouden blijft. De Commissie stelt een aanpak voor die ervoor moet zorgen dat wanneer terroristische inhoud wordt aangetroffen die inhoud zo snel mogelijk wordt verwijderd; onlineplatforms maatregelen nemen om te voorkomen dat hun diensten worden misbruikt en verwijderde inhoud elders opnieuw verschijnt en/of

wordt geüpload; de grondrechten van burgers op vrijheid van meningsuiting en vrijheid van informatie te allen tijde worden beschermd. Daartoe wordt het volgende voorgesteld:

Verwijderingsverzoeken (referrals)

De huidige werkwijze waarbij een competente autoriteit[1] in de lidstaat internetbedrijven attendeert op terroristische inhoud, wordt in de verordening vastgelegd en geüniformeerd. Internetbedrijven beoordelen het verzoek en beslissen om:

- De content te verwijderen;
- De toegang tot de inhoud onmogelijk te maken;
- De nationale autoriteit om nadere verduidelijking te vragen.

Op grond van de verordening moet in de gebruikersvoorwaarden van internetbedrijven het beleid ten aanzien van het verwijderen van terroristische inhoud zijn opgenomen.

Verwijderingsbevel (removal order)

- In aanvulling op het systeem van verwijderingsverzoeken maakt de verordening het mogelijk om een verwijderingsbevel te geven aan een internetbedrijf. Bij een dergelijk bevel dient de content binnen één uur verwijderd te worden.
- Het hostingbedrijf kan tegen het verwijderingsbevel een rechtsmiddel aanwenden. Als het rechtsmiddel slaagt, wordt de inhoud teruggeplaatst. Als het rechtsmiddel wordt afgewezen of de daarvoor gestelde termijn ongebruikt verstrijkt, blijft het verwijderingsbevel van kracht en moet de inhoud permanent worden verwijderd.
- Als een verwijderingsbevel is uitgevaardigd, moet het hostingbedrijf drie maanden daarna aan de competente autoriteit rapporteren over de proactieve maatregelen die zijn genomen om terroristische online te bestrijden. Deze proactieve maatregelen dienen te worden genomen om her-uploaden te voorkomen en het detectievermogen van het internetbedrijf te verhogen.
- Zijn deze proactieve maatregelen onvoldoende, dan is de competente autoriteit bevoegd om specifieke additionele proactieve maatregelen van het bedrijf te vragen.

Betere bescherming voor onlineplatforms

Internet Service Providers die met terroristische inhoud te maken hebben, zullen hun diensten en hun gebruikers beter moeten beschermen tegen misbruik door terroristen. De Commissie stelt voor dat bedrijven (geautomatiseerde) proactieve maatregelen nemen, bijvoorbeeld om te voorkomen dat verwijderde terroristische inhoud opnieuw wordt geüpload. Om administratieve lasten voor bedrijven te voorkomen, moeten deze proactieve maatregelen in verhouding staan tot het risico en tot de mate waarin een internetplatform vatbaar is voor terroristische inhoud.

Nauwere samenwerking

Dienstverleners en lidstaten moeten een contactpunt aanwijzen dat altijd bereikbaar is, zodat verwijderingsverzoeken en meldingen beter en sneller kunnen worden opgevolgd. Dit heeft als doel een kader op te zetten voor samenwerking tussen internetbedrijven, de lidstaten en Europol.

[1] Een competente autoriteit is een door een lidstaat aan te wijzen autoriteit(en) die bevoegd zijn de maatregelen uit artikelen 4, 5, 6 en 18 uit de verordening uit te oefenen.

Waarborgen

Omdat moet worden voorkomen dat legale inhoud ten onrechte wordt verwijderd, worden aanbieders van hostingdiensten verplicht om te beschikken over doeltreffende klachtenmechanismen en moeten zij gebruikers inlichten wanneer door hen geplaatste inhoud wordt verwijderd, tenzij er belangrijke veiligheidsredenen zijn om dat niet te doen. Wanneer gebruik wordt gemaakt van geautomatiseerde detectiemiddelen, moet worden voorzien in menselijk toezicht en verificatie om te voorkomen dat inhoud ten onrechte wordt verwijderd. De lidstaten moeten zorgen voor doeltreffende rechtsmiddelen.

Meer transparantie en verantwoording

Aanbieders van hostingdiensten zullen jaarlijks een transparantieverslag moeten publiceren en de lidstaten worden verplicht om jaarlijks verslag uit te brengen aan de Commissie over hun maatregelen om de toegang tot terroristisch inhoud te beperken. De Commissie zal een programma opzetten voor toezicht op de resultaten en het effect van de nieuwe regels.

