Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

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. 7

NOTA NAAR AANLEIDING VAN HET VERSLAG

Ontvangen 5 oktober 2022

Met veel belangstelling heb ik kennisgenomen van het verslag van de vaste commissie voor Justitie en Veiligheid. Graag maak ik van de gelegenheid gebruik om de in het verslag gestelde vragen te beantwoorden en te reageren op de gemaakte opmerkingen.

I. ALGEMEEN

1. Inleiding

De leden van de VVD-fractie hebben met belangstelling kennisgenomen van de 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) (hierna: het wetsvoorstel). Het is belangrijk dat alles op alles wordt gezet het misbruik van hostingdiensten voor illegale content, zoals terroristische doeleinden en kindermisbruik tegen te gaan en hierbij in het belang van onze nationale en internationale veiligheid samen te werken met alle lidstaten van de Europese Unie (EU). Deze leden onderschrijven de noodzaak van het wetsvoorstel en hebben nog enkele vragen aan de regering hierover.

De leden van de D66-fractie onderschrijven het belang van de verordening inzake het tegengaan van verspreiding van terroristische online-inhoud en van het toebedelen van de daarbij behorende taken en bevoegdheden aan een Nederlandse Autoriteit. Zij zijn echter nog niet overtuigd van de wijze waarop de Autoriteit op basis van dit wetsvoorstel wordt vormgegeven, in het bijzonder de wijze waarop de Autoriteit buiten de ministeriële verantwoordelijkheid wordt geplaatst. Zij hebben daarover nog enkele vragen.

De leden van de CDA-fractie hebben kennisgenomen van het voorliggende wetsvoorstel. Zij hebben geconstateerd dat het wetsvoorstel en de memorie van toelichting zijn aangepast naar aanleiding van het advies van de afdeling advisering van de Raad van State (hierna: de Afdeling).

kst-36138-7
ISSN 0921 - 7371
's-Gravenhage 2022

Ook begrijpen zij dat aangedrongen wordt op spoedige behandeling van het wetsvoorstel nu de Terroristisch Online Inhoud (TOI)-verordening op 7 juni 2022 van toepassing wordt en Nederland verplicht is per die datum uitvoeringsregelgeving gereed te hebben. Wel hebben zij nog een aantal inhoudelijke vragen ten aanzien van de op te richten Autoriteit.

De leden van de SP-fractie hebben met kritische belangstelling kennisgenomen van het bovengenoemde wetsvoorstel. Deze leden onderschrijven de strijd tegen terrorisme en terroristische online-inhoud. Recente aanslagen in de Europese Unie en daarbuiten hebben aangetoond dat terroristische inhoud zich via het internet razendsnel en soms zelfs live kan verspreiden. De doelstelling van de verordening wordt dan ook door deze leden gedragen. Desondanks hebben zij nog diverse vragen vooral in het licht van eerdere kritiek op het feit dat de autoriteiten die in de diverse lidstaten ingericht moeten worden vergaande bevoegdheden kregen in andere lidstaten.

Het lid van de BBB-fractie heeft met interesse kennisgenomen van het voorliggende wetsvoorstel en acht het van belang dat het verspreiden van terroristisch gedachtegoed moet worden tegengegaan. Daarbij heeft dit lid wel nog wat vragen.

2. De verordening

2.1 Totstandkoming verordening

De leden van de VVD-fractie lezen in de memorie van toelichting dat de Digital Services Act (DSA) een aanvulling is op de Terroristische Online Inhoud (TOI)-verordening en daaraan geen afbreuk mag doen. De DSA laat de TOI-verordening onverlet, zo schrijft de regering. Wel bevat het wetsvoorstel DSA-bepalingen om illegale online-inhoud aan te pakken, zo lezen deze leden in de memorie van toelichting. Dan blijft het van belang goed te onderscheiden wat exact zal worden geregeld via de bepalingen in de DSA en wat via de TOI-verordening wordt uitgevoerd. Kan de regering toelichten hoe de TOI-verordening zich verhoudt tot de DSA? Is het de verwachting dat naar aanleiding van eventuele implementatie van de DSA de uitvoeringswet TOI of bepalingen van de Wet bestuursrechtelijke aanpak online kinderpornografisch materiaal moeten worden gewijzigd, en zo ja, welke? Hoe wordt geanticipeerd op de DSA en doublures en versnippering van taken en bevoegdheden voorkomen?

De DSA zal in de toekomst het algemene kader vormen voor de bestrijding van illegale content online. Terroristische online-inhoud is daar één vorm van. Net als bijvoorbeeld laster, inbreuken op intellectuele eigendomsrechten, misleiding van consumenten, of bedreigingen. De DSA is daarmee een zogenoemde «lex generalis», ofwel horizontale wetgeving, die geen sectorspecifieke verboden of bepalingen bevat. Wel bevat de DSA minimumvereisten voor het tegengaan van álle onrechtmatige en strafbare content. De TOI-verordening daarentegen is een «lex specialis»: verticale sectorale wetgeving die toeziet op één specifieke vorm van illegale content: terroristische online-inhoud. Deze wetgeving bevat specifieke bepalingen voor de sector om maatregelen te nemen tegen terroristische online-inhoud en de verplichting om een autoriteit aan te wijzen die verwijderingsbevelen kan uitvaardigen om terroristische online-inhoud ontoegankelijk te doen maken. Het is een algemeen beginsel van het recht dat een lex specialis voorrang heeft op een lex generalis. Waar het om terroristische online-inhoud gaat heeft de TOI-verordening dus voorrang en is de DSA aanvullend.
Omdat de DSA geen sectorspecifieke bepalingen bevat, wordt niet verwacht dat de uitvoering van de DSA tot aanpassing van de Uitvoe-

ringswet TOI-verordening zal leiden. Het wetsvoorstel voor een bestuursrechtelijke aanpak van online kinderpornografisch materiaal wordt naar verwachting na de zomer als separaat wetsvoorstel bij uw Kamer ingediend. Daarbij zal zo nodig rekening worden gehouden met de DSA. Er is reeds nauwe onderlinge samenwerking tussen het Ministerie van Justitie en Veiligheid, verantwoordelijk voor de uitvoering van de TOI-verordening en het Ministerie van Economische Zaken en Klimaat, verantwoordelijk voor de uitvoering van de DSA. Voor de uitvoering van de TOI-verordening en de DSA zal deze samenwerking komende periode verder worden geïntensiveerd. Die samenwerking moet er ook voor zorgen dat doublures worden voorkomen en versnippering van taken en bevoegdheden wordt voorkomen.

In het verlengde hiervan vragen deze leden of de regering ook kan ingaan op de verhouding tussen de TOI-verordening en de voorgestelde Child Sexual Abuse (CSA)-verordening? Deze leden merken hierbij in het bijzonder op dat bij het schriftelijk overleg over de informele JBZ-raad van 11 en 12 juli door de regering is aangegeven dat de TOI-verordening enkel en alleen ziet op aanbieders van hostingdiensten, terwijl de voorgestelde CSA-verordening ook ziet op aanbieders van interpersoonlijke communicatiediensten en enkele bevoegdheden geeft ten aanzien van internet accessproviders en software application stores.
De leden van de VVD-fractie menen dat het in de praktijk voor de nieuwe Autoriteit veel en extra complexiteit kan opleveren wanneer bevoegdheden ten aanzien van het offline halen van terroristische online-inhoud geheel anders van opzet zijn en bovendien overige bevoegdheden die zien op de aanpak van CSA op grond van de voorgestelde CSA-verordening niet alleen zien op hostingbedrijven, maar ook van toepassing zijn op interpersoonlijke communicatiediensten en internet accessproviders. In hoeverre heeft de regering hierop reeds geanticipeerd door zoveel mogelijk taken, bevoegdheden en handhavingsmodaliteiten te uniformeren, zodat de aanpak van TOI en CSA elkaar kunnen versterken in plaats van nodeloos veel verschillen ontstaan. Graag ontvangen deze leden een reactie van de regering hierop. In het verlengde van het voorgaande vragen deze leden of de TOI dan wel de CSA ook van toepassing is op bedrijven die kindermisbruik laten zien met games of virtual reality. Zo nee, waarom niet? Als deze specifieke soort bedrijven niet hieronder vallen, hoe zou dit alsnog te regelen zijn?

De TOI-verordening stelt regels 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 van het openbare internet te verwijderen. De Autoriteit online Terroristisch en Kinderpornografisch Materiaal (ATKM) zal in de Uitvoeringswet TOI-verordening als bevoegde autoriteit in de zin van de TOI-verordening worden aangewezen. De ATKM is bevoegd een verwijderingsbevel uit te vaardigen, op grond waarvan de aanbieder binnen een uur de terroristische online-inhoud dient te verwijderen. Daarnaast kan de autoriteit een «blootstellingsbesluit» jegens een aanbieder nemen. Dit verplicht aanbieders van hostingdiensten die aan terroristische online-inhoud zijn blootgesteld om specifieke maatregelen te nemen om te voorkomen dat dat vaker gebeurd. Op grond van de TOI-verordening kan een buitenlandse autoriteit een grensoverschrijdend verwijderingsbevel uitvaardigen jegens een aanbieder die zijn hoofdvestiging in Nederland heeft en omgekeerd kan de ATKM een verwijderingsbevel uitvaardigen jegens een aanbieder die zijn hoofdvestiging in een andere lidstaat heeft. De TOI-verordening voorziet in een procedure waarbij de aanbieder die met een dergelijk verwijderingsbevel wordt geconfronteerd, de autoriteit uit de lidstaat waar hij zijn hoofdvestiging heeft kan vragen te toetsen of sprake is van een ernstige of kennelijke inbreuk op de verordening of op de grondrechten en

vrijheden zoals verankerd in het Handvest. De TOI-verordening is per 7 juni 2022 van toepassing geworden.
De voorgestelde Verordening ter voorkoming en bestrijding van seksueel kindermisbruik (CSA-verordening) ziet op de voorkoming en bestrijding van seksueel kindermisbruik, waaronder online kinderpornografisch materiaal en grooming vallen. De verordening maakt het mogelijk verplichtingen op te leggen aan aanbieders van hostingdiensten, aanbieders van interpersoonlijke communicatiediensten en in bepaalde gevallen ook aan internet access providers en software application stores. Daarnaast verplicht de CSA-verordening elke lidstaat tot het aanwijzen van coördinerende autoriteiten. De coördinerende autoriteiten hebben rechtsmacht ten aanzien van aanbieders die hun hoofdvestiging hebben in de lidstaat van die coördinerende autoriteit. Het voorstel voor de CSA-verordening wordt momenteel in de Raadswerkgroep besproken en over de inhoud daarvan moet nog worden onderhandeld. Uw Kamer is over de inhoud voor de CSA-verordening geïnformeerd middels het BNC-fiche[1] en ook middels de inbreng verslag van een schriftelijk overleg over de geannoteerde agenda van de informele JBZ-Raad van 11 en 12 juli 2022[2]. Gelet op de fase waarin de onderhandelingen over de CSA zich momenteel bevinden, is nog niet duidelijk welke autoriteit(en) Nederland zal aanwijzen om toezicht te houden op de uitvoering van de CSA.
Het kabinet deelt de opvatting van de VVD-fractie dat een uniforme aanpak waar mogelijk, bijvoorbeeld bij ondersteunende faciliteiten zoals systemen en detectie, van belang is. Hier wordt dan ook rekening mee gehouden in de voorbereidingen voor en de inrichting van de toekomstige ATKM. De regering bestudeert momenteel wat de precieze verschillen zijn tussen de voorgestelde CSA-verordening en de TOI-verordening en zal zich er voor inzetten dat, waar mogelijk, de verwijdering van zowel terroristische online-inhoud als online kinderpornografisch materiaal op een uniforme wijze kan worden ingericht[3].
Op bedrijven die seksueel kindermisbruik laten zien met games of virtual reality is de CSA is ook van toepassing. De definitie van «materiaal van seksueel misbruik van kinderen» omvat namelijk volgens de CSA-verordening: materiaal dat kinderpornografie of pornografische voorstelling vormt, zoals gedefinieerd in artikel 2, respectievelijk de punten c) en e), van de Richtlijn kindermisbruik.[4] Daaronder kan ook virtuele kinderpornografie vallen – dat wil zeggen: materiaal dat is vervaardigd zonder de directe betrokkenheid van een echt kind – zoals seksueel misbruik van kinderen getoond met games of virtual reality. Dit geldt, gelet op het onderwerp waarop de TOI-verordening betrekking heeft, niet voor de TOI-verordening.

