Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

36 138

Regels ter uitvoering van Verordening (EU) 2021/784 van het Europees Parlement en de Raad van 29 april 2021 inzake het tegengaan van de verspreiding van terroristische online-inhoud (PbEU 2021, L 172) (Uitvoeringswet verordening terroristische online-inhoud)

Nr. 3

MEMORIE VAN TOELICHTING

I. Algemeen deel

1. Inleiding

Dit wetsvoorstel geeft uitvoering aan Verordening (EU) 2021/784 van het Europees Parlement en de Raad van 29 april 2021 inzake het tegengaan van de verspreiding van terroristische online-inhoud (PbEU 2021, L172); (hierna: de verordening). De verordening is van toepassing met ingang van 7 juni 2022.[1]

Een verordening heeft rechtstreekse werking en vereist dan ook geen omzetting door de nationale wetgever. Wel is een aantal wettelijke bepalingen nodig om uitvoering te kunnen geven aan de verordening. In lijn met het staande beleid omtrent implementatie van EU-regelgeving bevat bijgaand wetsvoorstel dan ook uitsluitend de bepalingen die nodig zijn om uitvoering te kunnen geven aan de verordening. Daar waar de

[1] Zie de bijlage bij deze memorie van toelichting voor de transponeringstabel.

kst-36138-3
ISSN 0921 - 7371
's-Gravenhage 2022

verordening ruimte laat voor nationale keuzes is er voor gekozen zoveel mogelijk aan te sluiten bij de bestaande praktijk.[2]

Zoals bij brief van 20 november 2020 is aangekondigd, worden de in dit wetsvoorstel voorgestelde taken en bevoegdheden belegd bij een nieuw op te richten zelfstandig bestuursorgaan.[3] Krachtens artikel 6 van de Kaderwet zelfstandige bestuursorganen (hierna: de Kaderwet) is de Minister van Binnenlandse Zaken en Koninkrijksrelaties daarom medeondertekenaar van dit wetsvoorstel.

Hierna zal eerst worden ingegaan op de hoofdverplichtingen van de verordening, waarna de uitvoering van de verordening middels onderhavig voorstel aan bod zal komen.

2. De verordening

2.1 Totstandkoming verordening

Het internet biedt ongekende mogelijkheden om te communiceren, te werken, te socialiseren en informatie en inhoud te creëren, te verkrijgen en te delen met honderden miljoenen mensen over de hele wereld. De terroristische aanslagen op Europese bodem in de afgelopen jaren hebben laten zien dat het internet ook misbruikt wordt door terroristen om aanhangers te indoctrineren en te werven, terroristische activiteiten voor te bereiden en te faciliteren, hun wreedheden te verheerlijken, anderen ertoe aan te zetten in hun sporen te treden en angst in te boezemen.

Naast de onwenselijkheid dat misbruik wordt gemaakt van deze internetplatforms, bestaat een gevaar voor de nationale veiligheid, gelet op het feit dat sociale media de afgelopen jaren steeds belangrijker zijn geworden voor het verspreiden van het terroristische gedachtengoed, het geven van geweldsinstructies, het aangaan van contacten en het onderhouden van een netwerk.

Internetplatforms hebben een bijzondere maatschappelijke verantwoordelijkheid om hun gebruikers te beschermen tegen blootstelling aan terroristische inhoud en om de veiligheidsrisico's voor de samenleving als geheel te beperken. Deze verantwoordelijkheid vloeit voort uit het gegeven dat voor de verspreiding van terroristische online-inhoud gebruik wordt gemaakt van hun diensten. De dienstverlening van deze aanbieders bestaat uit de opslag en doorgifte van gegevens die van een ander afkomstig zijn.

De maatregelen die tot nu toe zijn genomen om de verspreiding van terroristische online-inhoud tegen te gaan, zijn grotendeels vrijwillig van aard. Sinds 2015 zijn in de Europese Unie verschillende initiatieven ondernomen om de beschikbaarheid en verspreiding van online terroristisch materiaal te beperken. De vrijwillige samenwerking brengt beperkingen met zich mee. Zo zijn niet alle aanbieders van hostingdiensten betrokken bij het EU-Internetforum, waarin de Europese Commissie, lidstaten en internetbedrijven gezamenlijk op vrijwillige basis afspraken maken over de aanpak van terroristische online-inhoud, en volstaan de schaal en het tempo van de vooruitgang bij de aanbieders van hosting diensten niet om dit probleem adequaat aan te pakken.

---

[2] Aanwijzingen 9.4 en 9.7 van de Aanwijzingen voor de regelgeving (Bijlage bij het besluit van de Minister-President, Minister van Algemene Zaken, van 18 november 1992 tot vaststelling van de (Stcrt. 1992, 230))

[3] Kamerstukken II 2020/21, 31 015, nr. 208.

De verordening kwam tot stand na een aanbeveling van de Europese Commissie van 1 maart 2018 over maatregelen om illegale online-inhoud effectief te bestrijden (2018/334/EU), waarbij de Europese Commissie een effectbeoordeling heeft verricht (SWD/2018/408 final). Voorts heeft het Europees Parlement er in zijn resolutie over onlineplatforms en de digitale eengemaakte markt van 15 juni 2017 bij de platforms op aangedrongen krachtigere maatregelen te nemen om illegale en schadelijke inhoud online aan te pakken ((2016/2276(INI)).

Op dit moment vormt de Richtlijn elektronische handel het algemene kader (de *lex generalis*) voor de verantwoordelijkheid en aansprakelijkheid van online platformen en aanbieders van hostingdiensten voor inhoud die derden bij hen opslaan, of via hen verspreiden.[4] In april 2022 is er een voorlopig politiek akkoord bereikt over de herziening van deze richtlijn door middel van de zogenaamde Digital Services Act (hierna: «DSA»). Die zal in de toekomst het algemene kader vormen. De DSA is een zogenoemde *lex generalis,* horizontale wetgeving, die geen sectorspecifieke verboden of bepalingen bevat. Wel bevat dit voorstel bepalingen om illegale online-inhoud aan te pakken. De TOI-verordening is een *lex specialis*: verticale sectorale wetgeving die verplichtingen bevat voor de sector om maatregelen te nemen tegen specifiek terroristische online-inhoud. De DSA is een aanvulling op de TOI-verordening en mag daaraan geen afbreuk doen. De DSA laat derhalve de TOI-verordening onverlet.

2.2 Inhoud verordening

Hierna volgt een bespreking van de inhoud op hoofdlijnen van de verordening.

Toepassingsbereik

Artikel 1 van de verordening bevat het onderwerp en het toepassingsgebied van de verordening. In het eerste lid is vastgelegd dat de verordening uniforme regels vaststelt om het misbruik van aanbieders van hostingdiensten voor de verspreiding onder het publiek van terroristische online-inhoud tegen te gaan, door deze zo snel mogelijk na signalering van het openbare internet te verwijderen. Met het openbare internet wordt bedoeld dat deel van het internet dat door een gebruiker direct kan worden benaderd, bijvoorbeeld via een link, een adres of een inlog. Wanneer voor de toegang tot informatie registratie of toelating tot een groep gebruikers vereist is, valt zij alleen onder het bereik van de verordening wanneer gebruikers die toegang tot de informatie wensen, automatisch worden geregistreerd of toegelaten zonder menselijke beslissing of selectie van wie toegang krijgt.[5] De verordening biedt derhalve geen grondslag voor het kennisnemen van bronnen waarbij een aanvullende handeling, die in feite niet volledig geautomatiseerd is, is vereist en waarvoor een «deurbeleid» bestaat in de vorm van een beoordeling van de accounthouder (in enige mate doorbreken van een beveiliging). Om verspreiding van terroristische online-inhoud onder het publiek tegen te gaan, bevat de verordening verschillende maatregelen gericht op aanbieders van hostingdiensten en verplichtingen voor de lidstaten.

[4] Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt.
[5] Zie overweging 14 bij de verordening.

Voor aanbieders van hostingdiensten geldt dat de verordening redelijke en evenredige zorgplichten bevat die door aanbieders van hostingdiensten moeten worden nagekomen om de verspreiding onder het publiek van terroristische online-inhoud via hun diensten tegen te gaan en, zo nodig, de snelle verwijdering van of de snelle blokkering van de toegang tot dergelijke inhoud te garanderen.

Voor de lidstaten geldt dat zij maatregelen moeten invoeren overeenkomstig het Unierecht en met passende waarborgen ter bescherming van de grondrechten, met name de vrijheid van meningsuiting en van informatie in een open en democratische samenleving, teneinde:

i) terroristische inhoud te identificeren en de snelle verwijdering ervan door aanbieders van hostingdiensten te garanderen; en
ii) de samenwerking tussen de bevoegde autoriteiten van de lidstaten, aanbieders van hostingdiensten en, waar passend, Europol, te faciliteren.

De verordening is op grond van artikel 1, tweede lid, van de verordening, van toepassing op aanbieders van hostingdiensten die, ongeacht de plaats van hun hoofdvestiging, in de Unie diensten aanbieden, voor zover zij informatie onder het publiek verspreiden. De verordening is derhalve ook van toepassing op aanbieders van hostingdiensten die buiten het grondgebied van de Europese Unie zijn gevestigd, maar op dat grondgebied diensten aanbieden.

Wat onder «aanbieder van hostingdiensten» en «in de Unie diensten aanbieden» moet worden verstaan is vastgelegd in artikel 2 van de verordening. Een «aanbieder van hostingdiensten» is ingevolge het eerste lid een aanbieder van diensten als gedefinieerd in artikel 2, eerste lid, van de verordening een aanbieder van diensten als gedefinieerd in artikel 1, punt b), van richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad[6], die erin bestaan informatie die door een aanbieder van inhoud is verstrekt, op diens verzoek op te slaan en onder het publiek verspreiden. Onder het publiek verspreiden houdt in dat de informatie beschikbaar wordt gesteld aan een mogelijk onbeperkt aantal personen. Als registratie wordt vereist is sprake van «onder het publiek verspreiden» als toegang automatisch is zonder menselijke beslissing of selectie. Bijvoorbeeld als er voor toegang moet worden ingeschreven met een e-mailaccount. De diensten van aanbieders van hostingdiensten zijn zeer divers. Het gaat bijvoorbeeld om diensten als sociale-mediaplatforms, webhosting, videostreaming, diensten voor het delen van video- en audiobestanden en beelden, bestandsdeling en andere clouddiensten voor zover daarmee informatie aan derden beschikbaar wordt gesteld. Ondernemingen die dit soort diensten aanbieden worden geacht om aanbieders van hostingdiensten te zijn zoals bedoeld in de verordening. E-mails of particuliere berichtendiensten vallen buiten deze verordening.

De verordening is van toepassing op terroristische inhoud. Wat onder terroristische inhoud wordt verstaan is gedefinieerd in artikel 2, zevende lid, onderdelen a tot en met e van de verordening, waarin wordt aangesloten bij de definities van de misdrijven en activiteiten genoemd in Richtlijn (EU) 2017/541 van het Europees Parlement en de Raad van 15 maart 2017 inzake terrorismebestrijding en ter vervanging van Kaderbesluit 2002/475/JBZ van de Raad en tot wijziging van Besluit 2005/671/JBZ van de Raad (hierna: de CT-richtlijn). Deze definities komen dan ook overeen met de definities in het Wetboek van Strafrecht. Het gaat

[6] Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad van 9 september 2015 betreffende een informatieprocedure op het gebied van technische voorschriften en regels betreffende de diensten van de informatiemaatschappij (PB EU 2015, L 241).

daarbij om materiaal dat aanzet tot het plegen van terroristische misdrijven of tot het bijdragen aan terroristische misdrijven, dat deze misdrijven aanmoedigt of verdedigt, dat instructies geeft voor het plegen van dergelijke misdrijven of dat het deelnemen aan de activiteiten van een terroristische groepering bevordert.

Van belang is dat artikel 1, derde lid, van de verordening bepaalt dat materiaal dat voor educatieve, journalistieke, artistieke of onderzoeksdoeleinden of met het oog op het voorkomen of bestrijden van terrorisme, onder het publiek wordt verspreid, met inbegrip van materiaal dat een uiting vormt van polemische of controversiële standpunten in het publieke debat, niet mag worden beschouwd als terroristische inhoud. Middels een beoordeling wordt het werkelijke doel van die verspreiding bepaald en wordt nagegaan of het materiaal voor die doeleinden onder het publiek wordt verspreid. Deze bepaling is mede gelet op artikel 1, vierde lid, van de verordening van belang. Daarin is opgenomen dat de verordening niet tot gevolg heeft dat «de in artikel 6 VEU bedoelde rechten, vrijheden en beginselen wordt gewijzigd en doet geen afbreuk aan de fundamentele beginselen inzake de vrijheid van meningsuiting en van informatie, met inbegrip van de vrijheid en het pluralisme van de media.» Op de verhouding van de verordening tot onder meer de vrijheid van meningsuiting zal nog nader in paragraaf 3.7 en 5 worden ingegaan.

Verwijderingsbevelen

Aanbieders van hostingdiensten worden op grond van artikel 3 en 4 van de verordening verplicht opvolging te geven aan een verwijderingsbevel op grond waarvan zij terroristische inhoud zo spoedig mogelijk en in elk geval binnen één uur na ontvangst van het verwijderingsbevel dienen te verwijderen of de toegang tot deze inhoud voor alle lidstaten in de Europese Unie dienen te blokkeren. Een dergelijk bevel kan worden uitgevaardigd door elke lidstaat van de Europese Unie, en kan worden gericht jegens elke aanbieder van hostingdiensten die zijn diensten aanbiedt in de Europese Unie, ongeacht zijn plaats van vestiging. Een aanbieder van hostingdiensten die zijn hoofdvestiging niet in de Unie heeft moet op grond van artikel 17 van de verordening schriftelijk een natuurlijke persoon of rechtspersoon aanwijzen als zijn wettelijke vertegenwoordiger in de Unie voor de ontvangst, naleving en handhaving van verwijderingsbevelen en besluiten van de bevoegde autoriteiten.

Voor alle aanbieders van hostingdiensten geldt dat zij op grond van artikel 15 van de verordening een contactpunt moeten aanwijzen of oprichten voor de ontvangst en snelle behandeling van verwijderingsbevelen door middel van elektronische middelen. De aanbieder van hostingdiensten moet er tevens voor zorgen dat de informatie over het contactpunt openbaar wordt gemaakt. Het contactpunt mag enkel voor operationele doeleinden dienen. Het contactpunt moet het mogelijk maken om verwijderingsbevelen elektronisch in te dienen en moet beschikken over de technische of personele middelen om die snel te kunnen verwerken. Het contactpunt hoeft niet in de Unie te zijn gevestigd. De aanbieder van hostingdiensten moet vrij zijn om gebruik te maken van een bestaand contactpunt, op voorwaarde dat het contactpunt de in deze verordening vastgestelde functies kan uitoefenen.

Indien een bevoegde autoriteit nog niet eerder een verwijderingsbevel heeft uitgevaardigd aan een aanbieder van hostingdiensten, verstrekt zij ten minste twaalf uur voor de uitvaardiging van het verwijderingsbevel informatie aan die aanbieder van hostingdiensten over de toepasselijke procedures en termijnen. Dit geldt niet als er sprake is van een noodgeval.

Artikel 3, derde lid, van de verordening bevat de informatie die een verwijderingsbevel in ieder geval moet bevatten. Het gaat onder meer om de identificatiegegevens van de bevoegde autoriteit die het verwijderingsbevel uitvaardigt en de authenticatie van het verwijderingsbevel door die bevoegde autoriteit, een voldoende gedetailleerde motivering waarom de inhoud als terroristische inhoud wordt beschouwd en het moet voldoende informatie bevatten om de inhoud te kunnen vinden, en wel door een exacte uniform resource locator (URL-adres) en, zo nodig, aanvullende informatie om de terroristische inhoud te kunnen identificeren. Daarnaast moet ook eenvoudig te begrijpen informatie worden meegestuurd over de rechtsmiddelen waar de aanbieder van hostingdiensten en de aanbieder van inhoud over beschikken. Bijlage I bij de verordening bevat het voor een verwijderingsbevel te gebruiken model. De bevoegde autoriteit stuurt het verwijderingsbevel aan het contactpunt van de aanbieder van hostingdiensten met gebruikmaking van elektronische middelen die een schriftelijk bewijs kunnen genereren op zodanige wijze dat authenticatie van de afzender mogelijk wordt, met inbegrip van de juistheid van de datum en het tijdstip van verzending en ontvangst van het bevel.