Strenge sancties

De Commissie stelt voor om doeltreffende, evenredige en afschrikkende sancties op te leggen wanneer niet wordt voldaan aan een verwijderingsbevel. Als een dienstverlener systematisch nalaat terroristische inhoud te verwijderen, moet een financiële sanctie worden opgelegd van maximaal 4% van de wereldwijde omzet over het vorige jaar.

b) Impact assessment Commissie

In de Impact Assessment wordt geconcludeerd dat – ondanks de op vrijwillige basis gemaakte stappen – een aantal maatregelen nodig is om het beleidsdoel van effectieve bestrijding van terroristische online content te realiseren. Uit het Assessment kwam naar voren dat een ruimere definitie van terroristische content, waaronder ook training en werving («recruitment») voor terrorisme vallen, de voorkeur geniet boven een definitie die alleen ziet op aanzetten («incite») tot terrorisme. Proactieve maatregelen die beperkt worden tot het voorkomen van het re-uploaden van terroristische content zou minder impact hebben vergeleken met maatregelen die er ook op toezien nieuwe vormen van terroristische content te detecteren. Ook wordt geconcludeerd dat verwijderingsverzoeken niet alleen van Europol moeten komen, maar ook van lidstaten omdat zij een belangrijke bijdrage kunnen leveren aan de algehele bestrijding van terroristische online content.

3. Nederlandse positie ten aanzien van het voorstel

a) Essentie Nederlands beleid op dit terrein

Digitale media zijn de afgelopen jaren steeds belangrijker geworden voor het verspreiden van het terroristische gedachtengoed, het geven van geweldsinstructies, het aangaan van contacten en het onderhouden van een netwerk. De terroristische uitingen online dragen bij aan radicaliseringsprocessen en werken faciliterend voor terroristische bewegingen, bijvoorbeeld als mechanisme voor mobilisatie. De kennis en kunde van terroristen op het terrein van digitale media neemt verder toe en zij benutten de mogelijkheden die moderne digitale media bieden.

De overheid werkt op nationaal en internationaal niveau aan het tegengaan van de verspreiding van terroristische uitingen. Onderdeel hiervan is het investeren in preventie met als doel de aanwas van de terroristische bewegingen te voorkomen. Binnen deze aanpak past het vroegtijdig onderkennen van extremistische structuren en activiteiten om (preventieve) interventies te kunnen faciliteren. Hierbij is ook het verwijderen van terroristische content van belang. Op dit moment vervult de Internet Referral Unit (IRU) van de politie hierin een belangrijke rol. De IRU laat terroristische content verwijderen door internetbedrijven. Dit gebeurt op vrijwillige basis via verwijderverzoeken.

b) Beoordeling + inzet ten aanzien van dit voorstel

Nederland is positief over de op vrijwillige basis genomen maatregelen door het bedrijfsleven, maar ziet tevens in dat wettelijke maatregelen nodig zijn om private betrokkenheid en effectiviteit te vergroten. Nederland is over het algemeen positief en verwelkomt deze inspanning van de Commissie. Het voorstel sluit aan op het beleidsmatige uitgangspunt dat de bestrijding van terroristische online content van wezenlijk belang is. Het is essentieel dat dergelijke inhoud zo snel mogelijk wordt verwijderd om verdere verspreiding ervan te voorkomen. Daarbij waardeert Nederland dat is gekozen voor een aanpak in samenwerking met internetbedrijven als uitgangspunt. Na een eerste bestudering van het voorstel zal Nederland aandacht vragen voor de volgende onderdelen van de verordening:

Uniforme aanpak

In dit voorstel van de Europese Commissie is niet uitgewerkt hoe deze verordening kan worden toegepast door de lidstaten. Dit brengt het risico met zich mee dat de lidstaten kiezen voor verschillende aanpakken. Hierdoor kunnen mogelijk verschillen ontstaan die de uniforme aanpak zouden kunnen bemoeilijken. De ene lidstaat zal kiezen voor een administratiefrechtelijke aanpak, de andere voor een strafrechtelijke aanpak. Hoewel Nederland ermee instemt dat het aan de lidstaten wordt gelaten om een aanpak in te richten die het beste past binnen het nationale rechtssysteem, zal Nederland er aandacht voor vragen dat een compromis wordt gevonden dat de samenwerking tussen de lidstaten stroomlijnt.