2.2 Inhoud verordening

De leden van de SP-fractie constateren dat de regering met deze uitvoeringswet de verordening inzake het tegengaan van de verspreiding van terroristische online-inhoud uitvoert. De regering geeft echter aan dat Nederland al in grote mate voldoet aan de verordening. In de praktijk ziet de wet alleen toe op het inrichten van de Autoriteit Online Terroristische en Kinderpornografisch Materiaal (AOTKM) als zelfstandig bestuurs-

---

[1] Kamerstukken II 2020/21, 22 112, nr. 2926.
[2] Kamerstukken II 2021/22, 32 317, nr. 767.
[3] Tevens ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer.
[4] Richtlijn 2011/93/EU van het Europees Parlement en de Raad van 13 december 2011 ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie, en ter vervanging van Kaderbesluit 2004/68/JBZ van de Raad (PbEU 2011, L 335).

orgaan (zbo). Deze leden onderschrijven het oprichten van een Autoriteit die terroristisch materiaal gaat laten verdwijnen. Daarin bestaat thans een lacune.
Hebben de leden van de SP-fractie het goed begrepen dat de AOTKM via automatische werken het internet gaat afspeuren op zoek naar materiaal dat als terroristische inhoud geldt en dat de beoordeling of materiaal daadwerkelijk onder deze verordening valt ook door een geautomatiseerd werk kan worden verricht? Waarom is hier volgens de regering geen sprake van automatische censuur van het internet? Klopt het tevens dat hostingdiensten niet tot automatische beoordeling worden aangezet? Is het bij grote hostingdiensten niet veel voordeliger met automatische filters te gaan werken waarmee automatische surveillance alsnog uit deze verordening volgt? Kan de regering kortom nog eens uitleggen waarom deze vergaande inbreuk op de mensenrechten geoorloofd is zonder tussenkomst van een rechter en of er voldoende waarborgen gaan gelden? Waarom zou hier geen sprake zijn van een opmaat naar grootschalige internetsurveillance of surveillance kapitalisme? Kan de regering uitgebreid stilstaan bij dit kritieke punt van zorg?

Er wordt momenteel onderzocht op welke wijze geautomatiseerde zoekslagen kunnen helpen bij het detecteren van vermoedelijk terroristische online-inhoud. In de memorie van toelichting bij het wetsvoorstel heb ik aangegeven dat bij de detectie van vermoedelijk terroristische online-inhoud gebruik wordt gemaakt van geautomatiseerde monitoringsinstrumenten. Daarmee is niet gezegd dat sprake is van geautomatiseerde verwijdering van terroristische online-inhoud. Bij beoordeling van de vraag of de aangetroffen online-inhoud te bestempelen is als terroristisch online-inhoud vindt namelijk altijd een menselijke toets plaats (zie paragraaf 5.2 van de memorie van toelichting bij de Uitvoeringswet TOI-verordening). De definitie van terroristische online-inhoud in de TOI-verordening sluit aan bij de bestaande definities van terroristische misdrijven in de Richtlijn inzake terrorismebestrijding (Richtlijn 2017/541/EU) en is geïmplementeerd in het Nederlandse wetboek van strafrecht. Deze definitie is leidend voor de beoordeling voor het inzetten van de bevoegdheden van de autoriteit en dus voor het besluit om een verwijderingsbevel uit te vaardigen.
Het is juist dat artikel 5, lid 8 van de TOI-verordening het de autoriteit verbiedt specifieke maatregelen op te leggen die een aanbieder van hostingdiensten ertoe verplichten om geautomatiseerde instrumenten te gebruiken. Deze bepaling is op verzoek van Nederland opgenomen omdat het opleggen van de verplichting door de overheid in strijd is met artikel 7, derde lid, van de Grondwet. Dit Grondwetsartikel verbiedt iedere preventieve beperking van de uitingsvrijheid door de overheid die gegrond is op de inhoud ervan.[5] Dit laat overigens onverlet dat een aanbieder van hostingdiensten er zelfstandig voor kan kiezen om gebruik te maken van geautomatiseerde instrumenten zoals een upload filter, iets dat door veel platformen reeds wordt gedaan. Wanneer dergelijke geautomatiseerde instrumenten worden ingezet in het voorkomen van de verspreiding van terroristisch online-inhoud dient de aanbieder van hostingdiensten – conform overweging 23 in samenhang mat artikel 24 van de TOI-verordening – over de nodige capaciteiten te beschikken voor toezicht en verificatie door mensen. Daarnaast geldt ook voor aanbieders van hostingdiensten 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

[5] HR 7 november 1892, W 6259; Kamerstukken II 1975/76, 24 872, nr. 3, p. 18 en Kamerstukken II 1976/77, 13 872, nr. 7, p. 26. Zie ook B.P. Vermeulen, «Commentaar op artikel 7 van de Grondwet», in: E.M.H. Hirsch Ballin en G. Leenknegt (red.), Artikelsgewijs commentaar op de Grondwet, webeditie 2019 (www.nederlandrechtsstaat.nl).

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 (zie ook artikel 5, eerste lid van de TOI-verordening). Anders dan de SP is het kabinet gelet op het voorgaande van oordeel dat het detecteren van terroristische online-inhoud door de autoriteit en de verplichting voor aanbieders van hostingsdiensten om specifieke maatregelen te treffen niet kunnen worden aangemerkt als censuur.

3. Wetsvoorstel en uitvoering

3.1. De bevoegde instantie: keuze voor een zbo

De leden van de VVD-fractie hebben kennisgenomen van het voornemen van de regering de ATKM op te richten als zbo. Kan de regering duiden welke partijen zijn vertegenwoordigd in de ATKM, en met welke partijen de ATKM nu en in de toekomst nauw dient samen te werken?

De ATKM is een zelfstandig bestuursorgaan. Er is geen sprake van deelname of vertegenwoordiging van andere partijen in de ATKM. Verwijderingsbevelen worden dus gegeven door het zelfstandig bestuursorgaan ATKM; andere partijen zijn bij het geven van die bevelen niet betrokken. De ATKM zal voor de goede uitvoering van zijn werk contacten onderhouden met autoriteiten van andere lidstaten. De samenwerking met de hostingsector wordt momenteel nader vormgegeven als onderdeel van de voorbereiding van de oprichting van de ATKM. Daarnaast verplicht artikel 8, eerste lid van de Uitvoeringswet de autoriteit om te overleggen met de politie, het Openbaar Ministerie, de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (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.

Kan de regering bevestigen dat alle grondslagen teneinde informatie uit te wisselen tussen de ATKM en de samenwerkende partijen voortvloeien uit de verordening zelf of worden geregeld in onderhavig wetsvoorstel?

Voor wat betreft de grondslag om persoonsgegevens te delen met Europol en aangewezen autoriteiten in andere lidstaten volgt de grondslag uit de TOI-verordening zelf. Voor zover de verwerking van bijzondere of strafrechtelijke persoonsgegevens op grond van de Uitvoeringswet noodzakelijk is voor de uitoefening van de bevoegdheden van de autoriteit op grond van die wet, is een grondslag te vinden in artikel 9 van de Uitvoeringswet. Daarmee is een grondslag gegeven voor het delen van (bijzondere en strafrechtelijke) persoonsgegevens in het kader van bijvoorbeeld een verwijderingsbevel maar ook met de politie, het OM en de veiligheidsdiensten. Andere grondslagen om gegevens te delen dan voortvloeiend uit de verordening of de Uitvoeringswet zijn er inderdaad niet, kan ik deze leden bevestigen.

De leden van de D66-fractie constateren dat de Afdeling verschillende vraagtekens plaatst met betrekking tot de keuze voor een zbo, die door de regering maar deels worden geadresseerd. Daarmee wordt immers een uitzondering gemaakt op de grondwettelijk verankerde ministeriële verantwoordelijkheid en daarmee op het afleggen van verantwoordelijkheid aan het parlement en aan de samenleving. Kan de regering toelichten welke andere opties zij heeft overwogen voor het vormgeven van de Autoriteit? Kan zij daarbij specifiek toelichten welke bestaande

instanties hiervoor in aanmerking kwamen en waarom die uiteindelijk toch niet geschikt zijn bevonden? Welke keuzes maken andere lidstaten in het aanwijzen van een Autoriteit? De regering voert als argument aan om de ontoegankelijkmaking van terroristische online-inhoud niet bij het OM te beleggen, dat daarmee capaciteit vanuit het OM wordt vrijgehouden. Deze leden vragen in hoeverre het aantrekken van mensen voor een nieuwe Autoriteit verschilt van het aantrekken van extra mensen voor het OM ter uitvoering van deze taak. Kan de regering dit toelichten?

De leden van de CDA-fractie merken op dat het verantwoordingsonderzoek 2021 van de Algemene Rekenkamer (AR) begint als volgt: «Het Ministerie van JenV is een ingewikkeld departement waaronder ongeveer 50 organisaties met soms een grote mate van zelfstandigheid ressorteren. Het is voor de Minister dan ook een forse opgave om een dergelijke organisatie doeltreffend aan te sturen.» Deze leden vragen of de keuze voor een nieuwe zbo de aansturing van het departement niet ingewikkelder zal maken. Waarom denkt de regering dat dit toch de juiste keuze is met inachtneming van de aanbevelingen van de AR?