De aanbieder van de hostingdiensten stelt de bevoegde autoriteit zonder onnodige vertraging aan de hand van het in bijlage II van de verordening opgenomen model, in kennis van de verwijdering van de terroristische inhoud of van de blokkering in alle lidstaten van de Europese Unie (of EU) van de toegang tot de terroristische inhoud, met vermelding van met name het tijdstip van die verwijdering of blokkering. De verwijdering of blokkering moet immers zo spoedig mogelijk, maar uiterlijk binnen één uur na ontvangst van het verwijderingsbevel plaatsvinden. Indien er echter sprake van is dat de aanbieder van hostingdiensten dit bevel niet kan uitvoeren, vanwege overmacht of omdat het feitelijk onmogelijk is, met inbegrip van objectief te rechtvaardigen technische of operationele redenen, stelt hij de bevoegde autoriteit die het verwijderingsbevel heeft uitgevaardigd daar zonder onnodige vertraging van in kennis. Dit laatste aan de hand van het model opgenomen in bijlage III van de verordening. De termijn van één uur vangt in dat geval aan vanaf het moment dat de onmogelijkheid ophoudt te bestaan.
Ook kan het voorkomen dat de aanbieder van hostingsdiensten het verwijderingsbevel niet kan naleven omdat het kennelijke fouten bevat of niet voldoende informatie bevat om het uit te voeren. Ook dan stelt hij de bevoegde autoriteit die het verwijderingsbevel heeft uitgevaardigd zonder onnodige vertraging in kennis en vraagt hij de nodige verduidelijking aan de hand van het model in bijlage III van de verordening. De termijn van één uur vangt in dat geval aan vanaf het tijdstip van ontvangst van de verduidelijking.

Op grond van artikel 11, eerste en tweede lid, van de verordening is de aanbieder van een hostingdienst verplicht bij verwijdering of blokkering van de te verwijderen inhoud aan de aanbieder van inhoud informatie beschikbaar te stellen over die verwijdering of de blokkering van de toegang. Tevens dient de aanbieder van een hostingdienst de aanbieder van inhoud, wanneer deze daarom verzoekt, in kennis te stellen van de redenen voor de verwijdering en van zijn rechten om het verwijderingsbevel te betwisten, dan wel een afschrift van het verwijderingsbevel te verstrekken. Op grond van het derde lid van artikel 11 kan de bevoegde autoriteit echter besluiten dat de aanbieder van hostingdiensten geen informatie openbaar maakt over de verwijdering van of de blokkering van de toegang tot terroristische inhoud, indien dat noodzakelijk en evenredig is om redenen van nationale veiligheid, zoals het voorkomen, onderzoeken, opsporen en vervolgen van terroristische misdrijven. Dit zolang het nodig is, maar niet langer dan zes weken te rekenen vanaf dat besluit, waarbij de termijn met zes weken verlengd kan worden indien dat nog

steeds gerechtvaardigd is. Van belang is in dit kader dat op grond van artikel 8 van onderhavig voorstel er zogenoemde «deconflictie» plaatsvindt op basis waarvan de Autoriteit over de uitoefening van zijn taken en bevoegdheden overlegt met de politie, het openbaar ministerie, de Algemene Inlichtingen- en Veiligheidsdienst en de Militaire Inlichtingen- en Veiligheidsdienst. Dit om te voorkomen dat de inzet van taken en bevoegdheden van de betrokken organisaties elkaar doorkruisen.

Grensoverschrijdende verwijderingsbevelen

Een verwijderingsbevel kan grensoverschrijdend zijn, dat wil zeggen uitgevaardigd door de bevoegde autoriteit van een andere lidstaat dan waar de aanbieder van hostingdiensten zijn hoofdvestiging of wettelijke vertegenwoordiger heeft. Het internet is van nature grensoverschrijdend en inhoud die in één lidstaat wordt gehost, is normaal gesproken toegankelijk voor alle andere lidstaten. Alle overige onderdelen van de verordening zijn echter nationaal: de handhaving van de verplichtingen uit de verordening, het treffen van specifieke maatregelen en de mogelijkheid tot sanctionering zijn exclusief voorbehouden aan de autoriteit(en) van de lidstaat waar de desbetreffende aanbieder van hostingdiensten is gevestigd.

Aan grensoverschrijdende verwijderingsbevelen zijn in artikel 4 van de verordening nog enkele aanvullende eisen gesteld. Zo stuurt de bevoegde autoriteit die het verwijderingsbevel uitvaardigt in ieder geval een afschrift van het verwijderingsbevel aan de bevoegde autoriteit van de lidstaat waar de aanbieder van hostingsdiensten zijn hoofdvestiging of wettelijke vertegenwoordiger heeft.

De ontvangende bevoegde autoriteit heeft vervolgens op grond van artikel 4, derde lid, van de verordening, het recht om binnen 72 uur een met redenen omkleed besluit te nemen, houdende dat het verwijderingsbevel naar zijn oordeel in strijd is met de inhoud of strekking van de verordening, of in strijd is met de fundamentele rechten en vrijheden zoals neergelegd in het Handvest van de Grondrechten van de Europese Unie. Een dergelijke beslissing is bindend voor de uitvaardigende lidstaat, en verplicht de uitvaardigende lidstaat ertoe zijn verwijderingsbevel in te trekken. Het verwijderingsbevel heeft geen rechtsgevolgen meer en de aanbieder van hostingdiensten herstelt de inhoud of maakt die weer toegankelijk.

Zowel de aanbieders van hostingdiensten tegen wie het verwijderingsbevel zich richt als de aanbieder van inhoud kunnen een verzoek indienen bij de ontvangende bevoegde autoriteit om het verwijderingsbevel te toetsen. Alvorens de betreffende ontvangende bevoegde autoriteit een besluit neemt stelt hij echter eerst de bevoegde autoriteit, die het verwijderingsbevel heeft uitgevaardigd, in kennis van het voornemen en de redenen daartoe. Indien het besluit is genomen wordt zowel de bevoegde autoriteit die het verwijderingsbevel heeft uitgevaardigd in kennis gesteld, als de aanbieder van hostingdiensten, de aanbieder van inhoud en Europol overeenkomstig artikel 14 van de verordening.

Concreet betekent het voorgaande dat Nederland, net als de overige lidstaten, een beslissend veto heeft tegen een door een andere lidstaat uitgevaardigd verwijderingsbevel jegens een in Nederland gevestigde aanbieder van hostingdiensten. Via deze weg is het ook mogelijk om in Nederland een rechtsmiddel aan te wenden tegen de uitvoering van een grensoverschrijdend verwijderingsbevel uit een andere lidstaat.

In dit kader is overigens artikel 14 van de verordening relevant, op basis waarvan de bevoegde autoriteiten informatie uitwisselen, coördineren en samen met elkaar werken en, waar passend, met Europol, met betrekking tot verwijderingsbevelen, met name teneinde dubbel werk te voorkomen, de coördinatie te verbeteren en inmenging in onderzoeken in verschillende lidstaten te voorkomen. Deze samenwerking is mede van belang in verband met onderzoeken die door politie, AIVD en MIVD kunnen plaatsvinden en gelet op het overleg dat met deze partijen plaatsvindt in artikel 8 van onderhavig voorstel. Bij een grensoverschrijdend verwijderingsbevel zal op basis van artikel 14 van de verordening dan ook aandacht aan inmenging in onderzoeken in verschillende lidstaten besteed moeten worden.

Ter verduidelijking van bovenstaande procedure als voorbeeld een fictief scenario:
De autoriteit in België stuurt een verwijderingsbevel naar de in Nederland gevestigde aanbieder van hostingdiensten, waar passend Europol en de bevoegde autoriteit in Nederland. De bevoegde autoriteit in Nederland kan het van België ontvangen verwijderingsbevel onderzoeken, op:

- basis van een verzoek (te doen binnen 48 uur na ontvangst van het verwijderingsbevel) van de aanbieder van hostingdiensten aan de bevoegde autoriteit in Nederland om het verwijderbevel te onderzoeken[7];
- verzoek (te doen binnen 48 uur na ontvangst van het verwijderingsbevel) van degene wiens content is verwijderd[8];
- eigen initiatief (binnen 72 uur na ontvangst van het verwijderingsbevel)[9].

Dit onderzoek wordt binnen 72 uur na ontvangst van het verzoek van de aanbieder van hostingdiensten of van degene wiens content is verwijderd danwel na ontvangst van het verwijderingsbevel van de Belgische autoriteit afgerond. De bevoegde autoriteit in Nederland kan ten aanzien van een verwijderingsbevel besluiten dat sprake is van:

- Een ernstige of kennelijke inbreuk op de verordening;
- Een inbreuk op de grondrechten en vrijheden zoals verankerd in het Handvest van de grondrechten van Europese Unie.

Als de bevoegde autoriteit in Nederland van oordeel is dat sprake is van een dergelijke inbreuk, wordt dit besluit medegedeeld aan de Autoriteit in België, waar passend Europol en de aanbieder van hostingdiensten of de aanbieder wiens inhoud is verwijderd. Het oordeel van de bevoegde autoriteit in Nederland is bindend voor de uitvaardigende lidstaat. Het door de Belgische autoriteit uitgevaardigde verwijderingsbevel heeft geen rechtgevolg meer en de aanbieder van hostingdiensten zal direct het materiaal op zijn platform herstellen.

Specifieke maatregelen

De verordening verplicht aanbieders van hostingdiensten verder tot het treffen van specifieke maatregelen om de verspreiding van terroristische online-inhoud tegen te gaan, indien de aanbieder is blootgesteld aan terroristische online-inhoud. Dit is geregeld in artikel 5 van de verordening. Een aanbieder is blootgesteld aan terroristische online-inhoud indien de bevoegde autoriteit een «blootstellingsbesluit» heeft genomen en meegedeeld aan de aanbieder van hostingdiensten. De blootstelling wordt op basis van objectieve factoren vastgesteld, zoals het feit dat de

[7] Zie artikel 4, vierde lid van de verordening.
[8] Zie artikel 4, vierde lid van de verordening.
[9] Zie artikel 4, derde lid van de verordening.

aanbieder in de twaalf voorafgaande maanden twee of meer definitieve verwijderingsbevelen heeft ontvangen.

De aanbieder is in dat geval verplicht om in zijn algemene voorwaarden bepalingen op te nemen om het misbruik van zijn diensten voor de verspreiding van terroristische online-inhoud tegen te gaan en deze voorwaarden toe te passen. Ook is de aanbieder verplicht om specifieke maatregelen te nemen tegen misbruik van zijn diensten. De keuze ten aanzien van de te treffen maatregelen blijft bij de aanbieder. De maatregen moeten echter voldoen aan de in artikel 5, vierde lid, van de verordening opgenomen voorwaarden, waaronder de eisen dat deze doeltreffend, doelgericht en evenredig zijn en worden toegepast op een zorgvuldige en niet-discriminerende wijze waarbij rekening gehouden wordt met grondrechten, waaronder de vrijheid van meningsuiting. Gedacht kan worden aan maatregelen van technische of van operationele aard, bijvoorbeeld aan een systeem waarmee gebruikers terroristische online-inhoud bij de aanbieder kunnen melden. Als een aanbieder technische maatregelen treft, moet zijn voorzien in menselijk toezicht of verificatie door mensen. Bij de vaststelling welke maatregelen redelijkerwijs van een aanbieder kunnen worden gevergd spelen elementen als grootte, financiële draagkracht en de mate van blootstelling aan online terroristisch materiaal een rol. De verordening verplicht aanbieders van hostingdiensten niet tot een algemene vorm van toezicht, noch om actief naar online terroristisch materiaal te zoeken en ook niet om automatische instrumenten te gebruiken.[10]

Een aanbieder van hostingdiensten die specifieke maatregelen moet nemen stelt binnen drie maanden na ontvangst van het blootstellingsbesluit de bevoegde autoriteit van de lidstaat waar zijn hoofdvestiging of wettelijke vertegenwoordiger is gevestigd op de hoogte van de specifieke maatregelen die hij heeft genomen of voornemens is te nemen. Hierna rapporteert de aanbieder van hostingdiensten op jaarbasis. De bevoegde autoriteit kan de desbetreffende aanbieder van hostingdiensten de verplichting opleggen tot het treffen van (aanvullende) maatregelen indien op basis van de verslagen of andere objectieve factoren blijkt dat de specifieke maatregelen niet aan de voorwaarden voldoen. Ook in dit geval blijft de keuze van de te treffen maatregelen bij de aanbieder.

Een aanbieder van hostingdiensten kan te allen tijde de bevoegde instantie verzoeken om herziening van het blootstellingsbesluit en waar passend deze in te trekken of te wijzigen. Binnen drie maanden neemt de bevoegde autoriteit een met redenen omkleed besluit op basis van objectieve factoren. Intrekking van het blootstellingsbesluit heeft tot gevolg dat de verplichting tot het nemen van specifieke maatregelen vervalt.

Klachtenprocedure

Op grond van artikel 10 van de verordening is de aanbieder van hostingdiensten verplicht ervoor te zorgen dat er doeltreffend en toegankelijk een klacht kan worden ingediend door de aanbieders van inhoud tegen de verwijdering of blokkering van de toegang tot zijn materiaal ten gevolge van de hierboven genoemde specifieke maatregelen die genomen moesten worden vanwege blootstelling aan terroristische inhoud. In deze klacht verzoekt de aanbieder van inhoud om het herstel of het weer toegankelijk maken van de inhoud die is verwijderd of geblokkeerd. Indien

[10] Zie ook artikel 14 en 15 Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt.

na onderzoek door de aanbieder van de hostingdiensten blijkt dat de verwijdering of de blokkering onterecht was, herstelt hij de inhoud of deblokkeert deze zonder onnodige vertraging. Ook stelt de aanbieder van de hostingdienst de klager binnen twee weken na ontvangst van de klacht in kennis van het resultaat van de klacht en stelt hem in kennis van de redenen indien de klacht wordt afgewezen.

Bewaring van verwijderde of geblokkeerde inhoud

Artikel 6 van de verordening geeft regels over het bewaren van terroristische inhoud die op grond van een verwijderingsbevel of als gevolg van een specifieke maatregel is verwijderd of tot welke de toegang is geblokkeerd. De betrokken aanbieder van hostingdiensten is verplicht deze inhoud en de bijbehorende gegevens gedurende een periode van 6 maanden te behouden ten behoeve van een (bestuursrechtelijke) procedure, een klacht als bedoeld in artikel 10, of voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven. De terroristische inhoud wordt, op verzoek van de bevoegde autoriteit of rechterlijke instantie, gedurende een nader bepaalde periode bewaard indien en zolang zulks nodig is voor lopende administratieve of gerechtelijke (toetsings)procedures. Aanbieders van hostingdiensten zorgen ervoor dat voor de bewaarde terroristische inhoud en de bijbehorende gegevens passende technische en organisatorische waarborgen gelden. Daarbij moet worden voorzien in een hoog niveau van beveiliging van de betrokken (bijzondere) persoonsgegevens. Aanbieders van hostingdiensten evalueren die waarborgen en actualiseren deze indien nodig.

Transparantieverplichting voor aanbieders van hostingdiensten

Naast de bovengenoemde verplichtingen bevat artikel 7 van de verordening transparantieverplichtingen voor alle aanbieders van hostingsdiensten. Op grond van het eerste lid geldt dat aanbieders van hostingdiensten in hun algemene voorwaarden hun beleid vastleggen voor het tegengaan van de verspreiding van terroristische inhoud via hun diensten. Indien toepasselijk met inbegrip van een toelichting van de werking van specifieke maatregelen, waaronder indien van toepassing, het gebruik van automatische instrumenten.

Verder zijn aanbieders van hostingdiensten verplicht jaarlijks te rapporteren over de acties die zij hebben ondernomen of moeten nemen op grond van de verordening tegen de verspreiding van terroristische inhoud. Een dergelijk rapport wordt gepubliceerd en bevat onder meer informatie over de door de hostingdienst genomen maatregelen met betrekking tot de identificatie en verwijdering van of blokkering van de toegang tot terroristische inhoud en het aantal items dat is geblokkeerd naar aanleiding van verwijderingsbevelen of specifieke maatregelen. Dit is geregeld in artikel 7, tweede en derde lid van de verordening.