Handhaafbaarheid

Online content kan door bevoegde autoriteiten binnen de lidstaten gekwalificeerd worden als terroristisch. Deze autoriteiten beschikken tevens over de bevoegdheid om verwijderingsbevelen uit te vaardigen bij alle hostingbedrijven die diensten leveren binnen de EU, ongeacht de plaats van vestiging. Nederland onderkent dat er een risico is dat lidstaten het niet eens zijn over een oordeel. Het is onduidelijk welke mechanismen de verordening voorziet voor dergelijke situaties. Nederland heeft de voorkeur om bij een verwijderingsbevel aan een in Nederland gevestigd internetbedrijf tijdig te worden geïnformeerd. Nederland hecht tevens aan tijdige afstemming met de betrokken lidstaat over het bevel. Nederland zal zich hiervoor inzetten tijdens de onderhandelingen. Ditzelfde geldt voor de mogelijkheid dat de bevoegde autoriteiten van de ene lidstaat de bevoegdheid hebben om aan bedrijven in andere lidstaten rechtstreeks dwangmaatregelen op te leggen.

Waarborging fundamentele rechten

Nederland oordeelt dat voorkomen moet worden dat uitingen onterecht worden verwijderd. Dit betekent dat Nederland kritisch kijkt naar de in de verordening voorgestelde proactieve maatregelen, de autoriteit die verzoeken kan doen, en werking van *removal orders* en de rechtsbescherming tussen en in de lidstaten.

Nederland ondersteunt de vrijwillige benadering van de Commissie, waarin bedrijven gestimuleerd worden om met creatieve oplossingen de proactieve verwijdering van terroristische inhoud tegen te gaan. Daarbij komt kijken dat bedrijven tevens gebruik kunnen maken van bestaande structuren zoals de *database of hashes* die regelmatig door bedrijven wordt aangevuld. Artikel 6, tweede lid spreekt over een verplichting om het opnieuw uploaden van eerder verwijderde terroristische uitlatingen tegen te gaan. De betekenis van deze bepaling is nog onduidelijk. Nederland zal in het vervolg van de onderhandelingen de relatie tussen dit artikel en het censuurverbod in artikel 7 van de Grondwet nader bestuderen. Het kabinet zal hierbij nauwlettend in de gaten houden dat eventuele voorstellen niet in strijd zijn met het grondwettelijk censuurverbod. Nederland zal tevens verduidelijking vragen van de opties die hosting service providers hebben in de omgang met referrals onder artikel 5, vijfde lid.

Proactieve maatregelen

Hosting serviceproviders worden in artikel 6 van het voorstel verplicht om proactieve maatregelen te treffen die de verspreiding van terroristische inhoud tegengaan. Gezien de definitie van hosting serviceprovider vallen hier ook diensten onder die serverruimte leveren aan bedrijven. Het is niet duidelijk hoe dit soort diensten uitvoering moeten geven aan de verplichting om proactieve maatregelen te nemen. Dit dient in de onderhandelingen over het voorstel nader te worden verduidelijkt. Nederland zal zich ervoor inzetten tijdens de onderhandelingen dat de bedrijven die enkel en alleen dienen als serverruimte leverancier geen proactieve maatregelen hoeven te nemen die de verspreiding van terroristische content tegengaat. Deze verantwoordelijkheid dient te liggen bij bedrijven die hun website en/of sociale domein dagelijks beheren en het dichtst bij de consument staan. Daarnaast lijken de proactieve maatregelen niet uitvoerbaar met betrekking tot end-to-end encryptie. Nederland is derhalve van mening dat dit buiten de werking van de verordening dient te blijven.

Verhouding tot de e-commerce richtlijn

De Europese Commissie stelt in het voorstel dat gevolg geven aan de verplichtingen uit het voorstel er niet toe leidt dat hosting serviceproviders de beperkte aansprakelijkheid die zij genieten op grond van de e-commerce richtlijn (2000/31/EG) verliezen. Nederland is tevreden dat de Europese Commissie dit tot doel heeft. Nederland hecht daarbij aan zoveel mogelijk consistentie met de e-commerce richtlijn.

c) Eerste inschatting van krachtenveld

Tijdens een eerste bespreking van het voorstel in Raadsverband werd het voorstel door een meerderheid van de lidstaten positief ontvangen. De lidstaten maakten evenwel nog veel studie voorbehouden. Als aandachtspunten werden onder meer genoemd fundamentele rechten en waarborgen tegen over verwijdering, verschillen tussen de inrichting van de nationale systemen en de implementatietermijn. Voor een nadere

duiding van het krachtenveld zullen de verdere besprekingen moeten worden afgewacht.