Het lid van de BBB-fractie merkt op dat door de Afdeling wordt gesteld dat een grondige en zorgvuldige motivering van de pro's en contra's voor de instelling van een nieuw zbo noodzakelijk is. Dit lid is het daarmee eens en kan, ondanks dat is aangegeven dat er nog geen orgaan is dat belast is met het verwijderen van online terroristisch materiaal, niet helder krijgen waarom deze bevoegdheid niet kan worden toebedeeld aan een al bestaande zbo. Kan de regering dit uitleggen?

Met het oog op de inrichting van de autoriteit is een verkenning uitgevoerd om te onderzoeken welke organisatievorm het meest geschikt was voor de uitvoering van de taken van de autoriteit op grond van de TOI-verordening. In deze verkenning is zowel gekeken naar het beleggen van de taken bij bestaande organisaties als naar de oprichting van een nieuwe organisatie. Daarbij is bezien of de taak kon worden uitgevoerd door het Agentschap Telecom, de Inspectie voor Justitie en Veiligheid (Inspectie JenV) en de Autoriteit Consument en Markt (ACM). Hieronder zal worden toegelicht waarom daar niet voor is gekozen.

Strafrecht of bestuursrecht?

Primair is verkend 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. Gelet hierop viel aanwijzing van het Openbaar Ministerie (hierna: OM) als autoriteit in de zin van de TOI-verordening af.

Verhouding tot de Minister

Vervolgens is bezien wat de verhouding van de autoriteit tot de Minister zou moeten zijn. Uitgangpunt van het kabinetsbeleid is dat publieke taken onder volledige ministeriële verantwoordelijkheid worden uitgevoerd, zodat de verantwoordelijke bewindspersoon op alle aspecten van de

uitvoering (politiek) aanspreekbaar is. Dat laat onverlet dat het in bepaalde situaties noodzakelijk kan zijn een zelfstandig bestuursorgaan in te stellen. In dit specifieke geval is de primaire reden voor de keuze om de taak van het ontoegankelijk doen maken van terroristische online-inhoud bij een zbo te beleggen de wens (de schijn van) politieke inmenging in de vrijheid van meningsuiting te voorkomen. Het ontoegankelijk maken van gegevens op internet, louter vanwege de inhoud daarvan, vormt naar zijn aard een beperking van de vrijheid van meningsuiting, zoals neergelegd in artikel 7 van de Grondwet en artikel 10 van het Europees Verdrag voor de Rechten van de Mens en de fundamentele vrijheden (EVRM). Het is vaste rechtspraak dat met (legitieme en noodzakelijke) beperkingen op dit grondrecht terughoudend en zorgvuldig moet worden omgegaan. Een bevoegdheid die de vrijheid van meningsuiting beperkt, moet daarom met voldoende waarborgen zijn omgeven, zodanig dat een willekeurige inmenging wordt voorkomen. Door de bevoegde autoriteit vorm te geven als een zbo waarbij aanvullende waarborgen zijn gesteld aan de vereiste onafhankelijkheid is naar het oordeel van de regering voldaan aan de vereiste onafhankelijke oordeelsvorming: een zbo is in zijn taakuitoefening niet hiërarchisch ondergeschikt aan enige politieke ambtsdrager, zodat oordeelsvorming onafhankelijk van de politiek is geborgd.

Gelet op de wens de autoriteit zodanig vorm te geven dat oordeelsvorming onafhankelijk van de politiek is geborgd, werd de Inspectie JenV, een dienstonderdeel van het Ministerie van JenV, niet geschikt geacht als autoriteit in de zin van de TOI-verordening. Bovendien past de taak die op grond van de TOI-verordening aan de autoriteit toekomt ook niet goed bij de andere taken van de Inspectie JenV. De Inspectie voor JenV houdt immers toezicht op andere organisaties op het terrein van JenV, terwijl van de bevoegde autoriteit op grond van de verordening wordt gevraagd onderzoek te doen naar terroristische online-inhoud en toe te zien op de naleving van verwijderingsbevelen van aanbieders van hostingdiensten.

Geen agentschap

Er is niet voor 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, omdat, anders dan voor een zbo geldt, deze hiërarchisch ondergeschikt is aan een Minister. Mede om die reden is er niet voor gekozen het Agentschap Telecom aan te wijzen als autoriteit in de zin van de TOI-verordening.

Geen regulier dienstonderdeel met inperking bevoegdheid Minister

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.

Keuze voor een nieuw zbo

Overwogen is om de ACM, ook een zbo, als autoriteit in de zin van de TOI-verordening aan te wijzen. Daarvoor is niet gekozen omdat het opschonen van internet van terroristische online-inhoud fundamenteel ongelijksoortig is aan de bestaande toezichtfuncties van de ACM, en zich bevindt in een voor de ACM onbekende keten. De werkzaamheden van de ACM hebben immers tot doel goed functionerende markten, ordelijke en transparante marktprocessen en een zorgvuldige behandeling van consumenten te bevorderen. Daaronder valt onder meer het bewaken, bevorderen en beschermen van een effectieve mededinging en gelijke concurrentievoorwaarden op markten en het wegnemen van belemmeringen daarvoor. De taak die de bevoegde autoriteit op grond van de TOI-verordening gaat uitoefenen, heeft een heel ander doel dat niet past bij de taak en het werkgebied van de ACM.

Omdat er geen bestaand zelfstandig bestuursorgaan was dat kon worden belast met het (doen) ontoegankelijk maken van terroristische online-inhoud, is gekozen voor het instellen van een nieuw zbo: de ATKM. De bevoegdheden die de Kaderwet zbo's toekent aan de Minister zijn in onderhavig voorstel zodanig ingeperkt, dat de Minister uitsluitend kan ingrijpen ten aanzien van het financieel beheer en de administratieve organisatie. De Minister blijft overigens verantwoordelijk voor het (wettelijk) stelsel. De Minister heeft daartoe enige bevoegdheden ten aanzien van het zbo, zoals het voordragen voor benoeming van de bestuurders en het financieel beheer.

Keuze voor het bestuursrecht

De leden van de CDA-fractie merken op dat de regering duidelijk maakt dat de verordening tot doel heeft terroristische online-inhoud zo spoedig mogelijk ontoegankelijk te maken en verdere verspreiding tegen te gaan. Niet om diegenen die de inhoud produceren en op internet plaatsen op te sporen en te vervolgen. Vandaar dat de keuze valt op het bestuursrecht. De voornoemde leden willen graag weten of ook andere EU-lidstaten een dergelijk onderscheid kennen tussen het bestuursrecht en het strafrecht en in dit geval om soortgelijke reden kiezen voor het bestuursrecht? Kan de regering aangeven welke andere EU-lidstaten kiezen voor het bestuursrecht? Zijn er ook lidstaten die kiezen voor het strafrecht? Zo ja, kan de regering aangeven waarom die lidstaten die keuze maken?

De bevoegde autoriteit(en) in de andere EU-lidstaten worden op verschillende wijze vorm gegeven. Zo kiest een aantal lidstaten ervoor de autoriteit onder te brengen bij de politie of het Openbaar Ministerie. Sommige EU-lidstaten kiezen ervoor de taken van de TOI-verordening te spreiden over meerdere bevoegde autoriteiten, bijvoorbeeld over meerdere ministeries of meerdere operationele instanties. Het kabinet beschikt niet over een uitputtend overzicht van de specifieke juridische inbedding van iedere EU-lidstaat ten aanzien van de implementatie van de TOI-verordening, mede omdat nog niet alle EU-lidstaten een autoriteit hebben aangewezen. Een overzicht van de EU-lidstaten die hun bevoegde autoriteit gereed hebben is te vinden op de website van de Commissie[6].

[6] Zie: https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/prevention-radicalisation/terrorist-content-online/list-national-competent-authority-authorities-and-contact-points_en.

3.2. Taken en positionering

De leden van de VVD-fractie begrijpen dat de TOI-verordening onder andere erop is gericht dat de Autoriteit hostingbedrijven aanspreekt wanneer Terroristische online inhoud niet op tijd wordt verwijderd. Onder hostingbedrijven hangen vaak resellers en daaronder hangt pas de content. Klopt het dat hostingbedrijven zich op geen enkele manier kunnen verschuilen achter voor hen onbekende resellers? In welke mate geldt voor hostingbedrijven straks het know-your-client-principe, in welke mate wordt dat geëist in de TOI-verordening en hoe wordt dat in Nederland straks geregeld?

Voor een goede beantwoording van deze vraag is het van belang goed te onderscheiden wie in de verordening wordt aangeduid als aanbieder van een hostingdienst. De aanbieder van hostingdiensten is degene die content opslaat voor de aanbieder van inhoud. Deze aanbieder van hostingdiensten kan opslagruimte huren bij een derde partij, bijvoorbeeld een datacenter. Artikel 15, eerste lid van de TOI-verordening verplicht elke aanbieder van een hostingdienst een contactpunt aan te wijzen of op te richten en de informatie daarover openbaar te maken. Hiermee wordt getracht te voorkomen dat de autoriteit een verwijderingsbevel stuurt naar een verhuurder van opslagruimte terwijl het verwijderingsbevel eigenlijk naar de reseller – als aanbieder van hostingdiensten als bedoeld in de verordening – had moeten worden gestuurd. De autoriteit kan de aanbieder van een hostingdienst sanctioneren wanneer deze verzaakt om een contactpunt aan te wijzen.
Het kan voorkomen dat de autoriteit het verwijderingsbevel richt aan de verhuurder van opslagruimte, aangezien die het IP-adres beheert. Op grond van artikel 3, achtste lid van de verordening dient een aanbieder van hostingdiensten aan te geven wanneer het verwijderingsbevel kennelijke fouten bevat waardoor hij het verwijderingsbevel niet uit kan voeren. Eén van die fouten kan zijn dat het verwijderingsbevel niet aan hem had moeten worden geadresseerd maar aan zijn klant. Daarnaast kan de autoriteit bij de verhuurder van de opslagruimte gegevens van de reseller vorderen (artikel 5:17 Algemene wet bestuursrecht). Dergelijke gegevens zullen dan wel bekend moeten zijn bij de verhuurder van de opslagruimte. Het is echter niet aannemelijk dat een reseller, als klant, volledig onbekend is. De reseller zal immers ook betalingsverplichtingen aan de verhuurder hebben voor de huur van opslagruimte.
De TOI-verordening verplicht niet tot het know-your-client-principe. De DSA gaat onlineplatforms die consumenten de mogelijkheid bieden overeenkomsten op afstand te sluiten met handelaren, zoals Booking.com, Instagram, TikTok, YouTube, Marktplaats, Bol.com, verplichten tot het know-your-client-principe (in artikel 24 quater van de DSA-verordening). Een dergelijke verplichting geldt echter niet voor aanbieders van hostingdiensten.