Transparantieverplichting voor bevoegde autoriteiten

Artikel 8 van de verordening schrijft verschillende transparantieverplichtingen voor aan de nationale bevoegde autoriteit(en). Deze autoriteit(en) publiceren jaarlijks en publiekelijk over:

– Het aantal uitgevaardigde verwijderingsbevelen, waaronder het aantal verwijderingsbevelen dat grensoverschrijdend ontvangen is en het aantal dat getoetst is onder artikel 4, informatie over de uitvoering die aan de verwijderingsbevelen is gegeven, met inbegrip van het aantal gevallen waarin terroristische inhoud verwijderd werd of de toegang

daartoe geblokkeerd werd en het aantal gevallen waarin terroristische inhoud niet verwijderd werd of de toegang daartoe niet geblokkeerd werd;
– Het aantal besluiten dat overeenkomstig de verordening is genomen, waaronder ook informatie over de uitvoering die aanbieders van hostingdiensten aan die besluiten hebben gegeven, met inbegrip van een beschrijving van de specifieke maatregelen.
– Het aantal keer dat het treffen van specifieke maatregelen aan een aanbieder van hostingdiensten is voorgeschreven, de daartegen ingestelde rechtsmiddelen, en de uitkomsten daarvan;
– Het aantal sancties dat is opgelegd.

Aanwijzing van bevoegde autoriteiten

Op grond van artikel 12, eerste lid, van de verordening wijst iedere lidstaat de bevoegde autoriteit (of bevoegde autoriteiten) aan voor het uitvaardigen en toetsen van verwijderingsbevelen, het toezien op de uitvoering van specifieke maatregelen en het opleggen van sancties. Daarnaast is iedere lidstaat verplicht ervoor zorg te dragen dat binnen de bevoegde autoriteit een contactpunt wordt aangewezen of opgericht en dat openbaar wordt gemaakt wie het contactpunt is. Dit contactpunt kan worden gebruikt voor de behandeling van verzoeken om verduidelijking en feedback met betrekking tot de door die bevoegde autoriteit uitgevaardigde verwijderingsbevelen. Vervolgens zijn de lidstaten verplicht om op uiterlijk 7 juni 2022 de Commissie in kennis te stellen van de bevoegde autoriteit. Ook van alle wijzigingen dienen de lidstaten de Commissie op de hoogte stellen, waarna de Commissie deze kennisgevingen in het Publicatieblad van de EU publiceert. Daarnaast stelt de Commissie een onlineregister op met de door de lidstaten gemelde bevoegde autoriteiten en contactpunten en actualiseert deze op regelmatige basis.

Artikel 13 stelt regels over de bevoegde autoriteiten. Ingevolge het eerste lid zorgen de lidstaten ervoor dat deze autoriteiten voldoende capaciteit en middelen tot hun beschikking hebben om hun taken en bevoegdheden op grond van de verordening uit te oefenen. Het tweede lid geeft regels over de onafhankelijkheid van deze bevoegde autoriteiten en bepaalt dat deze autoriteiten hun taken en bevoegdheden op objectieve en niet-discriminatoire wijze uitoefenen, met volledig respect voor de fundamentele rechten. Deze regels zijn opgenomen als belangrijke waarborg omdat het verwijderen van online uitingen, ook als deze terroristisch zijn, raken aan fundamentele rechten zoals de vrijheid van meningsuiting. Het tweede lid bepaalt daarom dat de bevoegde autoriteit geen instructies van andere instanties vraagt of aanvaardt in verband met de uitoefening van de taken die hem op grond van de verordening zijn toegewezen, behoudens toezicht overeenkomstig de nationale Grondwet.

Informatie-uitwisseling en samenwerking

In artikel 14 van de verordening zijn regels opgenomen over de noodzakelijke samenwerking tussen aanbieders van hostingdiensten, bevoegde autoriteiten en Europol. Zo wisselen bevoegde autoriteiten informatie uit, coördineren ze en werken samen met elkaar. Waar passend, werken bevoegde autoriteiten samen met Europol rondom verwijderingsbevelen, met name om duplicate verwijderingsbevelen te voorkomen.

De lidstaten moeten voor dat doel tevens voorzien in passende en veilige communicatiekanalen of -mechanismen om ervoor te zorgen dat de relevante informatie tijdig wordt uitgewisseld. Ook zijn de lidstaten verplicht samen te werken met de bevoegde autoriteiten uit andere lidstaten en om ervoor te zorgen dat de bevoegde autoriteiten over alle

relevante informatie beschikken voor het toezicht op de specifieke maatregelen en de sanctionering. Lidstaten en aanbieders van hostingdiensten mogen met het oog op de effectieve uitvoering van de verordening en de voorkoming van dubbel werk, gebruikmaken van speciale instrumenten, met inbegrip van instrumenten die zijn ingesteld door Europol, met name om:

1. verwijderingsbevelen en de feedback over verwijderingsbevelen te verwerken en
2. de samenwerking met het oog op het bepalen en uitvoeren van specifieke maatregelen op grond van artikel 5 te faciliteren.

Het vijfde lid van artikel 14 regelt dat aanbieders van hostingdiensten die op de hoogte raken van terroristische inhoud die een onmiddellijk levensbedreigend gevaar vormen, snel de autoriteiten inlichten die in de betrokken lidstaten bevoegd zijn voor het onderzoek en de vervolging van strafbare feiten. Indien het onmogelijk is de betrokken lidstaten te bepalen, stellen de aanbieders van hostingdiensten het contactpunt van de bevoegde autoriteit in de lidstaat waar zij hun hoofdvestiging hebben of waar hun wettelijke vertegenwoordiger zijn verblijf- of vestigingsplaats heeft, daarvan in kennis en geven zij de informatie over die terroristische inhoud door aan Europol met het oog op passende opvolging. Tot slot worden de bevoegde autoriteiten aangemoedigd afschriften van de verwijderingsbevelen toe te zenden aan Europol, zodat Europol een jaarverslag kan opstellen met een analyse van de soorten terroristische inhoud waarover verwijderingsbevelen op grond van de verordening zijn uitgevaardigd. De grondslag voor uitwisseling met Europol is gelegen in artikel 14, eerste respectievelijk vijfde lid van de verordening.

Artikel 21 van de verordening bevat een verplichting tot monitoring voor lidstaten op grond waarvan de lidstaten bij hun bevoegde autoriteiten en de onder hun rechtsmacht vallende aanbieders van hostingdiensten, informatie verzamelen over de maatregelen die deze overeenkomstig de verordening in het daaraan voorafgaande kalenderjaar hebben genomen. Deze informatie zenden zij elk jaar uiterlijk op 31 maart aan de Commissie. Deze informatie omvat onder meer het aantal verwijderingsbevelen, de genomen specifieke maatregelen, het aantal verzoeken om toegang tot inhoud die aanbieders van hostingsdiensten hebben bewaard op verzoek van de bevoegde autoriteit of een rechterlijke instantie en dergelijke. De Commissie stelt aan de hand van deze informatie uiterlijk op 7 juni 2023 een gedetailleerd programma vast voor de monitoring van de resultaten en effecten van de verordening. Het monitoringprogramma vermeldt de indicatoren en middelen waarmee en de tijdstippen waarop de gegevens en ander nodig bewijsmateriaal moeten worden verzameld. Het specificeert de maatregelen die de Commissie en de lidstaten bij het verzamelen en analyseren van de gegevens en ander bewijsmateriaal moeten nemen om de voortgang te monitoren en de verordening vervolgens op grond van artikel 23 te evalueren.

Rechtsmacht

Artikel 16 geeft regels over de rechtsmacht en jurisdictie. Het eerste lid bepaalt dat de lidstaat waar de aanbieder zijn hoofdvestiging heeft, rechtsmacht heeft voor de artikelen 5 (specifieke maatrelen naar aanleiding van een blootstellingsbesluit), 18 (sanctionering) en 21 (monitoring). De handhaving van de verordening is daarmee een louter nationale aangelegenheid. Daarentegen is elke bevoegde autoriteit bevoegd om een verwijderingsbevel uit te vaardigen, ook als dat is gericht jegens een in een ander lidstaat gevestigde aanbieder van hostingdiensten. De handhaving van een dergelijk verwijderingsbevel, zoals het zo nodig afdwingen van de naleving daarvan en het opleggen van

sancties, berust echter exclusief bij de bevoegde autoriteit van de lidstaat waar de aanbieder van hostingdiensten zijn hoofdvestiging heeft of waar de wettelijke vertegenwoordiger zijn verblijf- of vestigingsplaats heeft.

Zoals hierboven reeds beschreven is de verordening van toepassing op elke aanbieder van hosting diensten die diensten aanbiedt binnen de Europese Unie, ongeacht diens plaats van vestiging. Artikel 17 verplicht tot het aanwijzen van een wettelijke vertegenwoordiger in de EU indien een aanbieder zijn hoofdvestiging niet in de EU heeft voor de ontvangst, naleving en handhaving van verwijderingsbevelen en besluiten van de bevoegde autoriteiten. De aanbieder van hostingdiensten dient zijn wettelijke vertegenwoordiger de nodige bevoegdheden en middelen te verlenen om verwijderingsbevelen en besluiten na te leven en om met de bevoegde autoriteiten samen te werken. De wettelijke vertegenwoordiger kan aansprakelijk worden gesteld voor inbreuken op de verordening, alsmede de aansprakelijkheid van de aanbieder van hostingdiensten.

Een aanbieder van hostingdiensten die zijn hoofdvestiging niet in de Unie heeft, wordt geacht onder de rechtsmacht te vallen van de lidstaat waar zijn wettelijke vertegenwoordiger zijn verblijf- of vestigingsplaats heeft. Indien een aanbieder van hostingdiensten heeft verzuimd een wettelijke vertegenwoordiger aan te wijzen, hebben alle lidstaten rechtsmacht. Indien een bevoegde autoriteit in het laatstgenoemde geval zijn rechtsmacht uitoefent stelt hij alle andere lidstaten daarvan in kennis.

Sanctionering en rechtsbescherming

Zoals eerder opgemerkt is de handhaving van de verordening een louter nationale aangelegenheid. Artikel 18 geeft daarover regels. Het is aan de lidstaat om de aard en hoogte van de sanctie te bepalen. De sanctie dient doeltreffend, evenredig en afschrikkend te zijn. Verder bevat de verordening regels omtrent een doeltreffende voorziening in rechte. Op deze onderwerpen zal in paragraaf 3.4 nader worden ingegaan. Wel stelt de verordening dat bij systematisch of aanhoudend verzuim, een financiële sanctie wordt opgelegd van ten hoogste 4% van de mondiale omzet van de aanbieder van hostingdiensten in het voorafgaande boekjaar.

3. Wetsvoorstel en uitvoering

3.1. De bevoegde instantie: keuze voor een zbo

Zoals hierboven beschreven verplichten de artikelen 12 en 13 tot het aanwijzen van een bevoegde autoriteit/bevoegde autoriteiten die aan de aldaar opgenomen voorwaarden voldoet/voldoen en de taken en bevoegdheden op grond van de verordening uitvoert/uitvoeren. Daarnaast volgt uit de doelstellingen van de verordening en meer specifiek artikel 1, eerste lid, onderdeel b, dat de lidstaten maatregelen invoeren ten einde terroristische inhoud te identificeren, de snelle verwijdering door aanbieders van hostingdiensten te garanderen en samen te werken met bevoegde autoriteiten van andere lidstaten, aanbieders van hostingdiensten en waar passend Europol.
De verordening vereist dat de lidstaten ervoor zorgen dat hun bevoegde autoriteiten hun taken uit hoofde van de verordening op objectieve en niet-discriminerende wijze uitoefenen met volledige eerbiediging van de grondrechten. Ook vereist de verordening dat de bevoegde autoriteiten instructies vragen noch aanvaarden van andere instanties met betrekking tot de uitoefening van hun taken uit hoofde van artikel 12, lid 1, van de verordening zijnde:
a) het uitvaardigen van verwijderingsbevelen op grond van artikel 3;
b) het toetsen van verwijderingsbevelen op grond van artikel 4;

c) het toezien op de uitvoering van specifieke maatregelen op grond van artikel 5;
d) het opleggen van sancties op grond van artikel 18.

Het voorgaande betekent dat geen andere instantie dan de bevoegde autoriteit invloed mag uitoefenen op beslissingen van inhoudelijke aard als het om de vrijheid van meningsuiting gaat.

Keuze voor het bestuursrecht

Verkend is of de Autoriteit vorm moest krijgen binnen het strafrecht of het bestuursrecht. Bij de keuze voor het bestuursrecht was ten eerste relevant dat de verordening een reparatoir karakter heeft. De verordening heeft niet tot doel om diegenen die terroristische online-inhoud produceren en op internet plaatsen op te sporen en te vervolgen; de verordening is er louter op gericht om terroristische online-inhoud zo snel mogelijk ontoegankelijk te maken en dit zo nodig af te dwingen om verdere verspreiding tegen te gaan. Ten tweede was relevant dat een aantal taken uit de verordening, zoals de bevoegdheid voor de Autoriteit om te bezien of de door de aanbieder van hostingdiensten getroffen maatregelen afdoende zijn, zich inhoudelijk minder goed leent voor uitvoering binnen het strafrecht.

In het bijzonder is bezien of kon worden volstaan met de in artikel 125p wetboek van Strafvordering (Sv) neergelegde strafrechtelijke bevoegdheid tot het geven van een bevel tot ontoegankelijkmaking. Hier wordt ook door de Afdeling naar gevraagd in haar advies. Hiervoor is niet gekozen. Van belang daarbij is dat strafrechtelijke vervolging van een aanbieder van hostingdiensten, als deze in beeld komt bij het Openbaar Ministerie (hierna: OM), wegens de middels zijn diensten opgeslagen en verspreide gegevens slechts in uitzonderlijke gevallen aan de orde is. In feite moet het dan gaan om een situatie waarin een aanbieder niet langer optreedt als een tussenpersoon die louter (en passief) gegevens van een ander doorgeeft, maar ook inhoudelijke betrokkenheid heeft of verkrijgt met de terroristische online-inhoud. Alleen dan is de aanbieder van een hosting-dienst immers strafbaar voor het via zijn diensten opslaan en verspreiden van terroristische online-inhoud. Een dergelijke situatie doet zich, gelet op de neutrale en passieve rol die deze aanbieders vervullen, zelden voor.

Daarnaast verplicht de verordening tot een specifiek op terroristische online-inhoud toegesneden instrumentarium. Artikel 125p Sv bevat de bevoegdheid van de Officier van Justitie om in het geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid, Sv een strafrechtelijk bevel tot het ontoegankelijk maken van online-inhoud uit te vaardigen aan een aanbieder van een communicatiedienst. Op grond hiervan dient deze terstond alle maatregelen te nemen die redelijkerwijs van hem kunnen worden gevergd om bepaalde gegevens die worden opgeslagen of doorgegeven ontoegankelijk te maken voor zover dit noodzakelijk is ter beëindiging van een strafbaar feit of ter voorkoming van nieuwe strafbare feiten. Artikel 67, eerste lid, Sv bevat niet alleen terroristische misdrijven maar is breder van aard. Ten slotte zou het (veel) vaker aanwenden van de in artikel 125p Sv neergelegde bevoegdheid een te groot beslag leggen op de capaciteit van het OM. Door de ontoegankelijkmaking van terroristische online-inhoud te beleggen bij een daarvoor toegeruste Autoriteit, kan de capaciteit van het OM worden vrijgehouden ten behoeve van de opsporing en vervolging van personen die zelf terroristische online-inhoud produceren en verspreiden.

Gelet op het voorgaande is er voor gekozen de Autoriteit binnen het bestuursrecht vorm te geven.