4. Beoordeling bevoegdheid, subsidiariteit en proportionaliteit

a) Bevoegdheid

De door de Commissie voorgestelde rechtsgrondslag voor het voorstel is artikel 114 van het VWEU, dat voorziet in maatregelen om de werking van de interne markt te waarborgen.

Artikel 114 VWEU is de rechtsgrondslag om de voorwaarden te harmoniseren waaronder aanbieders van hostingdiensten grensoverschrijdende diensten kunnen verlenen op de interne digitale markt en om verschillen tussen de bepalingen van de lidstaten aan te pakken die anders de werking van de interne markt zouden kunnen belemmeren. De rechtsgrondslag kan ook worden gebruikt voor het voorkomen van toekomstige obstakels voor economische activiteit als gevolg van verschillen in de manier waarop nationale wetten zich kunnen ontwikkelen. Artikel 114 VWEU kan daarnaast ook worden aangewend om verplichtingen op te leggen aan dienstverleners die buiten het grondgebied van de EU zijn gevestigd en waar hun dienstverlening de interne markt beïnvloedt, aangezien dit noodzakelijk is voor het beoogde doel van de EU.

Het kabinet kan zich vinden in de keuze voor deze rechtsgrondslag voor dit voorstel, aangezien het voorstel behalve het tegengaan van de verspreiding van terroristische online-content ook tot doel heeft de werking van de digitale interne markt te verbeteren. Dit voorstel beoogt een geharmoniseerd rechtskader tot stand te brengen om misbruik van hostingdiensten voor de verspreiding van terroristische online-inhoud te voorkomen, teneinde de goede werking van de digitale eengemaakte markt te waarborgen en tegelijkertijd het vertrouwen en de veiligheid te garanderen.

b) Subsidiariteit

Het oordeel van Nederland over de subsidiariteit is positief. Gezien het grensoverschrijdend karakter van internet en de grensoverschrijdende dimensie van de verspreiding van terroristische uitingen is een aanpak op het niveau van de Unie noodzakelijk. De voorgestelde maatregelen kunnen bijdragen aan het vergroten van de doeltreffendheid van de acties van hostingproviders tegen online terroristische inhoud. Ook zal nadere regelgeving meer bedrijven dwingen om actie te ondernemen en dit versterkt mogelijk de integriteit van de interne digitale markt. Deze aspecten zijn op individueel lidstatenniveau niet te bereiken.

c) Proportionaliteit

Het oordeel van Nederland over de proportionaliteit is positief met een kanttekening. De maatregelen en het instrument van de verordening staan in beginsel in evenredige verhouding tot het daarmee beoogde doel: een uniforme, effectieve en tijdige verwijdering van terroristische uitlatingen van het internet en de versterking van de interne digitale markt. Hierbij dient te worden aangetekend dat de verordening op een aantal aspecten nadere uitwerking behoeft om de gestelde doelstellingen op passende wijze te kunnen verwezenlijken. Dit betreft onder andere de reikwijdte van de verordening, handhaafbaarheid, de verhouding van het voorstel tot de fundamentele rechten (waaronder onze Grondwet) en de rechtsbescherming. Het kabinet zal hiervoor aandacht vragen.

5. Financiële implicaties, gevolgen voor regeldruk en administratieve lasten

a) Consequenties EU-begroting

Nederland is van mening dat de benodigde EU-middelen gevonden dienen te worden binnen de in de Raad afgesproken financiële kaders van de EU-begroting 2014–2020 en dat deze moeten passen bij een prudente ontwikkeling van de jaarbegroting. De Commissie voorziet echter geen budgettaire implicaties voor de EU-begroting.

Zoals vastgelegd in de Kamerbrief van 1 juni 2018 over de Kabinetsappreciatie van het Commissie MFK-voorstel, maken de onderhandelingen over de toekomst van de verwijdering van terroristische online content voor wat betreft de financiële aspecten, integraal onderdeel uit van de onderhandelingen over het Meerjarig Financieel Kader (MFK) 2021–2027. Nederland hecht eraan dat besprekingen over de toekomst van de verwijdering van terroristische online content niet vooruitlopen op de integrale besluitvorming betreffende het MFK. De beleidsmatige inzet van Nederland bij de onderhandelingen zal ondersteunend moeten zijn aan de Nederlandse inzet in de MFK-onderhandelingen zoals hierboven toegelicht, te weten een ambitieus gemoderniseerd en financieel houdbaar MFK. Dit vraagt scherpe keuzes, én bezuinigingen. Om het vertrek van het Verenigd Koninkrijk op te kunnen vangen en nieuwe prioriteiten te kunnen financieren moeten substantiële bezuinigingen worden doorgevoerd. Binnen dit kader blijft vanzelfsprekend de ruimte bestaan om op de inhoud actief in te spelen op het verloop van de onderhandelingen.