De leden van de D66-fractie merken op dat hoewel het logisch klinkt de Autoriteit op afstand te zetten ter bevordering van de onafhankelijkheid, is het gevolg daarvan dat deze niet meer onder de ministeriële verantwoordelijkheid valt en dus buiten de controle van het parlement. De noodzaak daartoe moet volgens deze leden dan ook stevig onderbouwd worden, zeker gegeven de ingrijpende bevoegdheden die de Autoriteit zal krijgen. De situatie moet voorkomen worden waarin de Tweede Kamer kritiek heeft op bijvoorbeeld te brede bevoegdheden voor de Autoriteit, zonder dat daar een debat over gevoerd kan worden met de regering. In de reactie op de Afdeling herhaalt de regering de argumentatie dat middels een zbo de onafhankelijke oordeelsvorming is geborgd. De Afdeling wijst er echter juist op dat de richtlijn niet zozeer voorschrijft dat de regering geen beleidsregels zou mogen opstellen voor de taakuitoefening van de

Autoriteit in het algemeen, enkel dat inmenging in concrete gevallen niet mogelijk moet zijn. Ook volgens de Kaderwet staat het stellen van beleidsregels niet in de weg van onafhankelijke taakuitoefening door een zbo. Daarom verzoeken deze leden de regering nogmaals te onderbouwen waarom ook het stellen van beleidsregels volledig buiten de ministeriële verantwoordelijkheid zou moeten worden geplaatst.

De bevoegdheden die de Kaderwet zbo's toekent aan de Minister zijn in onderhavig voorstel inderdaad zodanig ingeperkt, dat de Minister uitsluitend kan ingrijpen ten aanzien van het financieel beheer en de administratieve organisatie. Daarmee is onder andere de mogelijkheid voor de Minister om (vooraf vastgestelde) beleidsregels te stellen over zowel de taakuitoefening in algemene zin als ten aanzien van het beleid in individuele zaken, uitgesloten. Een bevoegdheid van de Minister om beleidsregels te stellen ten aanzien van de autoriteit past naar het oordeel van de regering in dit geval niet bij de vereiste onafhankelijkheid. Door het stellen van beleidsregels zou de Minister immers (kunnen) bepalen hoe de belangenafweging van de autoriteit plaats heeft, hoe de feiten worden vastgesteld of hoe wettelijke voorschriften bij het gebruik van de bevoegdheden van de autoriteit moeten worden uitgelegd. Juist gelet op het belang dat de regering hecht aan oordeelsvorming door de autoriteit onafhankelijk van de Minister acht zij het aangewezen de invloed van de Minister op de autoriteit door middel van deze uitzonderingen op de Kaderwet zbo's waar mogelijk in te perken. De Minister kan zich aldus niet mengen in de uitoefening van de kerntaak van de autoriteit.

De Minister kan door het parlement worden aangesproken op zijn stelselverantwoordelijkheid. Vandaar dat de Minister enige bevoegdheden ten aanzien van het zbo heeft, zoals het voordragen voor benoeming van de bestuurders en het financieel beheer.

De leden van de CDA-fractie vragen hoe het staat het met de voorbereiding van de bouw van de (definitieve) Autoriteit? Kan de regering de Kamer het tijdschema voor de oprichting van de Autoriteit sturen? Wie gaat de regering, tot het moment dat de definitieve Autoriteit geactiveerd is, met de taak belasten om verwijderbevelen uit te vaardigen? Hoe zorgt de regering ervoor dat een tijdelijke Autoriteit zoveel mogelijk tot onafhankelijke oordelen kan komen?

In de beantwoording op de gestelde vragen van het lid Bikker (ChristenUnie) heb ik uw Kamer op 9 juni 2022 geïnformeerd over de voortgang van de nieuw op te richten autoriteit.[7] De inrichting van de autoriteit verloopt voortvarend en het streven is de autoriteit in het najaar voor in ieder geval de taken die voortvloeien uit de TOI-verordening operationeel te laten zijn. Indien er onverhoopt van het tijdsschema wordt afgeweken, zal ik uw Kamer tijdig informeren.
Voor de implementatie van de TOI-verordening in Nederland is de onderhavige uitvoeringswet, die de bevoegde autoriteit aanwijst, noodzakelijk. De uitvoeringswet vormt de grondslag voor het aanwijzen van de autoriteit en het uitvoeren van de taken uit de verordening. Een tijdelijke oplossing, voorafgaand aan de inwerkingtreding van deze Uitvoeringswet, vereist eveneens een wettelijke basis en is daarom geen werkbaar tussentijds alternatief. Zie voor een uitgebreidere toelichting de beantwoording van de Kamervragen van lid Bikker over «de voortgang omtrent de autoriteit terroristische content en kinderporno».[8]

[7] Aanhangsel Handelingen II 2021/22, nr. 3063.
[8] Aanhangsel Handelingen II 2021/22, nr. 3063.

De leden van de SP-fractie hebben nog enkele vragen met betrekking tot de reikwijdte van het wetsvoorstel. Er kan namelijk een meningsverschil tussen de verschillende autoriteiten in de Europese lidstaten ontstaan over de definitie van terroristische inhoud. In het ergste geval kan dit zelfs worden misbruikt door de ene lidstaat om hostingdiensten in een andere lidstaat te censureren. Is de definitie van terroristische inhoud volgens de regering voldoende afgebakend om de AOTKM te bewapenen om zich te verzetten tegen onrechtmatige besluiten van de autoriteiten uit de andere lidstaten? Op wie zien de autoriteiten toe? Gaat het om de grote hostingdiensten, zoals YouTube, of wordt zelfs de hypothetische modelvliegtuigenclub uit Dieren met een online forum waarop de vijf leden zich begeven onderworpen aan de autoriteiten uit de lidstaten? Hoe zit het eigenlijk met natuurlijke personen die voor niet-zakelijk gebruik hostingdiensten aanbieden? Vallen die ook onder deze richtlijn? Hierbij denken deze leden bijvoorbeeld aan een online forum waarop discussies kunnen worden gevoerd of zelfs onschuldig kooktips worden gedeeld.

Wat onder terroristische inhoud wordt verstaan is beschreven in artikel 2, zevende lid van de TOI-verordening. Daarin wordt verwezen naar de definities van terroristische misdrijven en terroristische groeperingen in artikel 3 en 4 van Richtlijn (EU) 2017/541 inzake terrorismebestrijding.[9] Het gaat onder meer om materiaal dat aanzet tot het plegen van terroristische misdrijven indien dat materiaal direct of indirect, bijvoorbeeld door terroristische daden te verheerlijken, het plegen van terroristische misdrijven bepleit, waardoor een gevaar ontstaat dat een of meer van die misdrijven mogelijk worden gepleegd of een persoon of een groep personen aanspoort om deel te nemen aan de activiteiten van een terroristische groepering. De definities in de TOI-verordening sluiten derhalve nauw aan bij de bestaande definities van terroristische misdrijven in deze richtlijn en zoals geïmplementeerd in het Nederlandse wetboek van strafrecht. Daarmee is sprake van een goede afbakening van het begrip terroristische inhoud.

Daarnaast kent de TOI-verordening in artikel 4, derde lid en verder, de autoriteit het recht toe om binnen 72 uur een met redenen omkleed besluit te nemen, houdende dat een buitenlands 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. Aanbieders van hostingdiensten of aanbieders van inhoud kunnen de autoriteit in het land van vestiging hierom ook verzoeken waarna de autoriteit een oordeel moet vellen over het buitenlandse verwijderingsbevel. Daarvoor zou bijvoorbeeld aanleiding kunnen zijn indien de Nederlandse autoriteit van oordeel is dat niet is voldaan aan de definitie van terroristische inhoud. 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.
De bevoegde autoriteiten kunnen een verwijderingsbevel uitvaardigen aan een aanbieder van hostingdiensten. Een aanbieder van hostingdiensten is een aanbieder van diensten die erin bestaan informatie die door een aanbieder van inhoud is verstrekt, op diens verzoek op te slaan (zie artikel 1, punt b, van Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad). Een voorbeeld hiervan is een dienstverlener die aan particulieren of bedrijven ruimte aanbiedt om op diens servers

[9] 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, PbEU L 88.

websites, afbeeldingen of videobestanden op te slaan. Daarbij wordt geen onderscheid gemaakt tussen grote en kleine aanbieders van hostingdiensten en ook niet naar de aard van de hostingdienst (zakelijk of niet zakelijk). Een online platform waarop discussie wordt gevoerd of kooktips worden uitgewisseld dat zich op het openbare internet bevindt en dus publiek toegankelijk is, valt ook onder deze definitie.

Hoe zijn de vele, diverse hostingdiensten betrokken bij de totstandkoming van deze Uitvoeringswet? Deze leden lezen over het uitvoeren van een MKB-toets, maar zijn met name de kleine hostingdiensten wel echt betrokken geweest bij dit wetsvoorstel? Zo nee, waarom niet?

In het gehele proces, van de Europese onderhandelingen tot het inrichten van de ATKM, is de sector betrokken. Hierbij is getracht om alle typen aanbieders van hostingdiensten te betrekken. Voor wat betreft de kleine hostingdiensten is gebruik gemaakt van drie koepelorganisaties[10] die zowel grote, middelgrote als kleine bedrijven vertegenwoordigen en daarmee de belangen en kwetsbaarheden voor kleine hostingdiensten naar voren hebben gebracht. Daarnaast zijn, bijvoorbeeld in het kader van de MKB-toets, kleine hostingdiensten uitgenodigd om ook zelfstandig hun observaties met mijn ministerie te delen.

Hebben de leden van de SP-fractie het goed begrepen dat de regering het voornemen heeft de AOTKM later ook de bevoegdheid te geven om kinderpornografisch materiaal te laten verwijderen? Kan de regering deze keuze toelichten? Want hoe verhoudt deze Autoriteit zich dan tegenover het bestaande Expertisebureau Online Kindermisbruik (EOKM)? Daar kunnen partijen nu toch ook al een melding maken van het aantreffen van kinderpornografisch materiaal? Deze leden beseffen dat het EOKM geen verwijderingsbesluiten en blootstellingsbesluiten kan nemen of dwangsommen kan opleggen, maar het EOKM kan wel hostingdiensten reeds benaderen en werkt ook actief met hostingdiensten samen. Vreest de regering niet dat de AOTKM een deel van de rol van het EOKM gaat overnemen?