Keuze voor een nieuwe zbo

Het kabinetsbeleid neemt tot uitgangspunt dat publieke taken onder volledige ministeriële verantwoordelijkheid worden uitgevoerd, zodat de verantwoordelijke bewindspersoon op alle aspecten van de uitvoering (politiek) aanspreekbaar is.[11] Dat laat onverlet dat het in bepaalde situaties noodzakelijk kan zijn een zelfstandig bestuursorgaan in te stellen. Dat is mogelijk als is voldaan aan één van de in artikel 3, eerste lid, van de Kaderwet genoemde instellingsmotieven. Op grond van artikel 3, eerste lid, aanhef en onderdeel a, van de Kaderwet zbo's, kan een zelfstandig bestuursorgaan worden ingesteld indien er behoefte is aan onafhankelijke oordeelsvorming op grond van specifieke deskundigheid. Zoals aangekondigd in de Kamerbrief van 20 november 2020, is daarvan in dit geval sprake.[12] Het ontoegankelijk maken van gegevens op internet, louter vanwege de inhoud daarvan, vormt naar zijn aard een beperking van de vrijheid van meningsuiting. De vrijheid van meningsuiting is in een democratische rechtsstaat cruciaal, en is onder meer neergelegd in artikel 7 van de Grondwet en artikel 10 van het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (hierna: EVRM). Het is vaste rechtspraak dat met (legitieme en noodzakelijke) beperkingen op dit grondrecht terughoudend moet worden omgegaan.[13]

Een bevoegdheid die de vrijheid van meningsuiting beperkt, moet met voldoende waarborgen zijn omgeven, zodanig dat een willekeurige inmenging wordt voorkomen.[14] Uit de rechtspraak van het Europees Hof voor de Rechten van de Mens (hierna: EHRM) volgt dat het in de regel de onafhankelijke rechter is die, waar noodzakelijk, bevoegd is om beperkende maatregelen te treffen ten aanzien van de vrijheid van meningsuiting.[15] Dat laat onverlet dat ook aan een ander orgaan, zoals een bestuursorgaan, de bevoegdheid kan worden geattribueerd om uitingen ontoegankelijk te maken. Uit de systematiek van de verordening en de keuzes die gemaakt zijn door de Europese wetgever volgt dat is gekozen voor een systeem waarbij een bevoegde instantie belast is met het uitvaardigen van onder meer verwijderingsbevelen naar aanleiding van geïdentificeerde terroristische inhoud en het opleggen van sancties, waarna er een doeltreffende voorziening in rechte is om onder meer een verwijderingsbevel te betwisten bij een rechterlijke instantie. Het ontbreken van rechterlijke toetsing vooraf moet dan worden gecompenseerd door andere waarborgen, zodanig dat onafhankelijke oordeelsvorming is geborgd.[16]

De Grondwet, het EVRM of de jurisprudentie noch de verordening verplichten tot instelling van een zbo. Echter, door de bevoegde autoriteit vorm te geven als een zelfstandig bestuursorgaan waarbij aanvullende waarborgen zijn gesteld, wordt onafhankelijke oordeelsvorming geborgd. Een zelfstandig bestuursorgaan is in zijn taakuitoefening immers niet hiërarchisch ondergeschikt aan enige politieke ambtsdrager.

De bevoegdheden die de Kaderwet zbo's toekent aan de Minister, waaronder de autoriteit ressorteert, zijn in onderhavig voorstel zodanig ingeperkt, dat de Minister uitsluitend kan ingrijpen ten aanzien van het

---

[11] Kamerstukken II 2014/15, 25 268, nr. 83.
[12] Kamerstukken II 2020/21, 31 015, nr. 208.
[13] Mede gelet op mogelijke «chilling effects». Daarmee wordt bedoeld dat individuen de vrijheid om zich uit te drukken niet of slechts verminderd ervaren, als gevolg van eerdere beperkingen daarop.
[14] Bijvoorbeeld HR 4 april 2017, ECLI:NL:HR:2017:584, r.o. 2.6.
[15] EHRM 10 september 2010, ECLI:CE:ECHR:2010:0914JUD003822403, r.o. 90–92.
[16] EHRM 7 juni 2007, ECLI:CE:ECHR:2007:0607JUD007136201, r.o. 45, en EHRM 30 september 2014, ECLI:CE:ECHR:2014:0930JUD000842905, r.o. 46.

financieel beheer en de administratieve organisatie. De Minister kan zich aldus niet mengen in de inhoudelijke uitoefening van de taak van de Autoriteit.

Daar staat tegenover dat de Minister namens de Staat der Nederlanden door de Europese Commissie aanspreekbaar is voor het nakomen van de verplichtingen op grond van de verordening. Het volledig uitsluiten van iedere mogelijkheid om bij een tekortkoming in de nakoming van de uitvoering van de verordening deze verantwoordelijkheid vorm te geven kan op gespannen voet komen te staan met deze verantwoordelijkheid. Vandaar dat de Minister enige bevoegdheden ten aanzien van het zelfstandig bestuursorgaan heeft, zoals het voordragen voor de benoeming van de bestuurders. Ook het parlement kan de Minister aanspreken. De Minister blijft immers stelselverantwoordelijk voor het publieke belang dat met het zbo wordt geborgd.

Er is geen bestaand bestuursorgaan dat is belast met het (doen) verwijderen of blokkeren van terroristische online-inhoud zodat het om die reden niet voor de hand ligt deze bijzondere taak bij een bestaand bestuursorgaan te beleggen. Daarom is gekozen voor instelling van een nieuw publiekrechtelijk zbo. Zoals in voormelde Kamerbrief van 20 november 2020[17] is aangekondigd, zal de Autoriteit tevens tot taak hebben om de ontoegankelijkmaking van online kinderpornografisch materiaal af te dwingen en onderzoek te doen naar, en informatie te verstrekken over de aanwezigheid van online kinderpornografisch materiaal teneinde de verspreiding daarvan te beperken.

Geen agentschap of deconcentratie

Er is niet gekozen om de bevoegde autoriteit vorm te geven als een agentschap. Een agentschap is een intern verzelfstandigd in de uitvoering werkzaam dienstonderdeel van een ministerie, met een eigen sturingsmodel en financiële administratie maar onder volledige ministeriële verantwoordelijkheid. Een agentschap is minder geschikt als organisatievorm voor de taken die de verordening toekent aan de bevoegde autoriteit. Waar op grond van de Kaderwet zbo's er een wettelijk regime is met waarborgen ten aanzien van de onafhankelijke oordeelsvorming, geldt voor een agentschap dat deze hiërarchisch ondergeschikt is aan een Minister, en zich daarom reeds moeilijk verhoudt tot de benodigde onafhankelijke oordeelsvorming.

Een alternatieve constructie die is overwogen betreft de constructie waarin de bevoegde autoriteit weliswaar wordt ondergebracht in een regulier dienstonderdeel van een departement, maar waarbij de bevoegdheid van de Minister om in individuele gevallen aanwijzingen of instructies te geven wordt beperkt. Daar is evenwel niet voor gekozen omdat het leidt tot de ongewenste situatie dat de Minister beperkt wordt in zijn mogelijkheid tot ingrijpen, maar toch volledig politiek verantwoordelijk blijft voor de wijze waarop de bevoegde autoriteit zijn taken vervult. Dit naast het feit dat juist het regime zoals opgenomen in de Kaderwet zbo's al is ingericht om waarborgen voor de onafhankelijkheid te creëren.

3.3 Taken en positionering

De Autoriteit krijgt middels artikel 2 van onderhavig voorstel de taken en bevoegdheden die noodzakelijk zijn om de verordening uit te kunnen voeren.
Deze taak omvat:

[17] Kamerstukken II 2020/21, 31 015, nr. 208.

a. Het uitvoeren van de in artikel 1 van de verordening bedoelde maatregelen ten einde terroristische inhoud te identificeren en de snelle verwijdering ervan door aanbieders van hostingdiensten te garanderen en samen te werken met de bevoegde autoriteiten van de lidstaten, aanbieders van hostingdiensten en, waar passend, Europol;
b. Het uitvoeren van de taken en bevoegdheden die de verordening in artikel 12, eerste lid, aan de door de lidstaat aangewezen bevoegde instantie toekent.

Ten aanzien van de maatregelen die de lidstaten onder a moeten nemen geldt dat de Autoriteit de taak krijgt terroristische inhoud te identificeren, maar ook om samen te werken. De Autoriteit is niet alleen degene die maatregelen oplegt teneinde terroristische inhoud te verwijderen, maar ook een samenwerkingspartner en bemiddelaar tussen ogenschijnlijk tegengestelde belangen: een schoon internet en een open internet. Een schoon internet door het beschermen van burgers tegen terroristische inhoud rekening houdend met opsporings- en inlichtingenbelangen. Een open internet door het waarborgen van fundamentele rechten, zoals de vrijheid van meningsuiting. De Autoriteit hanteert een hybride aanpak: zij werkt via (horizontale) relaties samen met aanbieders van hosting-diensten. Waar dat (nog) niet voldoende effect sorteert, vervult zij een (verticale) toezichthoudersrol en zal zo nodig maatregelen nemen.

De Autoriteit is een aanvulling op de bestaande op vrijwilligheid gebaseerde samenwerking met de internetsector en een aanvulling op de strafrechtelijke opsporing en vervolging. De Autoriteit verricht haar taken en bevoegdheden in samenwerking met relevante ketenpartners.
Wat betreft het uitoefenen van de (horizontale) relatie met de sector is het van belang dat de Autoriteit op de hoogte is van de meeste recente ontwikkelingen en inzichten en weet wat er in de praktijk speelt, zodat ze een gerespecteerd gesprekspartner is voor andere partijen. Doel is om internetpartijen bij te staan bij het treffen van preventieve maatregelen om verspreiding van terroristische online-inhoud tegen te gaan (zorgplicht). De Autoriteit stimuleert de samenwerking tussen deze marktpartijen en bevordert dat zij, en hun belangenorganisaties, zoveel mogelijk zelf initiatieven ontplooien om instrumenten te ontwikkelen om terroristische online-inhoud te voorkomen en tegen te gaan. Deze partijen zijn daartoe bij uitstek in staat, omdat de technische ontwikkeling van ICT en internet wortelen in het marktdomein. De Autoriteit kan in dit licht bijvoorbeeld een procedure inrichten voor het kunnen ontvangen en opvolgen van meldingen van (vermoedelijk) terroristisch online-inhoud door derden.
Wat betreft de (verticale) toezichthoudersrol is het van belang dat de Autoriteit kordaat optreedt als de aanbieders van hostingdiensten niet of onvoldoende invulling geven aan hun zorgplicht om terroristische inhoud te verwijderen. Dat vergt een slagvaardige en onafhankelijke organisatie die om zo goed mogelijk invulling te geven aan deze taak, ook zelf onderzoek doet naar de aanwezigheid van terroristische online-inhoud. Waar mogelijk zal de Autoriteit dit in samenwerking met private en publieke partijen doen. Hier zal in paragraaf 3.4 nader op worden ingegaan. Ook kan de Autoriteit na een zelfstandige beoordeling een verwijderingsbevel uitvaardigen op aangeven van een bevoegde autoriteit van een andere EU-lidstaat. De Autoriteit ziet er op toe dat een bevel wordt opgevolgd en treedt zo nodig op door het opleggen van een bestuursrechtelijke sanctie.

Om een gedegen afweging te kunnen maken tussen enerzijds het belang van de vrijheid van meningsuiting en anderzijds het belang van het tegengaan van de verspreiding van terroristische online-inhoud gaat de autoriteit zelfstandig kennis opbouwen over welk materiaal als terroris-

tisch is te beschouwen. Daaronder valt ook kennis van de context waarin deze uitingen worden geplaatst, aangezien de verordening bepaalt dat materiaal dat voor educatieve, journalistieke, artistieke of onderzoeksdoeleinden of met het oog op het voorkomen of bestrijden van terrorisme onder het publiek wordt verspreid, met inbegrip van materiaal dat een uiting vormt van polemische of controversiële standpunten in het publieke debat, niet mag worden beschouwd als terroristische inhoud. Mede in het kader van het opleggen van specifieke maatregelen en bestuursrechtelijke sancties zal worden geïnvesteerd in kennis over de sector van aanbieders van hostingdiensten, zodat zo goed mogelijk kan worden beoordeeld of het opleggen van maatregelen en bestuursrechtelijke sancties proportioneel is en aan de juiste partij is gericht.

Met het oog op de effectieve uitvoering van deze verordening en de voorkoming van dubbel werk zal de Autoriteit waar mogelijk aansluiten op de instrumenten die worden ontwikkeld door Europol.

De Autoriteit kenmerkt zich door onafhankelijkheid en transparantie. Ze kan haar werk alleen goed doen als ze in haar oordeels- en besluitvorming over terroristische online-inhoud onafhankelijk en transparant is. Zowel de direct betrokkenen (zoals de aanbieders van hostingdiensten) als het brede publiek moeten kunnen nagaan waarom en op welke gronden besluiten worden genomen – en moeten daar ook tegenin kunnen gaan, waarbij er tegen besluiten rechtsbescherming open staat.

Ten aanzien van de vereiste onafhankelijkheid in de oordeels- en besluitvorming is in onderhavig voorstel in artikel 5 maatwerk opgenomen. Artikel 21 en 22 van de Kaderwet zijn niet van toepassing. Daardoor is de Minister niet bevoegd om beleidsregels te stellen ten aanzien van de Autoriteit en is de Autoriteit slechts verplicht inlichtingen te verstrekken of inzage te geven in zakelijke gegevens en bescheiden te verstrekken aan de Minister van Justitie en Veiligheid met betrekking tot het gevoerde financiële beheer en de administratieve organisatie. Artikel 23 van de Kaderwet vindt slechts toepassing ten aanzien van het door de Autoriteit gevoerde financiële beheer en de administratieve organisatie. Zoals eerder opgemerkt is de Minister verantwoordelijk voor een tekortkoming in de nakoming van de verordening en is hij daar door de Commissie op aanspreekbaar. Het voorstel bevat daarom enkele onderdelen die vereist zijn om de verplichtingen op grond van de verordening te kunnen nakomen. Dat betreft in ieder geval de verplichting om de in artikel 21, eerste lid, van de verordening bedoelde gegevens te verstrekken die ieder jaar uiterlijk op 31 maart aan de Commissie moeten worden verstrekt. Daarnaast stelt de verordening zoals in paragraaf 2.2 beschreven eisen aan het elektronische berichtenverkeer, waaronder bijvoorbeeld eisen aan de authenticatie. Omdat daarnaast is voorzien in de mogelijkheid van het vaststellen van gedelegeerde handelingen door de Commissie kan het noodzakelijk zijn nadere regels te stellen om aan de verordening te kunnen voldoen.

3.4. Toezicht, bevoegdheden en handhaving

Artikel 13, eerste lid, van de verordening bepaalt onder meer dat de lidstaten ervoor zorgen dat de bevoegde autoriteiten over de benodigde bevoegdheden beschikken om de doelstellingen uit hoofde van de verordening te verwezenlijken en hun verplichtingen uit hoofde van de verordening na te komen. In artikel 1 van de verordening zijn de doelstellingen die worden nagestreefd opgenomen, waarbij tevens is opgenomen dat lidstaten de maatregelen moeten nemen om terroristische inhoud te identificeren teneinde de snelle verwijdering ervan door aanbieders van hostingdiensten te garanderen.

Onderhavig voorstel kent de Autoriteit de taken en bevoegdheden toe zoals de verordening die toekent aan de bevoegde instantie. Daarnaast zijn de maatregelen die de lidstaten moeten nemen met het oog op de doelstellingen van de verordening zoals opgenomen in artikel 1, tweede lid, onderdeel b, van de verordening toegekend als taak aan de Autoriteit. Tevens is opgenomen dat de Autoriteit de ambtenaren aanwijst die belast zijn met het toezicht op de naleving. Hieruit volgt dat de betreffende ambtenaren de bevoegdheden bezitten die de Algemene wet bestuursrecht toekent aan personen die bij of krachtens wettelijk voorschrift belast zijn met het houden van toezicht op de naleving van het bepaalde bij of krachtens enig wettelijk voorschrift. Uit de taak die op grond van artikel 2, derde lid, onderdeel a, bij de Autoriteit wordt belegd volgt dat ten teneinde terroristische inhoud online te kunnen identificeren de Autoriteit online onderzoek verricht naar de verspreiding van deze inhoud onder het publiek. Gelet op het toepassingsbereik van de verordening dat zich richt op het «onder het publiek verspreiden», gaat het daarbij alleen om het openbare internet, zoals ook in paragraaf 2.2 beschreven. Wanneer voor de toegang tot informatie registratie of toelating tot een groep gebruikers vereist is, valt zij alleen onder het bereik van de Autoriteit wanneer gebruikers die toegang tot de informatie wensen, automatisch worden geregistreerd of toegelaten zonder menselijke beslissing of selectie van wie toegang krijgt.[19] Alleen dan kan namelijk worden gesproken van het «openbare internet». Dit voorstel biedt derhalve geen grondslag voor het kennisnemen van bronnen waarbij een aanvullende handeling, die in feite niet volledig geautomatiseerd is, is vereist en waarvoor een «deurbeleid» bestaat in de vorm van een beoordeling van de accounthouder (in enige mate doorbreken van een beveiliging). Voor de volledigheid wordt er op gewezen dat de Autoriteit krachtens dit wetsvoorstel niet wordt toegerust met opsporingsbevoegdheden, omdat dat niet past bij de taak die de verordening aan de Autoriteit toekent. De taak van de Autoriteit is immers het zo snel mogelijk offline laten halen dan wel ontoegankelijk doen maken van terroristische online-inhoud en niet het opsporen van de plaatsers of producenten van dit materiaal.