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

In algemene zin kan worden gezegd dat een nationale autoriteit moet worden opgericht of aangewezen, met de benodigde bevoegdheden, bemensing en rechtsbescherming. De te verwachte kosten kunnen daardoor aanzienlijk zijn. Hierbij staat voorop dat kosten zo beperkt mogelijk worden gehouden en dat de budgettaire consequenties zoals gebruikelijk is, worden ingepast op de begrotingen van de beleidsverantwoordelijke departementen.

c) Financiële consequenties (incl. personele) voor bedrijfsleven en burger

De Commissie voorziet ondersteunende maatregelen om de samenwerking tussen nationale autoriteiten en Europol, alsmede de samenwerking met hostingdienstverleners te vergemakkelijken. Ook voorziet de Commissie in Research, Development and Innovation steun voor het ontwikkelen en treffen van technologische oplossingen. Ook is aangegeven dat aanvullende bewustmakings- en ondersteunende instrumenten voor het MKB kunnen worden ingezet na de goedkeuring van de verordening. Een kwantificatie van deze financiële voorzieningen is nog niet gegeven.

d) Gevolgen voor regeldruk/administratieve lasten voor rijksoverheid, decentrale overheden, bedrijfsleven en burger

De Europese Commissie heeft de administratieve lasten in door middel van een Impact Assessment (SEC (2018) 397) in kaart gebracht. Hierin worden de administratieve lasten voor zowel hosting serviceproviders en overheden geadresseerd per te nemen maatregel. Afhankelijk van de grootte van het bedrijf, het bereik van het bedrijf en de mate waarin een bedrijf de beoordeling van een verwijderverzoek of bevel zelf ter hand

neemt en afhankelijk van de mate waarvan reeds technische voorzieningen (bijv. in het kader van regulier bedrijfscontinuiteitsmanagement) zijn getroffen voor de verwijdering van illegale content, is het de inschatting van de Commissie dat 0,5 tot 4 fte per bedrijf nodig zijn. Op grond van het voorstel worden hosting serviceproviders verplicht om informatie die of de toegang toe te blokkeren op te slaan voor 6 maanden of langer. Nederland ziet dat dit lasten creëert voor het bedrijfsleven.

e) Gevolgen voor concurrentiekracht

De Commissie identificeert in haar Impact Assessment naast de voorgaande lasten voor de bedrijven tevens kansen binnen de EU met betrekking tot de ontwikkeling van technologieën voor (automatische) inhoud detectie, filtering en moderatie. Dit biedt kansen voor de Nederlandse internetindustrie.

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 WVEU is verbindend in al haar onderdelen en rechtstreeks toepasselijk in elke lidstaat. Op een aantal onderdelen is er 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 bevoegde autoriteit 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, de inrichting van een contactpunt voor de ontvangst van verwijderingsbevelen en verwijderingsverzoeken, en de bijbehorende rechtsbescherming. Ook de verhouding van het voorstel tot art. 7 van de Grondwet verdient bijzondere aandacht.

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

Niet van toepassing.

c) Voorgestelde implementatietermijn (bij richtlijnen), dan wel voorgestelde datum inwerkingtreding (bij verordeningen en besluiten) met commentaar t.a.v. haalbaarheid

Artikel 24 noemt als termijn voor inwerkingtreding 6 maanden. 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. Nederland acht deze termijn dan ook niet haalbaar en zet in op een termijn van ten minste 24 maanden.

d) Wenselijkheid evaluatie-/horizonbepaling

Nederland onderschrijft het belang van een goed werkend monitoringsregime. De verordening voorziet hier reeds in artikel 21 in.

7. Implicaties voor uitvoering en/of handhaving

Voor de uitvoerende organisaties kunnen de consequenties omvangrijk zijn, derhalve zet Nederland zich in voor een ruime implementatietermijn.

8. Implicaties voor ontwikkelingslanden

Niet van toepassing.