Het is juist dat de regering voornemens is de ATKM tevens de bevoegdheid te geven om online kinderpornografisch materiaal ontoegankelijk te doen maken. Een separaat wetsvoorstel voor een bestuursrechtelijke aanpak van online kinderpornografisch materiaal zal daartoe naar verwachting na de zomer bij Uw Kamer worden ingediend. Voor het beleggen van deze beide taken bij één autoriteit is gekozen omdat de taken gelijksoortig zijn en de systematiek van inhoudsverwijdering overeenkomt. Beide zien immers op het ontoegankelijk doen maken van strafbaar materiaal van het openbare internet. Het is daarom doelmatig en doeltreffend als één autoriteit beide taken uitvoert. Ook komt het de zichtbaarheid voor de sector die met de autoriteit te maken krijgt ten goede als beide taken zijn belegd bij één instantie.
Het is juist dat het Expertisebureau Online Kindermisbruik (EOKM) verzoeken doet aan aanbieders om op vrijwillige basis online kinderpornografisch materiaal ontoegankelijk te maken.[11] Ongeveer 84% van de meldingen van het EOKM wordt in dit regime van zelfregulering door de

[10] ISPconnect, NLDigital, Stichting DINL.
[11] Dit is vastgelegd in de gedragscode met addendum en ondertekend door Koepelverenigingen van hostingbedrijven en van digitale infrastructuur, telecombedrijven en internetbedrijven. De gedragscode is te raadplegen op https://www.noticeandtakedowncode.nl.

branche adequaat opgepakt.[12] Niettemin acht ik een wetsvoorstel waarin de autoriteit de wettelijke taak krijgt om online kinderpornografisch materiaal ontoegankelijk te doen maken noodzakelijk als sluitstuk van deze zelfregulering. In 16% van de gevallen wordt geen of onvoldoende opvolging gegeven aan een melding en blijft het kinderpornografisch materiaal op zijn minst langer dan 24 uur zichtbaar. Een wet waarbij de ATKM deze taak krijgt, is daarom onmisbaar om alle betrokken bedrijven te bewegen dit type materiaal op zo kort mogelijke termijn ontoegankelijk te maken en handhavend op te kunnen treden indien dat niet gebeurt. Het EOKM zal zich na inwerkingtreding van de wet bestuursrechtelijke aanpak van online kinderpornografisch materiaal bezig blijven houden met het doen van verzoeken om online kinderpornografisch materiaal vrijwillig ontoegankelijk te maken.

Daarnaast hebben leden van de SP-fractie vragen over de verhouding van het voornemen de Autoriteit ook de bevoegdheid te geven kinderpornografisch materiaal te bestrijden tot het recente voorstel van de Europese Commissie (EC) voor een verordening ter voorkoming en bestrijding van seksueel kindermisbruik. Dat voorstel creëert immers verplichtingen voor lidstaten die veel verder gaan dan dat de Nederlandse regering voor ogen lijkt te hebben. Klopt dat? Kan de regering exact de verschillen en overeenkomsten schetsen? Waarom heeft de EC er niet voor gekozen bij de bestrijding van kinderpornografisch materiaal aansluiting te zoeken bij de bestrijding van terroristisch online-inhoud?

De voorgestelde verordening voor de aanpak van seksueel kindermisbruik legt lidstaten verplichtingen op om de verspreiding van online seksueel kindermisbruik en grooming tegen te gaan. Dit voorstel wordt momenteel in de Raadswerkgroep besproken en er over de inhoud moet nog worden onderhandeld. Uw Kamer is over de inhoud van de CSA-verordening geïnformeerd middels het BNC-fiche[13] en ook middels de inbreng verslag van een schriftelijk overleg over de geannoteerde agenda van de informele JBZ-Raad van 11 en 12 juli 2022[14]. Het is juist dat de voorgestelde verordening een breder bereik heeft dan het wetsvoorstel voor een bestuursrechtelijke aanpak van online kinderpornografisch materiaal, omdat de verordening beoogt naast online seksueel kindermisbruik ook grooming te bestrijden. De verordening maakt het voorts mogelijk verplichtingen op te leggen aan aanbieders van hostingdiensten, aanbieders van interpersoonlijke communicatiediensten en in bepaalde gevallen ook aan internet access providers en software application stores. Daarnaast verplicht de CSA-verordening elke lidstaat tot het aanwijzen van coördinerende autoriteiten. De coördinerende autoriteiten hebben rechtsmacht ten aanzien van aanbieders die hun hoofdvestiging hebben in de lidstaat van die coördinerende autoriteit.
Het wetsvoorstel voor een bestuursrechtelijke aanpak van online kinderpornografisch materiaal wordt naar verwachting na de zomer bij uw Kamer ingediend. Naar verwachting ziet dit wetsvoorstel alleen op de verwijdering en ontoegankelijkmaking van kinderpornografisch materiaal en maakt het het mogelijk om verplichtingen op te leggen aan aanbieders van hostingdiensten en onder voorwaarden aan aanbieders van communicatiediensten. Ik ben voornemens de ATKM de bevoegdheid te geven om een bindende aanwijzing en een zorgplicht op te leggen. De ATKM kan

[12] Dit blijkt onder meer uit een monitor van de Technische Universiteit Delft. De monitor geeft inzicht in de effecten van de zelfregulering, door meldingen van het EOKM te volgen. Op 8 oktober 2020 is het rapport hierover genaamd »CSAM Hosting Monitor» aan de Tweede Kamer aangeboden (Kamerstukken II 2020/21, 31 015, nr. 203). Het rapport maakt inzichtelijk welke tussenpersonen in Nederland een rol hebben in het hosten, opschonen en schoonhouden van het internet van kinderpornografisch materiaal.
[13] Kamerstukken II 2020/21, 22 112, nr. 2926.
[14] Kamerstukken II 2021/22, 32 317, nr. 767.

op grond van het wetsvoorstel voor een bestuursrechtelijke aanpak van online kinderpornografisch materiaal een aanwijzing alleen richten tot aanbieders die in Nederland zijn gevestigd.
De regering bestudeert momenteel wat de precieze verschillen zijn tussen de voorgestelde CSA-verordening en de TOI-verordening en zal zich er voor inzetten dat, waar mogelijk, de verwijdering van zowel terroristische online-inhoud als online kinderpornografisch materiaal op een uniforme wijze kan worden ingericht.

Voor wat betreft de verhoudingen met andere wetgeving zijn de leden van de SP-fractie ook geïnteresseerd in de verhouding tot de huidige Richtlijn elektronische handel en de toekomstige DSA. Welke verplichting bevat de DSA ten behoeve van illegale inhoud? Komt er eindelijk een vergewisplicht voor internetgebruikers, zoals de SP-leden eerder hebben bepleit?

De DSA, waarover in april van dit jaar een voorlopig politiek akkoord is bereikt, bevat minimumvereisten voor het tegengaan van álle onrechtmatige en strafbare content. Tussenpersonen die hostingdiensten aanbieden worden onder meer verplicht om een elektronische procedure in te richten waarmee derden de mogelijkheid krijgen om vermeende illegale inhoud onder de aandacht te brengen van die tussenpersonen. Die meldingen moeten voldoen aan minimale (kwaliteit)eisen. Na het behandelen van de melding moet de aanbieder van hostingdiensten de melder tekst en uitleg geven over zijn besluit. Aanbieders van hostingdiensten die tevens aan de definitie van online platform voldoen worden verplicht tot aanvullende maatregelen. Zij moeten bijvoorbeeld een interne bezwaarprocedure hebben waarmee gebruikers bezwaar kunnen maken tegen besluiten om bijvoorbeeld informatie of gebruikersaccounts te verwijderen. Verder moeten ze procedures inrichten voor «vertrouwde melders». Daarnaast moet een online platform dat kennis verkrijgt van een dreigend strafbaar feit met gevolgen voor de veiligheid of het leven van een persoon daar melding van maken bij de bevoegde nationale instantie(s). Ook mogen online platformen die consumenten de mogelijkheid bieden online een aankoop te doen alleen handelaren op hun platform toelaten die bepaalde gegevens hebben verstrekt en zijn ze verplicht te controleren of die informatie betrouwbaar is (zgn. «know-your-business customer» concept).
Aan very large online platforms («VLOPs») worden nog verdere verplichtingen opgelegd. Die zien niet alleen op de bestrijding van illegale inhoud, maar ook op het adresseren van systemische risico's. Mede daarom worden ze verplicht jaarlijks een risicoanalyse te verrichten waarbij wordt onderzocht voor welke systemische risico's de diensten die zij aanbieden vatbaar zijn.
In de DSA is geen algemene vergewisplicht opgenomen. Ook de TOI-verordening strekt niet tot introductie van een vergewisplicht. Een vergwisplicht verplicht de uploader van het materiaal zich er van te vergwissen dat het materiaal dat hij upload met toestemming van de eigenaar of afgebeelde plaatsvindt. De ATKM richt zich op strafbare terroristische online-inhoud. Voor strafbaar materiaal is het niet relevant dat een internetgebruiker zich vergewist van de toestemming of rechtmatigheid omdat het materiaal vanwege zijn de strafbaarheid in het geheel niet opgeslagen of verspreid mag worden onder het publiek. Rondom het vergewissen als internetgebruiker voor onrechtmatig materiaal verwijs ik u naar mijn schriftelijke antwoorden op vragen van het lid Van Nispen (SP) aan de Minister van Justitie en Veiligheid over een vergewisplicht voor websites met naaktbeelden en pornografisch materiaal op 30 maart jl.[15].

[15] Aanhangsel Handelingen II 2020–21, nr. 2277.

3.3. Toezicht, bevoegdheden en handhaving

De leden van de VVD-fractie merken op dat in de memorie van toelichting een aantal opmerkingen zijn gemaakt over de taken, de bevoegdheden en de handhaving die het wetsvoorstel toekent aan de Autoriteit. Zo is onder andere opgenomen dat de Autoriteit de ambtenaren aanwijst die belast zijn met het toezicht op de naleving. Deze leden hebben hier een aantal vragen over.
De monitor van de TU Delft wordt nergens in de memorie van toelichting genoemd. De leden van de VVD-fractie begrijpen uit de Kamerbrief van 29 juni 2022 (2022D27927) over de rapportage van de TU Delft dat de monitor op termijn wordt overgedragen aan de Autoriteit en dat de Autoriteit op termijn de monitor zal gebruiken ten behoeve van diens monitoringstaak. Kan de regering toelichten op welke manier de monitor in de toekomst wordt gebruikt, waarom is gekozen daar in onderhavig wetsvoorstel geen aandacht aan te besteden en kan zij tevens bevestigen dat de TU Delft ook de komende jaren via rapportages de prestaties van hostingbedrijven inzichtelijk blijft maken en dat er aldus ook sprake blijft van naming en shaming van hostingbedrijven die onvoldoende voortgang boeken bij het tijdig uitvoeren van verwijderingsbevelen?

De Monitor inzake online seksueel kindermisbruik waaraan in de brief van 29 juni 2022 wordt gerefereerd is door de TU Delft ontwikkeld en heeft betrekking op online seksueel kindermisbruik.[16] Deze onafhankelijke monitor geeft inzicht in hoeveel beeldmateriaal van seksueel kindermisbruik er in Nederland wordt gehost, welke bedrijven dit doen en hoe lang dit materiaal online staat. Ik ben voornemens de taak om dat materiaal ontoegankelijk te doen maken in het wetsvoorstel bestuursrechtelijke aanpak online kinderpornografisch materiaal aan de ATKM te attribueren. Ten behoeve van diens monitoringsbevoegdheid wordt de monitor daarom op termijn aan de ATKM overgedragen. Deze Uitvoeringswet heeft betrekking op de uitvoering van de TOI-verordening en ziet op terroristische online-inhoud. Om die reden is er in deze Uitvoeringswet en bijbehorende memorie van toelichting geen aandacht besteed aan de Monitor.