In het kader van het onderzoek van de Autoriteit kunnen tevens persoonsgegevens worden verwerkt. Omdat daarbij mogelijk (bijzondere) persoonsgegevens worden verwerkt is in artikel 9 van onderhavig voorstel voorzien in een grondslag voor het verwerken van bijzondere persoonsgegevens. Hierop wordt nader ingegaan in paragraaf 5 van deze memorie van toelichting.

Artikel 18 van de verordening bepaalt dat de lidstaat de overtreding van de aldaar opgenomen voorschriften dient te voorzien van sancties, waarbij met het opleggen van de sanctie rekening moet worden houden met de in het tweede lid opgenomen omstandigheden. In artikel 12, tweede lid van het voorstel zijn de maximale boetehoogtes opgenomen voor overtreding van bepalingen van de verordening. De verordening biedt in het tweede lid van artikel 18 expliciet ruimte voor nationaal maatwerk bij de keuze of en zo ja, welke sanctie wordt opgelegd. Dit is van bijzonder van belang voor het MKB. Voor het MKB zal het een zwaardere belasting zal zijn om te voldoen aan alle verplichtingen die voor deze sector uit de verordening voortvloeien. Artikel 18 biedt een expliciete grondslag om daar rekening mee te houden bij de vraag of een sanctie wordt opgelegd. Factoren die worden betrokken zijn onder meer: de aard en omvang van de overtreding, de mate van verwijtbaarheid, het bestaan van eerdere overtredingen, de financiële draagkracht en de mate van medewerking. In aanvulling hierop wordt expliciet aandacht besteed aan de aard en grootte van de betrokken aanbieders van hostingdiensten,

[19] Zie overweging 14 bij de verordening.

in het bijzonder als het gaat om micro- en kleine ondernemingen zoals bedoeld in de Aanbeveling van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen.[20] De opgelegde boete zal proportioneel moeten zijn in het licht van de geconstateerde overtreding. Het is hierbij allereerst aan de toezichthouder om de hoogte van de boete te motiveren.

3.5 Rechtsbescherming

Artikel 9 van de verordening bepaalt dat aanbieders van hostingdiensten en aanbieders van inhoud recht hebben op een doeltreffende voorziening in rechte. Aanbieders van hostingdiensten hebben het recht om:

- Een op grond van artikel 3, eerste lid, uitgevaardigd verwijderingsbevel te betwisten bij de rechterlijke instantie van de lidstaat van de bevoegde autoriteit die het verwijderingsbevel heeft uitgevaardigd;
- Een besluit op grond van artikel 4, vierde lid (verzoek tot toetsing van grensoverschrijdende verwijderingsbevel), artikel 5, vierde lid (blootstellingsbesluit), zesde lid (besluit specifieke maatregelen voldoen niet), zevende lid (verzoek tot herziening) te betwisten bij de rechterlijke instantie van de lidstaat van de bevoegde autoriteit die het besluit heeft genomen.

Aanbieders van inhoud wiens materiaal na een verwijderingsbevel verwijderd is of waartoe de toegang na een verwijderingsbevel geblokkeerd is, hebben recht:

- een op grond van artikel 3, lid 1, uitgevaardigd verwijderingsbevel te betwisten bij de rechterlijke instanties van de lidstaat van de bevoegde autoriteit die het verwijderingsbevel heeft uitgevaardigd en;
- het recht om een besluit op grond van artikel 4, lid 4 (verzoek tot toetsing), te betwisten bij de rechterlijke instanties van de lidstaat van de bevoegde autoriteit die het besluit heeft genomen.

Artikel 3, negende lid, van de verordening bepaalt in dit kader dat een verwijderingsbevel definitief is bij het verstrijken van de termijn voor het instellen van een hoger beroep indien geen hoger beroep is ingesteld overeenkomstig het nationaal recht, of wanneer het na een hoger beroep is bevestigd. Daarnaast regelt dit lid dat wanneer het verwijderingsbevel definitief wordt, de bevoegde autoriteit die het verwijderingsbevel heeft uitgevaardigd, de bevoegde autoriteit van de lidstaat waar de aanbieder van hostingdiensten zijn hoofdvestiging of waar zijn wettelijke vertegenwoordiger zijn verblijf- of vestigingsplaats heeft, daarvan in kennis stelt.

De bovengenoemde besluiten zijn onderworpen aan de gebruikelijke bestuurlijke rechtsbescherming, zoals geregeld in de Algemene wet bestuursrecht (hierna: Awb). Dit betekent allereerst dat er bezwaar openstaat, gevolgd door beroep bij de bestuursrechter, en ten slotte hoger beroep bij de Afdeling bestuursrechtspraak van de Raad van State.

3.6. Verhouding tot het strafrecht

In artikel 54a van het Wetboek van Strafrecht (hierna: Sr) is opgenomen dat bij het gehoor geven aan een dergelijk bevel, de tussenpersoon die een communicatiedienst verleent bestaande in de doorgifte of opslag van gegevens die van een ander afkomstig zijn, bij een strafbaar feit dat is begaan met gebruikmaking van die dienst als zodanig niet wordt vervolgd. Met artikel 13 van onderhavig voorstel wordt in artikel 54a Sr

[20] Aanbeveling van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen (kennisgeving geschied onder nummer C(2003) 1422), 2003/361/EG.

het verwijderingsbevel dat kan worden uitgevaardigd uit hoofde van de verordening toegevoegd. Op deze wijze geldt dan ook voor de situatie dat de aanbieder van een hostingdienst die gehoor geeft aan een verwijderingsbevel niet wordt vervolgd voor een strafbaar feit dat is begaan met gebruikmaking van diens hostingdienst door middel van de inhoud die op grond van het verwijderingsbevel is verwijderd.

Artikel 8 van het voorstel bevat daarnaast een verplichting voor de autoriteit om over de uitoefening van zijn taken en bevoegdheden te overleggen met de politie, het Openbaar Ministerie en de AIVD en MIVD. Dit is van belang om te voorkomen dat de taakuitoefening van de Autoriteit het voorkomen, onderzoeken, opsporen en vervolgen van terroristische misdrijven op enige manier belemmert. Tevens is een bevoegdheid opgenomen voor de Autoriteit om gegevens of inlichtingen te delen verkregen bij de uitvoering van zijn taken deze aan de politie en inlichtingendiensten MIVD en AIVD te verstrekken voor zover deze dienstig kunnen zijn bij de uitoefening van diens taken.

3.7 Verhouding tot hoger recht

De verordening en de maatregelen die daaruit voortvloeien kunnen raken aan in het EVRM, het Handvest van de Grondrechten en de Grondwet vastgelegde rechten en vrijheden. De gevolgen die onderhavig voorstel met zich meebrengt vloeien voort uit de verordening waarbij de afwegingen ten aanzien van deze vrijheden door de Europese wetgever zijn gemaakt. Gelet op het belang van deze vrijheden wordt in deze paragraaf echter op met name de gevolgen voor de vrijheid van meningsuiting ingegaan. In de verordening is op diverse plekken het belang van waarborgen voor de vrijheid van meningsuiting, inclusief de vrijheid om inlichtingen of denkbeelden te ontvangen en door te geven in een open en democratische samenleving, zoals ook vastgelegd in het Handvest van de grondrechten onderkent en benadrukt.

In het EVRM is de vrijheid van meningsuiting vastgelegd in artikel 10 waarbij het tweede lid bepaalt dat deze vrijheid kan worden beperkt indien dit bij wet is voorzien en noodzakelijk is in een democratische samenleving, in het belang van de nationale veiligheid, territoriale integriteit of openbare veiligheid, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden, de bescherming van de goede naam of de rechten van anderen, om de verspreiding van vertrouwelijke mededelingen te voorkomen of om het gezag en de onpartijdigheid van de rechterlijke macht te waarborgen. De Grondwet bevat in artikel 7 het recht dat niemand voorafgaand verlof nodig heeft om door de drukpers gedachten of gevoelens te openbaren, behoudens ieders verantwoordelijkheid volgens de wet.
De verordening voldoet aan de bovengenoemde criteria die worden gesteld aan een inperking van de vrijheid van meningsuiting. Zo volgt uit artikel 7 van de Grondwet dat niemand voorafgaand verlof nodig heeft om gedachten of gevoelens te openbaren, behoudens ieders verantwoordelijkheid volgend de wet. Naast het feit dat een verordening rechtstreekse werking heeft en in die zin voldoet aan het criterium van een wettelijk voorschrift, geldt dat onderhavig voorstel ter uitvoering van de verordening verwijst naar de bepalingen van de verordening die zien op de inperking van de vrijheid van meningsuiting. Daarbij is er geen sprake van voorafgaand verlof noch kan sprake zijn van een verplichting voor aanbieders van hostingdiensten tot enige vorm van filtering vooraf. Een verwijderingsbevel wordt uitgevaardigd naar aanleiding van reeds openbaar gemaakte terroristische inhoud, waarop vervolgens rechterlijke toetsing mogelijk is.

Daarnaast is in de nationale uitvoering van de verordening in onderhavig voorstel expliciet gekozen voor het belasten van een nieuw in te richten zbo met de taken die ingevolge de verordening aan de bevoegde instantie toekomen als waarborg voor de onafhankelijke taakuitoefening. In aanvulling daarop zijn zoals in paragraaf 3.4 beschreven daarnaast een aantal bepalingen van de Kaderwet zbo's buiten toepassing verklaard waardoor de Minister alleen de mogelijkheid heeft om in te grijpen in het financieel beheer en de administratieve organisatie. Het is aan het zbo om daarnaast invulling te geven aan de passende bescherming van grondrechten bijvoorbeeld in kader van een verzoek tot beoordeling van een grensoverschrijdend verwijderingsbevel. Ook voor de aanbieders van hostingdiensten geldt dat zij bij het nemen van specifieke maatregelen dit op zorgvuldige, evenredige en niet-discriminerende wijze, doen met inachtneming onder alle omstandigheden van de grondrechten van de gebruikers, en met name rekening houdend met het fundamentele belang van de vrijheid van meningsuiting en van informatie in een open en democratische samenleving, teneinde te voorkomen dat materiaal dat geen terroristische inhoud bevat, wordt verwijderd. In dit kader zal met name de voorlichtende rol van het zbo relevant zijn zodat zij aanbieders van hostingsdiensten kunnen ondersteunen bij de beoordeling van terroristische online-inhoud.

Op de verhouding van het voorstel tot de bescherming van de persoonlijke levenssfeer wordt in paragraaf 5.2 nader ingegaan.

4. Financiële gevolgen

4.1 Financiële gevolgen voor het Rijk

De financiële gevolgen die voortvloeien uit de verordening en het onderhavige voorstel zijn voor het Rijk, specifiek voor het Ministerie van Justitie en Veiligheid. De lasten van de regeling zitten in het aanwijzen en inrichten van een bevoegde autoriteit die aan de opgenomen voorwaarden voldoet en de taken en bevoegdheden op grond van de verordening gaat uitvoeren.

De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) heeft namens de Minister van Justitie en Veiligheid de beschikbare financieringsbronnen voor (structurele) bekostiging van de bevoegde autoriteit in kaart gebracht. Het gaat hier om de volgende bronnen:

1. Structurele middelen die vrijvallen door de overdracht van taken van de Internet Referral Unit van de Nationale Politie aan de bevoegde autoriteit (IRU-middelen) van jaarlijks € 0,4 mln.
2. Begrotingsmiddelen JenV: reeds beschikbaar gestelde middelen van € 1,2 mln. in 2022, oplopend naar structureel € 3,2 mln. in 2025.
3. Het Europese Fonds voor Interne Veiligheid (ISF) heeft € 8,2 mln. toegekend aan de NCTV voor interne projecten, waarvan € 3,0 mln. is gemarkeerd voor de oprichting van de bevoegde autoriteit.

Een incidenteel bedrag van € 2.121.620,– vanuit de Nationale Politie (NP) wegens onderbesteding IRU-middelen over 2018, 2019 en 2020 zal worden ingezet voor de oprichting en inrichting van de bevoegde autoriteit.

4.2. Financiële gevolgen voor de sector

De financiële gevolgen voor de maatschappelijke sectoren, in het bijzonder de bedrijvensector van hosting service providers, zijn voorafgaand aan het wetgevingstraject uitgewerkt in het Impact Assessment van de Europese Commissie.

Kosten en benodigde middelen (tools) zijn afhankelijk van verschillende factoren, bijvoorbeeld grootte van de betreffende hosting service providers. Bijna 10.000 hostingserviceproviders in Europa zijn kleine, middelgrote of micro-ondernemingen, waarvan ongeveer de helft micro-ondernemingen. Aangezien grotere platforms steeds vijandiger staan tegenover terroristische online-inhoud, wordt illegale inhoud in toenemende mate verspreid via een diverse reeks kleinere platforms. Vergeleken met ongeveer 30% in 2017, werd bijna 70% van de doorverwijzingen van Europol in 2018 verzonden naar aanbieders van hostingdiensten die als kleine of micro-ondernemingen kunnen worden beschouwd.

Sommige verplichtingen uit de verordening brengen een last voor ondernemingen met zich mee, met name voor kleine en micro-ondernemingen, maar deze worden verzacht door ervoor te zorgen dat de maatregelen evenredig zijn en door het aantal bedrijven te verminderen dat ze moet toepassen op degenen die eraan blootgesteld zijn naar terroristische inhoud.

De belangrijkste kosten voor bedrijven worden geschat in fte en nader toegelicht in bijlage 4 van het Impact Assessment van de Europese Commissie. Enkel de hosting service providers die worden geconfronteerd met terroristische content dienen proactieve maatregelen te nemen. Geschat wordt dat het structurele inzet vergt van 1,0 – 11,5 fte plus de kosten voor het installeren van proactieve maatregelen. De werkelijke kosten zijn afhankelijk van risico, middelen, grootte en kwetsbaarheid van bedrijven. Daarnaast zullen er beperkte terugkerende kosten zijn.

De belangrijkste kosten houden verband met de toepassing van de deadline van 1 uur voor verwijderingsbevelen. Andere kostenposten hebben betrekking op het implementeren van contentmoderatie- of filtertechnologieën voor bedrijven die worden blootgesteld aan terroristische inhoud, evenals kosten in verband met de risicobeoordeling, actieplan voor corrigerende maatregelen, en het verstrekken van feedback over genomen maatregelen en transparantie- en rapportagevereisten. Aangezien deze verplichtingen betrekking hebben op verschillende functies en expertise, zullen ze over het algemeen toegewijd personeel of middelen vereisen. Aangenomen wordt dat een deel van de kosten wordt geabsorbeerd door moderatiefuncties die al bestaan voor andere soorten inhoud.

Er zijn geen financiële gevolgen voor decentrale overheden.

5. Overige gevolgen

5.1. Regeldruk en gevolgen voor bedrijven

Ten aanzien van het wetsvoorstel zelf geldt dat er geen gevolgen zijn voor de regeldruk. Gevolgen voor bedrijven vloeien volledig voort uit de verordening zelf. Onderhavig voorstel bevat geen aanvullende regels waaruit regeldruk voortvloeit. De Europese Commissie heeft bij de totstandkoming van het voorstel een impact assessment uitgevoerd waarin de gevolgen zijn beschreven en ook rekenschap is gegeven van de gehouden consultatie van het voorontwerp van de verordening.[21]

[21] Impact assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online van 12 december 2018, SWD(2018) 408 final

Uit het impact-assessment blijkt dat eenduidigere regels door de verordening ervoor zorgen dat fragmentatie van de markt wordt tegengegaan en juridische zekerheid en vertrouwen wordt vergroot. Op deze wijze worden de diensten van de aanbieders van hostingdiensten beschermd tegen misbruik voor terroristische doeleinden.

Bij het tegengaan van de verspreiding van terroristische online-inhoud is er voor de komst van deze verordening vooral sprake geweest van vrijwillige samenwerking tussen de aanbieders van hostingdienstenaanbieders van hostingdiensten en de Nederlandse en Europese autoriteiten. Deze verordening zorgt voor een meer verplichtend karakter en heeft om deze reden impact op de gehele sector, waarbij er onderscheid is tussen grote aanbieders van hostingdiensten als Facebook, Twitter en YouTube en kleinere aanbieders van hostingdiensten.

Er wordt in de verordening rekening gehouden met de proportionaliteit van verplichtende maatregelen ten aanzien van de grootte van de aanbieders van hostingdiensten. Ook gelden verplichtende maatregelen als verwijderingsbevelen en het nemen van specifieke maatregelen alleen voor aanbieders van hostingdiensten die worden geconfronteerd met terroristische content op hun platformen. In de impact assessment van de Europese Commissie wordt geschat dat 1,5% tot 4% van de kleine aanbieders van hostingdiensten met de verplichtingen van deze verordening te maken krijgen.