De leden van de CDA-fractie vragen hoe de regering zorgt voor een goede rollenscheiding van de toezichtstaak van de (tijdelijke) Autoriteit ten opzichte van de beleidsfunctie van de NCTV, waar het beleid is belegd? Voorts vragen de voornoemde leden wat de relatie wordt van de regering tot de tijdelijke Autoriteit?

De ATKM wordt opgericht met twee hoofdtaken, het tegengaan van de verspreiding van terroristische online-inhoud en de aanpak van online kinderpornografisch materiaal. De Minister van Justitie en Veiligheid is zowel beleidsverantwoordelijk voor contra-terrorisme en daarmee voor de implementatie van de TOI-verordening, als voor de aanpak van online kinderpornografisch materiaal. Daarmee is hij ook verantwoordelijk voor de wetgeving daaromtrent. Binnen het ministerie zijn deze taken belegd bij de NCTV respectievelijk het Directoraat-Generaal rechtspleging en rechtshandhaving(DGRR). De NCTV voert in het kader van haar beleidsrol een dialoog met de internetsector waarbij wordt gesproken over best practices en kennis wordt gedeeld. Ook laat de NCTV onderzoek uitvoeren naar de rol van internet op radicaliseringsprocessen.
Deze beleidsverantwoordelijkheid moet los worden gezien van de taken van het ATKM. Die taken worden krachtens deze wet toegekend aan het zelfstandig bestuursorgaan zelf, waarmee oordeelsvorming onafhankelijk van de Minister is geborgd. De bevoegdheden die de Kaderwet zbo's

[16] Kamerstukken II 2021/22, 34 843, nr. 61.

toekent aan de Minister, zijn in het wetsvoorstel zodanig ingeperkt, dat de Minister uitsluitend kan ingrijpen ten aanzien van het financieel beheer en de administratieve organisatie. De Minister kan zich aldus niet mengen in de inhoudelijke uitoefening van de taak van de autoriteit.
Er wordt geen tijdelijke autoriteit ingericht. Zie voor nadere toelichting op dit onderdeel de beantwoording van de vragen van de CDA-fractie onder 3.2. over de voorbereiding van de bouw van de autoriteit.

3.4. Rechtsbescherming

De leden van de VVD-fractie lezen in de memorie van toelichting dat aanbieders van hostingdiensten en aanbieders van content de besluiten op grond van de TOI-verordening kunnen betwisten bij de Autoriteit zelf in bezwaar en vervolgens bij de bestuursrechter en in hoger beroep bij de Afdeling bestuursrechtspraak van de Raad van State. Is bekend hoeveel zaken naar verwachting in bezwaar en hoger beroep zullen worden gevoerd op grond van onderhavig wetsvoorstel?

Het is op dit moment lastig in te schatten hoeveel terroristisch online-inhoud wordt geplaatst en daarmee ook hoeveel verwijderingsbevelen zullen worden uitgevaardigd. Omdat bezwaar en beroep wordt ingesteld naar aanleiding van deze verwijderingsbevelen, is het thans heel lastig in te schatten hoeveel bezwaar- en beroepzaken zullen worden ingesteld.

De leden van de D66-fractie merken op dat de Afdeling constateert dat er bevoegdheden worden gecreëerd voor onderzoek op het publieke internet middels geautomatiseerde monitoringsinstrumenten waarbij bijzondere persoonsgegevens mogen worden verwerkt, zonder dat de onderzoekstaak en de grenzen daarvan nader worden toegelicht. Deze leden delen de constatering dat juist bij bevoegdheden die ingrijpen in het recht op bescherming van de persoonlijke levenssfeer en de vrijheid van meningsuiting, deze afbakening van groot belang is. Waarom kiest de regering er niet voor deze verregaande bevoegdheden in te kaderen, ondanks het advies van de Afdeling en de wettelijke verplichtingen daartoe?

Deze uitvoeringswet regelt op nationaal niveau wat nodig is om de verordening goed uit te voeren en daarmee uitvoering te geven aan de verplichting die op de lidstaten rust om zorg te dragen voor de effectieve werking van de verordening. De verordening verplicht de lidstaten om ervoor te zorgen dat hun bevoegde autoriteiten over de bevoegdheden beschikken om de doelstellingen van de verordening te verwezenlijken (artikel 13, eerste lid van de verordening). Onder de doelstellingen van de verordening valt ook het identificeren van terroristische online-inhoud. Deze taak is in artikel 2, derde lid van de uitvoeringswet aan de Autoriteit toebedeeld.
De reikwijdte van deze taak wordt bepaald door de verordening zelf. De verordening stelt regels om het misbruik van hostingdiensten voor de verspreiding onder het publiek van terroristische online-inhoud tegen te gaan. Gelet hierop ziet het onderzoeksgebied van de Autoriteit enkel op materiaal dat zich op het openbare internet bevindt. 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. Uit de verordening volgt, nu het niet mogelijk is terroristische online-inhoud op een andere wijze te identificeren, dat de Autoriteit bevoegd is onderzoek te doen op het openbare internet. Nu die bevoegdheid niet door de verordening wordt beperkt, past het niet deze (alsnog) in de Nederlandse wetgeving te beperken.
Dat neemt niet weg dat de door de verordening aan de Autoriteit toegekende taak wel op andere wijze wordt beperkt. 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. 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).
Verder 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 van dit materiaal.
Voor de volledigheid zij vermeld dat de Autoriteit in het kader van het onderzoek op het openbare internet persoonsgegevens kan verwerken. Omdat daarbij mogelijk (bijzondere) persoonsgegevens worden verwerkt is in artikel 9 van onderhavig voorstel voorzien in een grondslag voor het verwerken van bijzondere persoonsgegevens.

Met betrekking tot de proportionaliteit van de maatregelen die de Autoriteit kan treffen stelt de regering dat die afhankelijk is van een veelheid van factoren. Op basis waarvan dient de Autoriteit die factoren te toetsen en hoe wordt toezicht hierop gehouden?

De Autoriteit kan op grond van artikel 5, vierde lid van de verordening op basis van objectieve factoren, zoals het feit dat de aanbieder van hostingdiensten in de voorafgaande twaalf maanden twee of meer definitieve verwijderingsbevelen heeft ontvangen, vaststellen dat een aanbieder van hostingdiensten is «blootgesteld» aan terroristische online-inhoud. De Autoriteit neemt dan een zogeheten blootstellingsbesluit. Dit blootstellingsbesluit verplicht de aanbieder van hostingdiensten er toe specifieke maatregelen te treffen om zijn diensten te beschermen tegen de verspreiding van terroristische online-inhoud onder het publiek. In het tweede lid van artikel 5 van de verordening is een niet-limitatieve opsomming opgenomen van de specifieke maatregelen die kunnen worden getroffen. Tevens moeten de maatregelen voldoen aan voorwaarden genoemd in artikel 5, lid 3 van de verordening. Zo moeten de maatregelen doeltreffend, doelgericht en evenredig zijn en moeten zij worden toegepast op een zorgvuldige en niet-discriminerende wijze. Daarnaast moeten zij worden toegepast op een manier die de rechten en rechtmatige belangen van de gebruikers ten volle in acht neemt, met name de grondrechten van de gebruikers inzake de vrijheid van meningsuiting en van informatie, de eerbiediging van het privéleven en de bescherming van persoonsgegevens. Of maatregelen die worden getroffen door een aanbieder van hostingdiensten proportioneel en effectief zijn, is afhankelijk van een veelheid aan factoren, die per geval verschillen. Daarbij is onder andere relevant hoeveel verwijderingsbevelen aan deze aanbieder van hostingdiensten zijn uitgevaardigd, wat de omvang en economische draagkracht van de aanbieder van hostingdiensten is, wat de invloed van zijn diensten op de verspreiding van terroristische inhoud is, bijvoorbeeld op basis van het aantal gebruikers in de Unie, alsook welke waarborgen zijn ingevoerd om misbruik van zijn diensten voor de verspreiding van terroristische online-inhoud tegen te gaan. In aanvulling hierop wordt expliciet aandacht besteed aan de aard en grootte van de betrokken aanbieders van hostingdiensten, 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.[17]
De aanbieder van hostingdiensten dient binnen drie maanden na ontvangst van het blootstellingsbesluit en vervolgens op jaarbasis verslag uit te brengen over de getroffen maatregelen. Indien de Autoriteit op basis van dat verslag en, in voorkomend geval, andere objectieve factoren van oordeel is dat de genomen specifieke maatregelen niet voldoen aan de leden 2 en 3 van artikel 5 van de TOI-verordening, richt de bevoegde autoriteit een besluit tot de aanbieder van hostingdiensten dat hem ertoe verplicht de aanvullende maatregelen te nemen om ervoor te zorgen dat aan de leden 2 en 3 wordt voldaan. De Autoriteit ziet daar op toe.

De leden van de CDA-fractie merken op dat de procedure waarin aanbieders van hostingdiensten en aanbieders verwijderingen kunnen betwisten voor hen duidelijk is. Vindt er vanuit het ministerie regelmatig contact plaats met een aantal hostingsdiensten en aanbieders om uit te leggen welke content verboden is? Met andere woorden, worden deze aanbieders op de hoogte gehouden, zodat men zelf in staat is voortijdig content te weren of te verwijderen voordat de Autoriteit hiertoe moet bevelen?

De ATKM krijgt een belangrijke voorlichtende rol om de aanbieders te ondersteunen bij de beoordeling van terroristische online-inhoud. Ook om ervoor te zorgen dat er geen materiaal wordt verwijderd door specifieke maatregelen van aanbieders van hostingdiensten dat geen terroristische online-inhoud bevat. Dit teneinde het recht op vrijheid van meningsuiting te borgen.

De leden van de SP-fractie hebben in het verleden kritische vragen gesteld over de rechtsbescherming van hostingdiensten en internetgebruikers inzake dit wetsvoorstel. De zorg van deze leden zit met name in het honoreren van verwijderingsbevelen van autoriteiten uit andere lidstaten en de rechtsbescherming die daarbij komt kijken. Hebben deze leden het goed begrepen dat hostingdiensten altijd achteraf bezwaar kunnen maken tegen het verwijderingsbesluit en tegen blootstellingsbesluiten in de lidstaat waar deze hostingdienst zich heeft gevestigd en dat altijd binnen maximaal 72 uur een besluit wordt genomen over de rechtmatigheid van het genomen besluit? Betekent dit dus dat verwijdering nooit vooraf tegen kan worden gehouden? Hoe verhoudt dit voorstel zich volgens de regering tot de motie van de leden Van Nispen en Van Toorenburg (Kamerstuk 22 112, nr. 2724)? In de memorie van toelichting licht de regering toe dat er achteraf rechtsmiddelen openstaan, maar de motie beschrijft toch duidelijk dat de nationale autoriteiten niet tussen verwijderingsbevelen van andere lidstaten moeten komen en dus niet achteraf met deze verzoeken moeten komen? Waarom meent de regering dan toch dat aan de motie is voldaan?