De grootste impact heeft het verwijderingsbevel waarvan online-inhoud binnen 1 uur moet worden verwijderd van het platform van de desbetreffende aanbieder van hostingdiensten. Dit betekent dat iedere aanbieder van hostingdiensten hiertoe de gelegenheid moeten creëren om aan deze verplichting te voldoen. Wel krijgen aanbieders van hostingdiensten informatie 12 uur van te voren over de toepasselijke procedures en termijnen van de bevoegde autoriteit indien de aanbieder nog niet eerder een verwijderingsbevel heeft ontvangen, tenzij sprake is van terdege gemotiveerde noodgevallen. Ook dienen aanvullende specifieke maatregelen te worden genomen door aanbieders van hostingdiensten om de verspreiding van terroristische online-inhoud via hun dienst te voorkomen, bijvoorbeeld door mechanismes voor gebruikersmoderatoren of mechanismes voor gebruikers om melding te kunnen maken.

Alhoewel de gevolgen voor de praktijk voortvloeien uit de verordening en niet uit onderhavig voorstel is er vanwege het belang voor betrokkenen voorzien in een MKB-toets, in de vorm van een ronde tafel bijeenkomt waarbij zes aanbieders van hostingsdiensten aanwezig waren.

Tijdens de MKB-toets werd een aantal aandachtspunten naar voren gebracht rond de procedures die te maken hebben met het opvolging geven aan een verwijderingsbevel. Het betreft hier met name de inschatting dat het verwijderingsbevel bij een bepaald type aangeboden diensten (zoals *unmanaged hosting*) moeilijk opvolgbaar kan zijn. Dit omdat de aanbieder van dit type diensten geen toegang heeft tot de servers waarop de betreffende inhoud door weer andere dienstverleners, die deze servers of delen daarvan onderhouden, wordt gehost. De verordening voorziet erin, dat aanbieders van hostingdiensten de autoriteit in kennis kunnen stellen wanneer zij door overmacht of feitelijke onmogelijkheden een verwijderingsbevel niet (tijdig) kunnen opvolgen. Dit dient wel vergezeld te gaan van een objectieve motivering met technische of operationele redenen en alleen voor situaties waarin het niet aan de aanbieder van hostingdiensten kan worden toegerekend. Voorbeeld van overmacht is als een aanbieder van hostingdiensten door

een stroomstoring (of andere calamiteit zoals brand) geen toegang heeft tot zijn servers.

Verder werd tijdens de MKB-toets naar voren gebracht dat een bepaalde categorie aanbieders van hostingdiensten terroristisch materiaal weliswaar kan verwijderen of ontoegankelijk kan maken, maar dat zij dit materiaal moeilijk zes maanden kunnen opslaan, zoals de verordening vereist met het oog op beschikbaarheid voor eventuele beroeps- en bezwaarprocedures. Daarnaast is het volgens deze aanbieders van hostingdiensten ook niet mogelijk om het verwijderde materiaal terug te zetten. Nu deze verplichtingen voortvloeien uit de verordening, hebben aanbieders van hostingdiensten de verantwoordelijkheid hieraan te voldoen. Het Ministerie van Justitie en Veiligheid zal vertegenwoordigers van de sector structureel betrekken bij de implementatie, teneinde gezamenlijk te komen tot een werkbare uitvoering van deze bepaling uit de verordening.

Dit geldt ook voor de bepalingen die betrekking hebben op de 24/7 bereikbaarheid van aanbieders van hostingdiensten en de verwijderingstermijn van één uur. Ook hieraan dienen aanbieders van hostingdiensten te voldoen, maar deze bepalingen kunnen vooral voor kleine aanbieders van hostingdiensten problematisch zijn. In de verordening is om deze reden bepaald dat de aanbieder van hostingdiensten vrij moet zijn om gebruik te maken van een bestaand contactpunt, op voorwaarde dat het contactpunt de in deze verordening vastgestelde functies kan uitoefenen.

Ook wordt er daarnaast naar gestreefd om in gezamenlijkheid tot werkbare oplossingen te komen. De Minister van Justitie en Veiligheid zal gedurende het implementatietraject bij de Europese Commissie en andere EU-lidstaten aandringen op uniformiteit bij de EU-brede implementatie en interpretatie van de verordening om de sector zoveel mogelijk helderheid te verschaffen. Ook zal hij inzetten op heldere en tijdige communicatie over de maatregelen waaraan aanbieders van hostingdiensten in Nederland op grond van de verordening dienen te voldoen.

5.2 Gevolgen voor de persoonlijke levenssfeer en verhouding tot de AVG

In het kader van de voorbereiding van de uitvoering van de verordening en de totstandkoming van het wetsvoorstel is een privacy impact assessment verricht waarmee rekening is gehouden bij de uitwerking van het voorstel.

Vanwege de verplichtingen op grond van de verordening krijgt de Autoriteit onder meer tot taak om terroristische online-inhoud te identificeren. Het identificeren van terroristische online-inhoud die onder het publiek wordt verspreid, vergt dat de Autoriteit onderzoek uitvoert op het publieke internet ten behoeve van het detecteren van deze inhoud. Daarbij zal gebruik gemaakt worden van geautomatiseerde monitoringsinstrumenten. Tijdens het bekijken en beoordelen van materiaal worden ook (bijzondere) persoonsgegevens verwerkt.

Deze taken op grond waarvan de verwerkingen plaatsvinden staan in artikel 2 van onderhavig voorstel, in samenhang met de artikelen van de verordening waarin de taakomschrijving is opgenomen.

De resultaten van het zelf detecteren en het gebruik maken van geautomatiseerde monitoringsinstrumenten kunnen aanleiding geven voor het opstellen van een verwijderingsbevel. Indien vermoedelijk terroristische online-inhoud wordt aangetroffen door de inzet van geautomatiseerde instrumenten wordt deze vervolgens altijd door middel van een mense-

lijke toets binnen de Autoriteit geverifieerd. Daarbij wordt beoordeeld of deze content gekwalificeerd kan worden als terroristische online-inhoud in de zin van de verordening. Ingeval van een verwijderingsbevel kan het ook gaan om de verwerking van bijzondere persoonsgegevens. Door een verwijderingsbevel wordt de vrijheid van meningsuiting beperkt van de persoon in kwestie. Dus de impact voor de betrokkenen kan groot zijn, maar proportioneel in het licht van het belang voor de nationale veiligheid.

Op grond van de Algemene verordening gegevensbescherming (AVG) geldt dat de verwerking alleen rechtmatig is indien aan tenminste een van de voorwaarden van artikel 6, eerste lid, AVG, is voldaan. De verwerking door de Autoriteit is noodzakelijk in verband met de in onderdeel c opgenomen grond dat de verwerking noodzakelijk is om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust en onderdeel e omdat deze noodzakelijk is voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen.

Ten aanzien van de verwerking van bijzondere persoonsgegevens geldt dat dit noodzakelijk is gelet op de in artikel 9, tweede lid, onderdeel g, van de AVG genoemde redenen van zwaarwegend algemeen belang, op grond van Unierecht of lidstatelijk recht, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene. In dit geval volgen de redenen uit het Unierecht, namelijk de verordening. Hetzelfde geldt voor de verwerking van strafrechtelijke gegevens als bedoeld in artikel 10 van de AVG. Dit volgt eveneens uit de verplichtingen die de verordening aan de lidstaten oplegt. Vanwege de bepalingen van de Uitvoeringswet AVG (UAVG) is in artikel 9 van onderhavig voorstel de grondslag voor deze verwerkingen nader vastgelegd.

De betrokkene kan tegen een verwijderingsbevel bezwaar maken. Voor de afhandeling van het bezwaar is het noodzakelijk dat de autoriteit beschikt over het verwijderingsbevel inclusief de onderliggende stukken/het verwijderde materiaal. Niet alleen voor de afhandeling van het bezwaar, maar ook voor het onderliggende bewijs met betrekking tot het blootstellingsbesluit is het noodzakelijk dat de Autoriteit beschikt over de verwijderde content.

De betrokkene (of zijn wettelijk vertegenwoordiger), kan op grond van de AVG bij de Autoriteit een verzoek indienen waarbij hij een beroep doet op een van zijn rechten als betrokkene. Het kan in voorkomend geval noodzakelijk zijn bepaalde rechten van betrokkenen in te perken indien dit noodzakelijk is op grond van de nationale veiligheid, de openbare veiligheid, de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid, of de bescherming van de betrokkene of van de rechten en vrijheden van anderen. Daarmee wordt aangesloten bij artikel 23, eerste lid, onderdelen a, c, d en i van de AVG die voorziet in de mogelijkheid om bij Unierechtelijke of lidstaatrechtelijke wetgevingsmaatregel die op de verwerkingsverantwoordelijke of de verwerker van toepassing is bepaalde rechten van betrokkene te beperken, op voorwaarde dat die beperking de wezenlijke inhoud van de grondrechten en fundamentele vrijheden onverlet laat en in een democratische samenleving een noodzakelijke en

evenredige maatregel is ter waarborging van een van de aldaar genoemde belangen.

In artikel 41 UAVG is eveneens een bepaling opgenomen die de mogelijkheid biedt om rechten van betrokkenen onder de aldaar genoemde voorwaarden in te perken. Artikel 10, tweede lid van onderhavig voorstel bevat een nadere concretisering van deze mogelijkheid, waarbij de voorwaarde is opgenomen dat bij gebruikmaking van deze bevoegdheid moet worden voorzien in een dragende onderbouwing, die schriftelijk wordt medegedeeld aan de betrokkene wiens rechten worden beperkt. Indien dit echter afbreuk doet aan het doel van de beperking kan de mededeling aan de betrokkene achterwege worden gelaten. In dat geval dient alsnog mededeling aan betrokkene te worden gedaan zodra de reden voor het achterwege blijven is vervallen. Het informeren van betrokkene doet dan immers geen afbreuk meer aan het doel van de beperking. Het voorgaande laat overigens de rechtsbescherming die openstaat op grond van de verordening en de verplichtingen op grond van artikel 11 van de verordening onverlet.

Op grond van artikel 6, eerste lid, van de verordening zijn aanbieders van hostingdiensten verplicht om verwijderde of geblokkeerde inhoud te bewaren, omdat de inhoud teruggeplaatst moet kunnen worden bijvoorbeeld naar aanleiding van een gerechtelijke procedure. Daarnaast kan dit noodzakelijk zijn met het oog op het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven. De aanbieder van hostingsdiensten dient deze gegevens in ieder geval zes maanden of op verzoek van de bevoegde autoriteit of rechterlijke instantie of gedurende een nader bepaalde periode te bewaren indien en zolang zulks nodig is voor lopende administratieve of gerechtelijke toetsingsprocedures. Het is mogelijk om die termijn op verzoek van de bevoegde autoriteit of rechterlijke instantie te verlengen indien en zo lang dit nodig is voor lopende administratieve of gerechtelijke toetsingsprocedures.

Voor zowel de verwerking van bijzondere persoonsgegevens als van strafrechtelijke gegevens geldt dat indien verwerking op grond van de AVG is toegestaan, passende en specifieke maatregelen moeten worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene. Dit staat in artikel 9 tweede lid onder g respectievelijk artikel 10 van de AVG. Deze passende en specifieke maatregelen kunnen bijvoorbeeld bestaan uit het opnemen van een bewaartermijn, maar ook uit andere passende en specifieke maatregelen. In navolging van het advies van de Afdeling advisering is er voor gekozen om in artikel 6, derde lid van het wetsvoorstel op te nemen dat persoonsgegevens die noodzakelijk zijn in verband met de uitvoering van de taken van de Autoriteit en de administratieve en gerechtelijke procedures niet langer kunnen worden bewaard dan noodzakelijk voor de doeleinden waarvoor ze zijn verzameld en in ieder geval niet langer dan een jaar na de laatste verwerking.

Gelet op het beginsel van opslagbeperking is het uitgangspunt dat (bijzondere) persoonsgegevens niet langer worden bewaard dan noodzakelijk is voor de doeleinden waarvoor zij zijn verzameld. Voor het onderhavige wetsvoorstel betekent dit dat persoonsgegevens en een kopie van de online-inhoud in beginsel dertien maanden moeten worden bewaard, opdat kan worden vastgesteld of een bedrijf in de afgelopen 12 maanden 2 of meer keer is blootgesteld aan terroristische online-inhoud en er een blootstellingsbesluit kan worden genomen. Ook voor het afhandelen van het bezwaar is deze termijn passend.

Voor de afhandeling van de beroep- of klachtenprocedures is het noodzakelijk om persoonsgegevens langer te bewaren. Deze gegevens zullen immers noodzakelijk zijn bij het voeren van de genoemde procedures. Een termijn van een jaar na de laatste verwerking van de persoonsgegevens wordt daarbij passend geacht, opdat ook de termijn van het instellen van vervolgprocedures zal zijn verstreken. Na afronding van deze procedures en nadat een eventuele beroepstermijn is verstreken, zullen persoonsgegevens worden verwijderd.

Naast het opnemen van een concrete bewaartermijn in de wet is voorzien in passende en specifieke maatregelen door het opnemen van een loggingsverplichting en een geheimhoudingsverklaring voor medewerkers van de Autoriteit. Tevens zullen slechts die personen die werkzaam zijn bij de Autoriteit en die toegang nodig hebben voor de uitoefening van hun taken toegang hebben tot de genoemde persoonsgegevens.

6. Advisering

Het wetsvoorstel strekt tot uitvoering van een verordening en deze wordt beleidsarm uitgevoerd. Zoals hiervoor is vermeld zijn het wetsvoorstel en de verordening gelet op het belang voor de praktijk wel besproken met de belangrijkste stakeholders middels een MKB-toets. De resultaten hiervan zijn beschreven in paragraaf 5.

Het wetsvoorstel is gedurende een termijn van vier weken geplaatst op internetconsultatie.nl en ter consultatie toegezonden aan een aantal instanties. Er zijn adviezen ontvangen van de Raad voor de rechtspraak (Rvdr), het college van procureurs-generaal, de Nederlandse Orde van Advocaten (NOvA), de Stichting Digitale Infrastructuur Nederland (DINL) & de vereniging Dutch Cloud Community (DCC) en de Autoriteit Persoonsgegevens (hierna: AP). Er is één anonieme reactie ontvangen via internetconsultatie.nl Het Adviescollege toetsing regeldruk (hierna: ATR) heeft het dossier niet geselecteerd voor een formeel advies, omdat dit wetsvoorstel één op één implementatie van Europese regelgeving betreft.

De regering is iedereen erkentelijk voor de ontvangen adviezen. De noodzaak om de verspreiding van terroristisch online-inhoud zo veel mogelijk te beperken, wordt onderschreven door de Rvdr, DINL & DCC. Er zijn in de consultatie-reacties diverse vragen gesteld. Hierna worden de adviezen samengevat weergegeven en thematisch besproken.

Gehanteerde definities

De NOvA raadt aan om in het wetsvoorstel bestuursrechtelijke aanpak online kinderpornografisch materiaal en het onderhavige wetsvoorstel dezelfde definitie van het begrip «aanbieder van hostingdiensten» te gebruiken. Daarnaast vraagt de NOvA om verduidelijking van het begrip «objectief te rechtvaardigen technische of operationele redenen» als genoemd in artikel 3, zevende lid van de verordening, in het bijzonder met betrekking tot kleinere aanbieders van hostingdiensten.

Voor het begrip «aanbieder van hostingdiensten» is in dit wetsvoorstel aangesloten bij de definitie zoals opgenomen in artikel 2, onder 1, van de verordening. Voor wat betreft de definitie van begrip «aanbieder van hostingdiensten» is in het wetsvoorstel voor een bestuursrechtelijke aanpak online kinderpornografisch materiaal is aangesloten bij artikel 138g Sv, dat weer aansluit bij artikel 14 Richtlijn inzake elektronische handel (2000/31 EG). Het is in het onderhavige wetsvoorstel niet mogelijk om af te wijken van de definitie als gegeven in de verordening.

Indien de aanbieder van hostingdiensten het verwijderingsbevel niet binnen een uur na de ontvangst ervan kan uitvoeren, vanwege overmacht of omdat het feitelijk onmogelijk is, met inbegrip van objectief te motiveren technische of operationele redenen, moet hij de bevoegde autoriteit die het verwijderingsbevel heeft uitgevaardigd daarvan zo spoedig mogelijk in kennis stellen. De aanbieder van hostingdiensten dient het verwijderingsbevel na te leven zodra de situatie opgelost is. De omstandigheid dat een aanbieder van hostingdienst klein is, levert als zodanig geen « objectief te rechtvaardigen technische of operationele reden» op die in de weg staat aan het voldoen aan de termijn van 1 uur voor verwijdering. Bij de totstandkoming van de verordening is onderkend dat de bepalingen die betrekking hebben op de 24/7 bereikbaarheid van aanbieders van hostingdiensten en de verwijderingstermijn van één uur vooral voor kleine aanbieders van hostingdiensten problematisch kan zijn. In de verordening is om deze reden bepaald dat de aanbieder van hostingdiensten vrij moet zijn om gebruik te maken van een bestaand contactpunt, op voorwaarde dat het contactpunt de in deze verordening vastgestelde functies kan uitoefenen.