Het is juist dat een aanbieder van hostingdiensten in eerste instantie binnen de termijn van één uur gevolg dient te geven aan het buitenlandse verwijderingsbevel. Op grond van artikel 4, derde lid en verder, van de TOI-verordening heeft iedere Autoriteit evenwel het recht om binnen 72 uur een met redenen omkleed besluit te nemen, houdende dat een buitenlands 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. Daarnaast kunnen ook aanbieders van

[17] 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.

hostingdiensten of aanbieders van inhoud de Autoriteit in het land van vestiging hierom verzoeken door binnen 48 uur na ontvangst van het verwijderingsbevel een met redenen omkleed verzoek in te dienen bij de bevoegde autoriteit in de eigen lidstaat. Een positieve beslissing van de Autoriteit is bindend voor de uitvaardigende lidstaat, en verplicht de uitvaardigende lidstaat ertoe zijn verwijderingsbevel in te trekken. Het verwijderingsbevel heeft in dat geval geen rechtsgevolgen meer en de aanbieder van hostingdiensten herstelt de inhoud of maakt die weer toegankelijk.
De motie Van Nispen/Van Toorenburg[18] roept de regering op zich te verzetten tegen een voorstel waarin een verwijderingsbevel uit een andere lidstaat rechtstreeks, zonder tussenkomst van een autoriteit in de ontvangende lidstaat, moet worden opgevolgd door een internetbedrijf, als daartegen geen rechtsmiddel openstaat in de ontvangende lidstaat. De inzet van de regering tijdens de onderhandelingen over de verordening is er steeds op gericht geweest te voorkomen dat een grensoverschrijdend verwijderingsbevel zonder tussenkomst van een autoriteit in de ontvangende lidstaat, moet worden opgevolgd door een aanbieder van hostingdiensten. Daarmee is aan de motie voldaan. Uiteindelijk is in de verordening voorzien in de mogelijkheid voor de autoriteit in de ontvangende lidstaat om te interveniëren bij een grensoverschrijdend verwijderingsbevel uit een andere lidstaat, overeenkomstig de wijze die Nederland voorstond.

Deelt de regering dat dit voorstel een vergaande impact heeft op de vrijheid van meningsuiting en dat deze verordening en de uitvoeringswet een ongekend precedent stellen in de geschiedenis van de Europese integratie? Zo nee, waarom niet? Zo ja, waarom legt de regering zich er dan bij neer?

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, met name de vrijheid van meningsuiting. 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. 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, derde lid 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

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

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 taakuitoefening onafhankelijk van de politiek. In aanvulling daarop is 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.
Ook voor aanbieders van hostingdiensten geldt dat zij bij het nemen van specifieke maatregelen dit op zorgvuldige, evenredige en niet-discriminerende wijze behoren te 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. Gelet op het voorgaande is de regering van oordeel dat de inbreuk die met de verordening en de Uitvoeringswet kan worden gemaakt op de vrijheid van meningsuiting gerechtvaardigd is en met voldoende waarborgen is omkleed.

Hoe zit het met internetgebruikers? Kunnen zij ook bezwaar maken wanneer hun materiaal in hun ogen onrechtmatig wordt verwijderd?

Op grond van artikel 9, tweede lid van de verordening hebben aanbieders van inhoud wiens inhoud na een verwijderingsbevel verwijderd is of waartoe de toegang na een verwijderingsbevel geblokkeerd is, recht op een doeltreffende voorziening in rechte. Dat recht omvat ten eerste het recht om 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. Ten tweede heeft de aanbieder van inhoud op grond van artikel 4, lid 4 van de verordening het recht om binnen 48 uur na ontvangst van respectievelijk een verwijderingsbevel of informatie op grond van artikel 11, lid 2, een met redenen omkleed verzoek in te dienen bij de bevoegde autoriteit van de lidstaat waar de aanbieder van hostingdiensten zijn hoofdvestiging of waar zijn wettelijke vertegenwoordiger zijn verblijf- of vestigingsplaats heeft, om het verwijderingsbevel te toetsen zoals bedoeld in de eerste alinea van artikel 4, lid 3 van de verordening. De hier genoemde besluiten die door de Nederlandse autoriteit zijn genomen, zijn onderworpen aan de gebruikelijke bestuursrechtelijke 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.

De leden van de SP-fractie lezen in artikel 8 van de voorgestelde uitvoeringswet dat de AOTKM verkregen persoonsgegevens of inlichtingen met de politie, het OM, de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en Militaire Inlichtingen- en Veiligheidsdienst (MIVD) mogen delen. Informatie kan tevens met Europol uitgewisseld worden. Kan de regering dit toelichten? Hoe verhoudt dit zich tot de keuze de AOTKM aan te wijzen

als bestuursrechtelijk bestuursorgaan? Hoe wordt voorkomen dat de AOTKM een verlengstuk wordt van één van de diensten?

Op grond van de verordening en de Uitvoeringswet heeft de ATKM eigen taken en eigen bevoegdheden. Dit neemt niet weg dat er raakvlakken zijn met het werk van andere instanties. Artikel 8 van de Uitvoeringswet bevat daarom 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 ATKM het voorkomen, onderzoeken, opsporen en vervolgen van terroristische misdrijven op enige manier belemmert. Tevens is een bevoegdheid opgenomen voor de autoriteit om gegevens die verkregen zijn bij de uitvoering van zijn taken te delen met de politie en de inlichtingendiensten MIVD en AIVD voor zover deze noodzakelijk kunnen zijn bij de uitoefening van hun taken.
Daarnaast bepaalt artikel 14, eerste lid van de verordening dat de bevoegde autoriteiten informatie uitwisselen met elkaar en waar passend met Europol met betrekking tot verwijderingsbevelen. Dit met name teneinde dubbel werk te voorkomen, de coördinatie te verbeteren en inmenging in onderzoeken in verschillende lidstaten te voorkomen.
Het voorgaande staat los van de keuze om de ATKM als zelfstandig bestuursorgaan met bestuursrechtelijke bevoegdheden vorm te geven en beoogt te voorkomen dat de autoriteit de werkzaamheden van opsporings- en veiligheidsdiensten doorkruist danwel de coördinatie te verbeteren. Het is aan de autoriteit om te beoordelen of hij deling van persoonsgegevens verkregen bij zijn taak noodzakelijk acht voor de uitoefening van de taken van de politie en de veiligheidsdiensten. De hiervoor genoemde verplichting voor de autoriteit om over de uitoefening van zijn taken overleg te voeren laat onverlet dat elke instantie op grond van zijn eigen taak en omstandigheden beoordeelt welke werkzaamheden zij uitvoert en van welke bevoegdheden hij gebruikt maakt.

Daarnaast zijn deze leden benieuwd hoe de NCTV zich gaat verhouden tot de AOTKM. Dit wordt niet of onvoldoende toegelicht in de memorie van toelichting. De NCTV is echter wel tot een berekening van de geschatte kosten van de AOTKM gekomen en ook van de subsidies die ten behoeve van de NCTV worden ingezet. Graag een toelichting van de regering op de rol van de NCTV.

De ATKM wordt opgericht met twee hoofdtaken, het tegengaan van de verspreiding van terroristische online-inhoud en de aanpak van online kinderpornografisch materiaal. De Minister van Justitie en Veiligheid is zowel beleidsverantwoordelijk voor contra-terrorisme en daarmee voor de implementatie van de TOI-verordening, als voor de aanpak van online kinderpornografisch materiaal. Daarmee is hij ook verantwoordelijk voor de wetgeving daaromtrent. Binnen het ministerie zijn deze taken belegd bij de NCTV respectievelijk het Directoraat-Generaal rechtspleging en rechtshandhaving(DGRR). Zo voert de NCTV in het kader van haar beleidsrol een dialoog met de internetsector waarbij wordt gesproken over best practices en kennis wordt gedeeld. Ook laat de NCTV onderzoek uitvoeren naar de rol van internet op radicaliseringsprocessen.
Deze beleidsverantwoordelijkheid moet los worden gezien van de taken van het ATKM. Die taken worden krachtens deze wet toegekend aan het zelfstandig bestuursorgaan zelf, waarmee oordeelsvorming onafhankelijk van de Minister is geborgd. De bevoegdheden die de Kaderwet zbo's toekent aan de Minister, zijn in het wetsvoorstel zodanig ingeperkt, dat de Minister uitsluitend kan ingrijpen ten aanzien van het financieel beheer en de administratieve organisatie. De Minister kan zich aldus niet mengen in de inhoudelijke uitoefening van de taak van de autoriteit.

3.5. Verhouding tot het strafrecht

De leden van de VVD-fractie onderschrijven de keuze van de regering om naast een strafrechtelijke aanpak ook een bestuursrechtelijk aanpak te introduceren in de vorm van een notice-and-takedown procedure met een bestuurlijke boete. Kan de regering toelichten wat de voorzienbare strafrechtelijke route is ingeval een hostingbedrijf herhaaldelijk een verzoek tot verwijderen negeert of herhaaldelijk bestuurlijke boetes krijgt opgelegd? Kan dan enkel strafrechtelijke vervolging plaatsvinden ex artikel 184 en 184a Sr? Kan de regering aangeven in welke gevallen sprake is van bestuurdersaansprakelijkheid wegens het inbreuk maken op de verordening?

De autoriteit kan een bestuursrechtelijke sanctie opleggen bij het niet (tijdig) opvolgen van het verwijderingsbevel, waarbij het de keuze heeft uit de last onder dwangsom en een bestuurlijke boete. Indien een aanbieder van hostingdiensten systematisch of aanhoudend weigert (tijdig) opvolging te geven aan een verwijderingsbevel, bedraagt de op te leggen bestuurlijke boete ten hoogste het bedrag dat is vastgesteld voor de zesde categorie, bedoeld in artikel 23, vierde lid, van het Wetboek van Strafrecht of, indien dat meer is, ten hoogste 4% van de mondiale omzet van de onderneming, onderscheidenlijk, indien de overtreding door een ondernemersvereniging is begaan, van de gezamenlijke omzet van de ondernemingen die van de vereniging deel uitmaken, in het boekjaar voorafgaande aan de beschikking waarin de bestuurlijke boete wordt opgelegd. Daarnaast kan de autoriteit op grond van artikel 5, vierde lid van de verordening op basis van objectieve factoren, zoals het feit dat de aanbieder van hostingdiensten in de voorafgaande twaalf maanden twee of meer definitieve verwijderingsbevelen heeft ontvangen, vaststellen dat een aanbieder van hostingdiensten is blootgesteld aan terroristische online-inhoud. Als de autoriteit gelet daarop een blootstellingsbesluit heeft genomen en dit besluit aan de aanbieder van hostingdiensten heeft medegedeeld, neemt de aanbieder van hostingdiensten specifieke maatregelen om zijn diensten te beschermen tegen de verspreiding van terroristische online-inhoud onder het publiek. Ook bij het niet (tijdig) opvolgen van een blootstellingsbesluit kan de autoriteit een last onder dwangsom of een bestuurlijke boete opleggen. De TOI-verordening en de Uitvoeringswet voorzien derhalve reeds in bestuursrechtelijke sanctiemogelijkheden. Toepassing van de artikelen 184 en 184a Sr (niet opvolgen ambtelijk bevel) is derhalve niet aan de orde.
Strafrechtelijke vervolging van een hostingsdienst kan wél aan de orde zijn indien de aanbieder van hostingdiensten 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 hostingdienst 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.