Bereikbaarheid en verwijderingstermijn

DINL en DCC verwachten problemen bij het opvolgen van de verwijderingstermijn. Van het MKB kan volgens DINL en DCC niet worden verwacht dat content op ieder moment van de dag binnen één uur offline gehaald wordt, zeker niet als het risico bestaat dat het bevel niet volledig accuraat, specifiek en uitvoerbaar is. Ook voorzien zij problemen bij de 24/7 gevraagde bereikbaarheid om een dergelijk bevel in ontvangst te kunnen nemen en gelijk te handelen.

Het is inderdaad zo dat aanbieders van hostingdiensten dienen te voldoen aan de verplichting om 24/7 bereikbaar te zijn opdat zij kunnen voldoen aan de verwijderingstermijn van één uur. Omdat deze verplichtingen vooral voor kleine aanbieders van hostingdiensten problematisch kunnen zijn, voorziet de verordening in artikel 15, eerste lid, in de mogelijkheid voor de aanbieder van een hostingdienst om gebruik te maken van een extern contactpunt, op voorwaarde dat het contactpunt de in deze verordening vastgestelde functies kan uitoefenen. Daarnaast schrijft de verordening in artikel 3, vierde lid, voor welke elementen in het verwijderingsbevel moeten worden opgenomen, waarmee wordt geborgd dat het verwijderingsbevel voldoende specifiek en uitvoerbaar is.

Bewaartermijn

Volgens DINL en DCC kunnen niet alle diensten voldoen aan de verplicht gestelde bewaartermijn. Aanbieders van bijvoorbeeld «unmanaged hosting» kunnen online-inhoud wel ontoegankelijk maken maar niet opslaan omdat zij tot de inhoud geen toegang hebben. DINL en DCC zien daarom graag een uitzondering voor dit type diensten.

De verordening bevat in artikel 6 de plicht voor aanbieders van hostingdiensten om terroristische online-inhoud die is verwijderd of geblokkeerd te bewaren en bevat geen uitzonderingen op die plicht. Nu deze verplichtingen voortvloeien uit de verordening, hebben aanbieders van hostingdiensten de verantwoordelijkheid hieraan te voldoen. Het Ministerie van Justitie en Veiligheid zal vertegenwoordigers van de sector structureel betrekken bij de implementatie, teneinde gezamenlijk te komen tot een werkbare uitvoering van deze bepaling uit de verordening.

De Autoriteit

DINL en DCC vragen de inzet en middelen voor de operationele uitvoering door de toezichthouder in de wet te borgen. De NOvA vraagt aandacht voor het waarborgen van kennis bij de autoriteit en daarmee samenhangend om ervoor te zorgen dat de autoriteit de middelen krijgt om daaraan gevolg te geven. Voorts wordt door DINL en DCC gevraagd hoe door de Nederlandse toezichthouder zal worden omgegaan met een door een andere lidstaat uitgevaardigd verwijderingsbevel. Gelet op de grote culture verschillen tussen de lidstaten, zien hostingbedrijven zich graag verzekerd van een interpretatie die past bij de Nederlandse culturele vrijheden en waarden. Daarnaast vraagt de NOVA toe te lichten waarom ervoor is gekozen twee autoriteiten op te richten voor enerzijds het ontoegankelijk maken van de kinderpornografisch materiaal en anderzijds het ontoegankelijk maken van terroristische online-inhoud. Tot slot raadt de NOvA aan de leden van de Autoriteit te verbieden een financieel belang te hebben in een aanbieder van een hostingdienst.

Alle lidstaten en dus ook Nederland zijn op grond van artikel 13, eerste lid, van de verordening verplicht de autoriteit voldoende middelen te verschaffen om de doelstellingen uit de verordening te verwezenlijken en de verplichtingen die de autoriteit op grond van de verordening heeft na te komen. In paragraaf 4.1 is beschreven welke incidentele en structurele middelen beschikbaar zullen zijn voor de Autoriteit. Dit is gebaseerd op een startscenario dat bestaat uit de minimale vereisten waar de Autoriteit aan moet voldoen volgens de verordening. Hiervoor is een inschatting gemaakt van de personele, ICT-, huisvesting- en overige verwachte kosten.

Indien de bevoegde autoriteit in Nederland op grond van artikel 4, eerste lid, van de verordening een afschrift van een verwijderingsbevel ontvangt van een buitenlandse autoriteit, kan de Nederlandse autoriteit op eigen initiatief binnen 72 uur na ontvangst het verwijderingsbevel toetsen om te bepalen of het een ernstige of kennelijke inbreuk inhoudt op de verordening of op de grondrechten en vrijheden zoals verankerd in het Handvest. De Autoriteit kan ook een toetsingsverzoek ontvangen van de aanbieder van hostingdiensten of de aanbieder van inhoud binnen 48 uur na ontvangst van respectievelijk het verwijderingsbevel en het afschrift van het verwijderingsbevel (ook op grond van artikel 4). Daarmee kan de Nederlandse Autoriteit recht doen aan de in artikel 4, eerste lid van de verordening genoemde rechten.

De NOvA vraagt naar de samenloop van het onderhavige wetsvoorstel met het wetsvoorstel bestuursrechtelijke aanpak online kinderpornografisch materiaal. Zoals in de Kamerbrief van 20 november 2020 is aangekondigd zal de Autoriteit zich tevens gaan richten op de ontoegankelijkmaking van online kinderpornografisch materiaal. Hiervoor wordt één Autoriteit opgericht, die beide taken zal vervullen. In artikel 14 van het onderhavige wetsvoorstel is een samenloopbepaling opgenomen voor het wetsvoorstel bestuursrechtelijke aanpak online kinderpornografisch materiaal. Aan de vraag of te benoemen leden van de Autoriteit een (financieel) belang hebben in een aanbieder van een hostingdienst, zal aandacht worden besteed in de wervingsfase voor leden van de Autoriteit en in stukken waar de integriteit aan de orde komt, zoals het bestuursreglement.

Verhouding Autoriteit – OM

De RvdR adviseert om in de toelichting nader in te gaan op de verhouding tussen de bevoegdheden van de Autoriteit en die van het Openbaar Ministerie om te voorkomen dat in individuele zaken de opsporing, vervolging en berechting van terroristische misdrijven verstoord wordt. Daarbij vragen zij in het bijzonder aandacht voor de vraag hoe het op grond van artikel 8 van het wetsvoorstel te voeren overleg eruit moet zien en welke bevoegdheidsuitoefening prevaleert.

Benadrukt wordt dat de verordening en de uitvoeringswet geen afbreuk doen aan de mogelijkheden tot strafrechtelijke opsporing, vervolging en berechting van diegenen die terroristische online-inhoud vervaardigen of verspreiden. De verordening en de uitvoeringswet zijn er louter op gericht terroristische online-inhoud zo snel mogelijk ontoegankelijk te doen maken. De Autoriteit enerzijds en opsporings- en inlichtingendiensten, het OM en de politie anderzijds bepalen in onderling overleg hoe de afstemming op grond van artikel 8 van de uitvoeringswet vorm krijgt.

Verhouding tot het strafrecht

De RvdR vraagt nader in te gaan op het verschil in rechtsbescherming dat bestaat tussen de uitoefening van de bevoegdheid van artikel 125p Sv, waar rechterlijke toetsing is voorzien aan de voorkant, en de vergelijkbare bevoegdheid van artikel 3 van de verordening, waarbij rechterlijke toetsing plaatsvindt als de beperking al heeft plaatsgevonden. De RvdR vraagt voorts aandacht voor de verbinding tussen het wetsvoorstel en de Wet justitiële en strafvorderlijke gegevens (Wjsg) en de Wet politiegegevens (Wpg). Dit acht de RvdR gewenst nu er sprake zal zijn van gegevensuitwisseling tussen de bevoegde autoriteiten en Europol en de nationale politie.

Het doel van de verordening is het tegengaan van verspreiding van terroristische online-inhoud en geen strafrechtelijke vervolging of opsporing van terroristische misdrijven. Door zowel de Raad als het Europees Parlement werd ondersteund dat snelheid daarbij prioriteit heeft om verdere verspreiding tegen te gaan. De insteek van de verordening is dan ook dat er geen aanvullende rechtelijke toets vooraf plaats vindt om aan de eis van een verwijderingstermijn van 1 uur te kunnen voldoen bij het opvolgen van verwijderingsbevelen. Overigens heeft Nederland zich er tijdens de EU-onderhandelingen hard voor gemaakt dat er een toegankelijk rechtsmiddel beschikbaar moet zijn in lijn met motie Van Nispen/Toorenburg.[22] In deze motie wordt de regering opgeroepen zich te verzetten tegen een voorstel waarin een verwijderingsbevel uit een andere lidstaat rechtstreeks moet worden opgevolgd, als daar tegen geen rechtsmiddel open staat in de ontvangende lidstaat. Zoals in paragraaf 3.5 is aangegeven staat tegen de diverse besluiten die op grond van de verordening worden genomen de gebruikelijke bestuursrechtelijke rechtsbescherming open zoals geregeld in de Algemene wet bestuursrecht. Dit betekent dat er bezwaar open staat, gevolgd door beroep bij de bestuursrechter en ten slotte hoger beroep bij de Afdeling bestuursrechtspraak van de Raad van State. Daarmee is voorzien in een voldoende rechtsbescherming.

Ten aanzien van de uitwisseling van gegevens tussen de Autoriteit en de politie kan het volgende worden opgemerkt. De onderhavige uitvoeringswet geeft de Autoriteit in artikel 9 een grondslag voor de verwerking van bijzondere en strafrechtelijke persoonsgegevens. Artikel 8, tweede lid

[22] Kamerstukken II, 2018–19, 22 112, nr. 2724.

van deze uitvoeringswet voorziet vervolgens in een grondslag voor de Autoriteit om deze gegevens verkregen bij de uitvoering van de aan hem krachtens deze wet opgedragen taken, aan de politie te verstrekken voor zover deze persoonsgegevens of inlichtingen noodzakelijk zijn voor de uitoefening van diens wettelijke taak, danwel aan de Algemene Inlichtingen- en Veiligheidsdienst en Militaire Inlichtingen- en Veiligheidsdienst voor zover deze noodzakelijk kunnen zijn voor hun taken op grond van de Wet op de inlichtingen- en veiligheidsdiensten 2017. Vervolgens geldt voor politie en de veiligheidsdiensten het op hen geldende wettelijke regime voor bescherming van persoonsgegevens en de daarbij behorende rechtsbescherming.

Ten aanzien van de uitwisseling van gegevens tussen de Autoriteit en Europol kan worden opgemerkt dat de verordening zelf een grondslag biedt voor de uitwisseling van gegevens tussen de Autoriteit en waar passend Europol.

Bestuursrechtelijke aspecten

De RvdR wijst er op dat de Autoriteit op grond van artikel 10 van het wetsvoorstel bevoegd is om een last onder dwangsom op te leggen ter handhaving van het bepaalde in artikel 18, eerste lid van de verordening, maar meent dat die niet goed mogelijk is omdat laatstgenoemd artikel alleen normen voor de lidstaat bevat. Daarnaast meent de RvdR dat in artikel 11 van het wetsvoorstel, dat voorziet in een boetebevoegdheid van de Autoriteit bij overtreding van enkele artikelen uit de verordening, de formulering uit deze artikelen van de verordening te weinig specifiek is. Overtreding hiervan die gesanctioneerd kan worden met een bestuurlijke boete is daardoor volgens de RvdR lastig vast te stellen. Zij adviseert daarom artikel 10 en 11 aan te passen. De NOvA heeft er op gewezen dat in artikel 11 van het wetsvoorstel wordt verwezen naar onjuiste artikelen uit de verordening.

Artikel 18, eerste lid van de verordening somt de artikelen op waarvoor de lidstaten voorschriften moeten vaststellen ten aanzien van sancties die van toepassing zijn op inbreuken van deze artikelen. Artikel 11 en 12 van het huidige wetsvoorstel voorzien in de in artikel 18, eerste lid van de verordening genoemde verplichting. In de consultatieversie van het wetsvoorstel bevatte het toenmalige artikel 11 (huidige artikel 12) onjuiste verwijzingen naar de in artikel 18, eerste lid van de verordening genoemde artikelen. Dit is aangepast. Nu de verordening reeds is aangenomen, is er geen nationale ruimte om af te wijken van de in artikel 18, eerste lid van de verordening genoemde artikelen waarvoor voorschriften moeten worden vastgesteld ten aanzien van sancties.

Verhouding tot verbod op algemene toezichtsverplichtingen

Tot slot vraagt de RvdR hoe de verplichting voor aanbieders van hostingdiensten om specifieke maatregelen te treffen om de verspreiding van terroristische online-inhoud via hun dienst tegen te gaan zich verhoudt tot het verbod op een algemene monitorverplichting voor aanbieders van hostingdiensten, zoals opgenomen in de Richtlijn inzake elektronische handel.[23]

[23] Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt.

De verplichting om specifieke maatregelen te treffen geldt niet voor alle aanbieders van hostingsdiensten, maar alleen bij aanbieders ten aanzien van wie de Autoriteit een blootstellingsbesluit heeft genomen. Deze aanbieders dienen specifieke maatregelen te treffen, zoals bijvoorbeeld genoemd in artikel 5, tweede lid van de verordening. De keuze van de specifieke maatregelen blijft bij de aanbieder van hostingdiensten berusten. Daarbij bepaalt artikel 5, lid 8 van de verordening dat de verplichting tot het nemen van specifieke maatregelen geen afbreuk doet aan artikel 15, lid 1, van de Richtlijn elektronische handel en dat deze voor aanbieders van hostingdiensten noch een algemene verplichting inhoudt om toezicht te houden op de informatie die zij doorsturen of opslaan, noch een algemene verplichting inhoudt om actief te zoeken naar feiten of omstandigheden die op illegale activiteiten duiden. De verplichting tot het nemen van specifieke maatregelen omvat evenmin een verplichting voor de aanbieder van hostingdiensten om automatische instrumenten te gebruiken.

Beperking rechten betrokkenen

De AP wijst er op dat betrokkene op grond van de AVG een verzoek kan indienen bij de Autoriteit om een beroep te doen op zijn rechten als betrokkene. In de toelichting was opgenomen dat deze rechten op grond van artikel 23, eerste lid, onder a AVG juncto artikel 41, eerste lid onderdeel a UAVG buiten toepassing konden worden gelaten voor zover dat noodzakelijk en evenredig was ter waarborging van de nationale veiligheid, de openbare veiligheid, de bescherming van betrokkenen of van rechten of vrijheden van anderen. De AP geeft daarbij aan dat onzeker is of de huidige opzet van artikel 41 UAVG tegemoetkomt aan de eisen van artikel 23 AVG. De AP wijst er op dat artikel 23, tweede lid AVG eist dat bepaalde aspecten in wetgeving worden geregeld terwijl artikel 41, tweede lid, UAVG deze aspecten overlaat aan de verwerkingsverantwoordelijke in het individuele geval. De AP adviseert gelet hierop ten aanzien van eventuele beperkingen in deze regelgeving uit te werken welke rechten van betrokkenen in welke omstandigheden in welke zin mogen worden beperkt.

Gelet op het advies van AP is een artikel (artikel 10) aan het wetsvoorstel toegevoegd en is paragraaf 5.2 aangepast.

II. Artikelsgewijs deel

Artikel 1. Definities

Dit artikel bevat de voor het voorstel benodigde definities.

Artikel 2. Autoriteit Online Terroristisch en Kinderpornografisch materiaal

Dit artikel regelt de oprichting van de Autoriteit Online Terroristisch en Kinderpornografisch materiaal. Dit is in paragraaf 3.1 van de memorie van toelichting toegelicht.

Artikel 3. Inrichting

Dit artikel regelt de inrichting van de Autoriteit en is in paragraaf 3.2 toegelicht.

Artikel 4. Bestuursreglement

In artikel 4 is opgenomen dat de Autoriteit een bestuursreglement vaststelt en dit na de goedkeuring als bedoeld in artikel 11 van de Kaderwet zelfstandige bestuursorganen in de Staatcourant bekend maakt. In de Kaderwet is geen verplichting opgenomen om een bestuursreglement vast te stellen. Het opstellen van een bestuursreglement dat goedkeuring behoeft van de Minister van Justitie en Veiligheid biedt ruimte om invulling te geven aan zijn algemene verantwoordelijkheid voor de Autoriteit en de verantwoordelijkheid die hij heeft ten aanzien van de op de lidstaat Nederland rustende verplichting uitvoering van de verordening.

Artikel 5. Kaderwet

Artikel 5 van onderhavig voorstel regelt het in paragraaf 3.2 en 3.3. beschreven maatwerk ten aanzien van de toepassing van de Kaderwet zbo's.

Artikel 6. Contactpunt en passende en veilige communicatiekanalen

In artikel 6, eerste lid, is opgenomen dat de Autoriteit ter uitvoering van artikel 12, tweede lid, van de verordening een contactpunt inricht en de informatie over dit contactpunt openbaar maakt. In het tweede lid is opgenomen dat de Autoriteit zorgt voor passende en veilige communicatiekanalen in de zin van artikel 14, derde lid, van de verordening. Beide bepalingen zijn opgenomen om te bewerkstelligen dat deze verplichtingen die in de verordening niet rechtstreeks aan de Autoriteit worden opgelegd, wel worden nagekomen en geen onduidelijkheid bestaat over de verantwoordelijkheid voor de nakoming van deze eisen.
In het derde lid is een voorziening getroffen voor de opslag van gegevens door de Autoriteit indien dit noodzakelijk is voor administratieve en gerechtelijke procedures. De verordening voorziet in regels voor opslag van gegevens door de aanbieders van hostingdiensten in artikel 6, eerste lid. De opslag voor gerechtelijke procedures door de bevoegde autoriteit is echter een nationale aangelegenheid. Bij het uitbrengen van een verwijderingsbevel wordt ingevolge de verordening in ieder geval een exacte uniform resource locator (URL-adres) opgenomen en, zo nodig, aanvullende informatie om de terroristische inhoud te kunnen identificeren. Het kan noodzakelijk zijn om in aanvulling daarop ook de terroristische online-inhoud op te slaan in het kader van bewijsvoering in gerechtelijke procedures. Daarbij is op advies van de Afdeling advisering van de Raad van State bepaald dat persoonsgegevens worden vernietigd zodra deze niet langer noodzakelijk zijn voor taken van de Autoriteit, in ieder geval uiterlijk een jaar na de laatste verwerking. Het derde lid van artikel 6 regelt dit.

Artikel 7. Elektronisch verkeer

Artikel 7 dient ter uitvoering van de bepalingen in de verordening die verplichten tot gebruikmaking van elektronische middelen waarbij er eisen worden gesteld aan de elektronische verzending van verwijderingsbevelen. Artikel 3, vierde lid, van de verordening bevat bijvoorbeeld de eis dat een verwijderingsbevel is voorzien van een (elektronisch) tijdstempel en een elektronische handtekening, waarbij in het vijfde lid is opgenomen dat elektronische middelen een schriftelijk bewijs moeten kunnen genereren op zodanige wijze dat authenticatie van de afzender mogelijk wordt, met inbegrip van de juistheid van de datum en het tijdstip van verzending en ontvangst van het bevel. Tevens is de Europese Commissie op grond van artikel 19 van de verordening bevoegd om gedelegeerde

handelingen vast te stellen die de verordening aanvullen met de nodige technische voorschriften voor de elektronische middelen die de bevoegde autoriteiten moeten gebruiken voor de verzending van verwijderingsbevelen. Om uitvoering te kunnen geven aan deze voorschriften en eventuele regels die de Commissie op grond van artikel 19, eerste lid, van de verordening vaststelt is in het tweede lid van artikel 7 dan ook opgenomen dat de Minister nadere regels kan stellen.

Artikel 8. Afstemming

Artikel 8 bevat in het eerste lid de verplichting voor de Autoriteit om te overleggen met de politie, het openbaar ministerie en de AIVD en de MIVD. Deze verplichting is opgenomen om te voorkomen dat de uitoefening van bevoegdheden door de Autoriteit bijvoorbeeld het onderzoeken of opsporen van terroristische misdrijven doorkruist. In het tweede lid is opgenomen dat de Autoriteit persoonsgegevens of inlichtingen verkregen bij de uitvoering van zijn krachtens de wet opgedragen taken aan de politie kan verstrekken voor zover deze noodzakelijk zijn voor de uitvoering van de politietaak zoals bedoeld in artikel 3 van de Politiewet 2012 en aan de AIVD en de MIVD gelet op hun taken op grond van de Wet op de inlichtingen- en veiligheidsdiensten 2017. De wijze waarop invulling wordt gegeven aan het overleg (bijvoorbeeld door middel van een «silent procedure») zal in samenspraak tussen de Autoriteit en de betrokken instanties ingevuld moeten worden. Net als de in artikel 14, vijfde lid, van de verordening opgenomen verplichting voor aanbieders van hostingdiensten om snel de voor de opsporing en vervolging bevoegde autoriteiten in te lichten indien zij stuiten op materiaal dat een onmiddellijk levensbedreigend gevaar inhoudt, kan ook de Autoriteit materiaal tegenkomen dat van belang is voor de opsporing en vervolging van terroristische misdrijven. Het tweede lid biedt dan ook een grondslag om deze gegevens met de politie te kunnen delen.

Artikel 9. Bijzondere persoonsgegevens

Dit artikel is in paragraaf 5.2 van deze memorie van toelichting toegelicht.

Artikel 10. Rechten van betrokkenen

Artikel 10 voorziet in de mogelijkheid om in concrete gevallen conform de voorwaarden die de AVG daaraan stelt de rechten van betrokkene te beperken. Dit is in paragraaf 5.2 toegelicht.

Artikel 11. Last onder dwangsom

Artikel 11 van onderhavig voorstel regelt dat de Autoriteit een last onder dwangsom kan opleggen ter handhaving van uit de verordening voortvloeiende verplichtingen.

Artikel 12. Bestuurlijke boete

Artikel 18, eerste lid, van de verordening bepaalt op welke inbreuken op de verordening de lidstaten voorschriften inzake sanctionering vaststellen. In artikel 12, eerste lid, van onderhavig voorstel is de bevoegdheid voor de Autoriteit geregeld om de overtreding van de betreffende voorschriften van de verordening een boete op te leggen. Het tweede lid bevat vervolgens de maximale boetehoogte.

Voor overtreding van artikel 3, derde en zesde lid, en 4, tweede en zevende lid van de verordening, die zien op de verplichting voor aanbieders van hostingsdiensten om binnen één uur na ontvangst van

een verwijderingsbevel terroristisch online-inhoud te verwijderen of ontoegankelijk te maken en dit te melden aan de bevoegde autoriteit, alsmede de verplichtingen omtrent grensoverschrijdende verwijderingsbevelen, is de tweede boetecategorie als bedoeld in artikel 23, vierde lid van het Wetboek van Strafrecht opgenomen. Er is gekozen voor de tweede categorie in verband met het in artikel 184 Wetboek van Strafrecht opgenomen sanctionering met dezelfde boetehoogte op het geen gehoor geven aan een ambtelijk bevel, in combinatie met de in artikel 125p van de in het Wetboek van Strafvordering opgenomen mogelijkheid tot afgifte van een bevel tot ontoegankelijk making. Voor overtreding van de overige voorschriften van de verordening is de maximale boetehoogte van de vijfde boetecategorie van het Wetboek van Strafvordering voorgesteld. Tot slot bevat het derde lid van artikel 12 conform artikel 18, derde lid, van de verordening een maximale boetehoogte voor systematisch en aanhoudend verzuim om terroristische online-inhoud te verwijderen of ontoegankelijk te maken.

Artikel 18, tweede lid, van de verordening vereist dat bij de sanctionering rekening gehouden wordt met de in de onderdelen a tot en met g opgenomen omstandigheden waaronder bijvoorbeeld de aard, de duur en de ernst van de inbreuk. Op grond van artikel 5:46, tweede lid, van de Algemene wet bestuursrecht geldt reeds dat het betreffende bestuursorgaan de bestuurlijke boete afstemt op de ernst van de overtreding en de mate waarin deze aan de overtreder kan worden verweten. Het bestuursorgaan houdt daarbij zo nodig rekening met de omstandigheden waaronder de overtreding is gepleegd. Deze omstandigheden betreffen uit hoofde van de verordening in ieder geval de in artikel 18, tweede lid, van de verordening opgenomen omstandigheden.

Artikel 13. Vervolgingsuitsluitingsgrond

Artikel 54a van het Wetboek van Strafvordering bepaalt thans dat een tussenpersoon die een communicatiedienst verleent bestaande in de doorgifte of opslag van gegevens die van een ander afkomstig zijn, bij een strafbaar feit dat met gebruikmaking van die dienst wordt begaan als zodanig niet wordt vervolgd indien hij voldoet aan een bevel als bedoeld in artikel 125p van het Wetboek van Strafvordering. Artikel 125p ziet op het in paragraaf 3.6 genoemde bevel tot ontoegankelijkmaking. Het ligt in de reden om ook ten aanzien van het gevolg geven aan een op grond van artikel 3, eerste lid, afgegeven verwijderingsbevel deze vervolgingsuitsluitingsgrond toe te passen. Het voorgestelde artikel 13 regelt dit.

Artikel14 bevat een samenloopbepaling voor het bij koninklijke boodschap van [PM datum] voorstel van wet [Wet bestuursrechtelijke aanpak van online kinderpornografisch materiaal ([PM Kamerstuknummer]). Deze samenloopbepaling bewerkstelligt dat het beoogde nieuwe zelfstandige bestuursorgaan slechts éénmaal wordt opgericht. Gelet op het verschil dat bestaat tussen artikel 2c van dat wetsvoorstel en artikel 5 van het onderhavige wetsvoorstel, wordt middels de samenloopbepaling aan artikel 2 van het onderhavige wetsvoorstel een vierde lid toegevoegd. De in het vierde lid opgenomen verplichting bevat een afwijking van de Kaderwet zbo's die voortvloeit uit de verordening. Om duidelijk en inzichtelijk te maken welke verplichtingen uit hoofde van de TOI-verordening op de Autoriteit rusten, is er voor gekozen deze verplichting in het onderhavige wetsvoorstel op te nemen. Ook is voorzien in een samenloopbepaling voor de beoogde wijziging van artikel 54a Sr.

Artikel 15 bevat een samenloopbepaling voor het bij koninklijke boodschap van 18 juli 2019 ingediende voorstel van wet tot wijziging van de Algemene wet bestuursrecht in verband met de herziening van

afdeling 2.3 van die wet (Wet modernisering elektronisch bestuurlijk verkeer). Hoewel het met dat wetsvoorstel voorgestelde artikel 2:7, derde lid, voorziet in een algemene grondslag voor het verzenden van een bericht langs elektronische weg, is niet uit te sluiten dat een aanbieder van hostingdiensten een natuurlijk persoon is. Een afwijking van het in dat wetsvoorstel voorgestelde artikel 2:8 blijft daarom noodzakelijk.

Artikel 16. Inwerkingtreding

De verordening is van toepassing met ingang van 7 juni 2022. Om die reden wordt op grond van de uitzondering «implementatie van bindende EU-rechtshandelingen, verdragen of andere besluiten van volkenrechtelijke organisaties» afgeweken van kabinetsbeleid inzake vaste verandermomenten en een minimuminvoeringstermijn, zoals opgenomen in aanwijzing 4.17 van de Aanwijzingen voor de regelgeving.

Deze toelichting wordt ondertekend mede namens de Minister van Binnenlandse Zaken en Koninkrijksrelaties.

De Minister van Justitie en Veiligheid,
D. Yesilgöz-Zegerius

Bijlage: transponeringstabel

Bepaling verordening	Uitvoeringsbepaling	Beleidsruimte	Toelichting
Artikel 1 Onderwerp en toepassingsgebied	Artikel 2, derde lid, voor wat betreft het eerste lid, onderdeel b van de verordening	–	–
Artikel 2 Definities	Geen nadere operationalisering vereist	–	–
Artikel 3 Verwijderingsbevelen	Geen nadere operationalisering vereist, met dien verstande dat ivm met het vijfde lid inzake het versturen van verwijderingsbevelen met elektronische middelen in artikel 7 verduidelijkt wordt dat artikel 2:14 van de Awb niet van toepassing is. Tevens is in artikel 7 een grondslag opgenomen voor het stellen van regels voor de uitvoering van het vierde en vijfde lid waarin eisen worden gesteld aan de wijze van verzending van berichten, waaronder de authenticatie van de afzender.		
Artikel 4 Procedure voor grensoverschrijdende verwijderingsbevelen	Geen nadere operationalisering vereist		
Artikel 5 Specifieke maatregelen	Geen nadere operationalisering vereist		
Artikel 6 Bewaring van inhoud en bijbehorende gegevens	Geen nadere operationalisering vereist		
Artikel 7 Transparantieverplichtingen voor aanbieders van hostingdiensten	Geen nadere operationalisering vereist		
Artikel 8 Transparantieverslagen van bevoegde autoriteiten	Geen nadere operationalisering vereist		
Artikel 9 Voorzieningen in rechte	Bestaand recht: artikel 1:3, derde lid, artikel 6:2 en hoofdstuk 7 en 8 Awb.		
Artikel 10 Klachtenmechanismen	Geen nadere operationalisering vereist		
Artikel 11 Informatie voor aanbieders van inhoud	Geen nadere operationalisering vereist		
Artikel 12 Aanwijzing van bevoegde autoriteiten	Artikel 2 Artikel 6, eerste lid.	De verordening bevat de randvoorwaarden voor aanwijzing van de bevoegde autoriteit. Binnen die voorwaarden is er beleidsruimte waar deze taak binnen de lidstaat te beleggen.	Dit onderdeel is toegelicht in paragraaf 3 van de memorie van toelichting.
Artikel 13 Bevoegde autoriteiten	Artikelen 2, 3 en 5.	–	De bevoegdheden en financiële middelen zijn in paragraaf 3.4 en 4.1 toegelicht. De onafhankelijkheid in paragraaf 3.1 tot en met 3.3 toegelicht.
Artikel 14 Samenwerking tussen aanbieders van hostingdiensten, bevoegde autoriteiten en Europol	Het derde lid van artikel 14 bevat de verplichting voor lidstaten om zorg te dragen voor passende en veilige communicatiekanalen of –mechanismen. Artikel 6, tweede lid, regelt dit.		
Artikel 15 Contactpunten van aanbieders van hostingdiensten	Geen nadere operationalisering vereist	–	–
Artikel 16 Rechtsmacht	Geen nadere operationalisering vereist		
Artikel 17 Wettelijke vertegenwoordiger	Geen nadere operationalisering vereist		

Bepaling verordening	Uitvoeringsbepaling	Beleidsruimte	Toelichting
Artikel 18 Sancties	Artikel 11 en 12	De verordening somt op voor welke inbreuken voorschriften inhoudende sancties moeten worden vastgesteld. De handhaving van de verordening is een nationale aangelegenheid.	Dit onderdeel is toegelicht in paragraaf 2.2 van de toelichting.
Artikel 19 Technische vereisten en wijzigingen van de bijlagen	Geen nadere operationalisering vereist		
Artikel 20 Uitoefening van de bevoegdheidsdelegatie	Geen nadere operationalisering vereist met dien verstande dat artikel 7, tweede lid, een grondslag biedt voor het stellen van regels ter uitvoering van de gelegeerde handelingen indien deze daartoe noodzaken.	–	–
Artikel 21 Monitoring	Artikel 5, tweede lid, ten aanzien van het verzamelen van de vereiste gegevens bij de autoriteit.	–	–
Artikel 22 Uitvoeringsverslag	Geen nadere operationalisering vereist		
Artikel 23 Evaluatie	–		
Artikel 24 Inwerkingtreding en toepassing	Geen nadere operationalisering vereist		
BIJLAGE I VERWIJDERINGSBEVEL (artikel 3 van Verordening (EU) 2021/... van het Europees Parlement en de Raad+)	Geen nadere operationalisering vereist		
BIJLAGE II FEEDBACK NA VERWIJDERING VAN OF BLOKKERING VAN DE TOEGANG TOT TERRORISTISCHE INHOUD	Geen nadere operationalisering vereist		
BIJLAGE III INFORMATIE OVER DE ONMOGELIJKHEID OM HET VERWIJDERINGSBEVEL UIT TE VOEREN	Geen nadere operationalisering vereist		