De leden van de SP-fractie lezen terechte punten van zorg bij de Afdeling om de bevoegdheden niet bij het OM te beleggen. De regering kiest er immers voor een bestuursrechtelijke grondslag te creëren. Kan de regering toelichten hoe deze keuze zich verhoudt tot artikel 125p van het Wetboek van Strafvordering?

Bij het tot stand komen van de Uitvoeringswet 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. Deze bepaling maakt het mogelijk om in het kader van een verdenking van een misdrijf als omschreven in artikel 67, eerste

lid, Sv een strafrechtelijk bevel tot ontoegankelijkmaking uit te vaardigen aan een aanbieder van een communicatiedienst. Hiervoor is toestemming van de officier van justitie vereist, evenals een voorafgaande machtiging van de rechter-commissaris. Er is niet voor gekozen de TOI-verordening met behulp van artikel 125p Sv uit te voeren. Van belang daarbij is dat strafrechtelijke vervolging van een aanbieder van hostingdiensten, als deze in beeld komt bij het 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 hostingdienst 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. Een krachtens artikel 125p Sv gegeven bevel kan strekken tot de ontoegankelijkmaking van elk type gegevens. Daarnaast is de verordening er op gericht terroristische online-inhoud zo snel mogelijk offline te doen halen en niet om degene die terroristische online-inhoud op internet plaatsen te vervolgen Tevens 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.

4. Financiële gevolgen

4.1. Financiële gevolgen voor het Rijk

De leden van de SP-fractie vragen de regering of zij vindt dat het wetsvoorstel wel deugdelijk is onderbouwd. Zij vernemen dat € 400.000 structureel vanuit de Internet Referral Unit (IRU) worden overgedragen aan de AOTKM. Wordt daarmee de IRU volledig opgeheven? Hoe verschillen de taken van de IRU van de AOTKM? Daarnaast zijn deze leden met name geïnteresseerd in de kasschuif die plaats lijkt te vinden met de onderbesteding van de middelen van de IRU uit de jaren 2018, 2019 en 2020. Waarom vond daar onderbesteding plaats en wordt die nu pas ingezet? De nationale politie kampt toch ook met forse tekorten. Waarom zijn die middelen niet daaraan toegevoegd? Was er in 2021 ook sprake van onderbesteding?
Daarnaast lezen de leden van de SP-fractie dat middelen uit het Fonds voor Interne Veiligheid zullen worden aangewend ten behoeve van de AOTKM. Deze middelen zijn echter aan de NCTV toegekend, zo begrijpen deze leden ten behoeve van interne projecten. Maar de AOTKM is toch geen intern project van de NCTV? Wat vindt de AR eigenlijk van deze dekking?

Ten behoeve van de beantwoording van de vragen over de financiering van de ATKM wordt eerst ingegaan op de structurele financiering van de ATKM en eventuele aanwending van middelen uit het EU fonds voor interne veiligheid. Vervolgens wordt ingegaan op de onderbesteding bij de internet referral unit (IRU) en de taken van de IRU. Vervolgens wordt antwoord gegeven op de vragen over de rol van de NCTV.

Structurele financiering en aanwending middelen uit het EU fonds voor interne veiligheid

Voor financiering van het wetsvoorstel wordt primair een bedrag vrijgemaakt binnen de begroting van het Ministerie van Justitie en Veiligheid van 1,2 miljoen euro per jaar (2022) oplopend naar 3,2 miljoen euro structureel (v.a. 2027). Daarnaast is eveneens structureel, 0,4 miljoen euro per jaar beschikbaar vanuit de onderbesteding van de Internet Referal Unit (IRU).
Deze structurele financiering dient in samenhang gezien te worden met de structurele financiering van 2,5 miljoen euro per jaar die eveneens binnen de begroting van het Ministerie van Justitie en Veiligheid is vrijgemaakt voor het wetsvoorstel bestuursrechtelijke aanpak online kinderpornografisch materiaal, dat uw Kamer naar verwachting na de zomer wordt toegezonden. Ingeschat wordt dat deze structurele financiering vooralsnog voldoende is om de ATKM te bekostigen.
In aanvulling op deze structurele financiering bestaat de mogelijkheid om een beroep te doen op het EU- fonds voor interne veiligheid voor kosten in de aanloopfase, opbouw of doorontwikkeling in de eerste jaren, bijvoorbeeld wanneer blijkt dat extra investeringen nodig zijn.

Onderbesteding IRU en taken IRU

De IRU is onderdeel van de Open Source Intelligence (OSINT)-afdeling van de Nationale Politie. Hiervoor is in 2018 ongeveer 1,7 miljoen euro beschikbaar gekomen als onderdeel van de door het kabinet Rutte III vrijgemaakte extra CT-gelden.[19] De onderbesteding bestaat uit het niet vanaf het begin volledig kunnen invullen van de bij haar oprichting ingeschatte maximale capacitaire behoefte van de IRU. Er was sprake van een opbouw- en ingroeimodel.
Met de komst van de ATKM wordt de IRU opgeheven en gaat de content moderatie taak (het detecteren van terroristische content met het oog op het doen verwijderen van deze content door hosting bedrijven) over naar de ATKM. Op het moment dat duidelijk werd dat voor deze taak een nieuwe autoriteit zou worden ingericht, is met de politie afgesproken de capaciteit van de IRU te bevriezen en de vrijvallende middelen aan te wenden voor de financiering van de (inrichting van deze) autoriteit. Met de Nationale Politie zullen afspraken worden gemaakt over samenwerking en snijvlaktaken.
De wel voor de IRU aangewende middelen en capaciteit zijn ten behoeve van haar bredere OSINT-taken in het CT-domein en zijn ondergebracht binnen de OSINT-eenheid bij de politie. De inzet wordt periodiek heroverwogen afhankelijk van prioriteitstelling binnen het CT-domein.

Rol en taken van de NCTV

De ATKM wordt opgericht met twee hoofdtaken, het tegengaan van de verspreiding van terroristische online-inhoud en de aanpak van online kinderpornografisch materiaal. De Minister van Justitie en Veiligheid is zowel beleidsverantwoordelijk voor contra-terrorisme en daarmee voor de implementatie van de TOI-verordening, als voor de aanpak van online kinderpornografisch materiaal. Daarmee is hij ook verantwoordelijk voor de wetgeving daaromtrent. Binnen het ministerie zijn deze taken belegd bij de NCTV respectievelijk DGRR. Deze beleidsverantwoordelijkheid moet

[19] Met het Regeerakkoord »Vertrouwen in de toekomst» (2017–2021) is met ingang van 2018 € 8 miljoen en vanaf 2019 jaarlijks € 13 miljoen extra per jaar beschikbaar gekomen voor contraterrorisme (CT). Een overzicht van de verdeling en besteding van de additionele gelden is op 28 november 2017 samen met de Notitie Integrale aanpak terrorisme 2017–2021 naar uw Kamer gestuurd (Kamerstukken II 2017/18, 29 754, nr. 436).

los worden gezien van de taken van het ATKM. Die taken worden krachtens deze wet toegekend aan het zelfstandig bestuursorgaan zelf, waarmee oordeelsvorming onafhankelijk van de Minister is geborgd. De bevoegdheden die de Kaderwet zbo's toekent aan de Minister, zijn in het wetsvoorstel zodanig ingeperkt, dat de Minister uitsluitend kan ingrijpen ten aanzien van het financieel beheer en de administratieve organisatie. De Minister kan zich aldus niet mengen in de inhoudelijke uitoefening van de taak van de autoriteit. Om praktische redenen is er voor gekozen om de financiering in de opbouwfase via het budget van de NCTV te laten lopen.

4.2. Financiële gevolgen voor de sector

In een aantal sectoren, denk aan de bankensector en de accountancy, betalen de ondernemingen die actief zijn in de sector voor de structurele inzet van het toezicht. De leden van de CDA-fractie vragen waarom er in dit geval niet voor gekozen is de hostingsbedrijven en aanbieders een heffing te laten betalen waaruit de Autoriteit gefinancierd wordt? Het is toch ook in het belang van de sector dat geen terroristische inhoud verspreid wordt via hun dienstverlening, zo menen deze leden. Om welke bedragen zou het gaan, indien de structuur van het toezicht op banken en accountants zou worden gevolgd, voor een gemiddeld hostingbedrijf? Is het niet vreemd dat de gewone belastingbetaler nu moet betalen voor een Autoriteit omdat hostingsbedrijven soms terroristische content aanbieden?

Momenteel is voorzien in een 100% dekking van de kosten van het ATKM door het Rijk. Hiervoor is gekozen omdat maar een beperkt aandeel van de aanbieders van hostingdiensten wordt geconfronteerd met terroristische online-inhoud op hun diensten. 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 ATKM ziet erop toe dat een bevel wordt opgevolgd als er terroristisch online-inhoud wordt aangetroffen en treedt zo nodig op door het opleggen van een bestuursrechtelijke sanctie. Hiermee betalen niet welwillende aanbieders van hostingdiensten die niet opereren conform de TOI-verordening indirect mee. Het geld dat wordt betaald als gevolg van bestuursrechtelijke sancties stroomt immers terug in de schatkist terwijl de rest van de sector niet onevenredig wordt geraakt.

5. Advisering

Verhouding Autoriteit – OM

De leden van de VVD-fractie zijn van mening dat het een verstandige keuze is van de regering te expliciteren dat er afstemming plaatsvindt tussen het OM en de Autoriteit, om te voorkomen dat in individuele zaken de opsporing, vervolging en berechting van misdrijven wordt verstoord. Het is belangrijk dat de Autoriteit, de opsporings- en inlichtingendiensten, het OM en de politie goede afspraken maken hoe de afstemming op grond van artikel 8 van de uitvoeringswet vorm krijgt. Gebeurt dat in de vorm van formele samenwerkingsafspraken op grond van een protocol? Deelt de regering de mening dat het ook verstandig kan zijn dat de Autoriteit in overleg met de opsporingsdiensten kan aangeven dat het wenselijk is een strafrechtelijk traject te beginnen wanneer de Autoriteit merkt dat een bestuursrechtelijk traject tot onvoldoende resultaten leidt?

Het kabinet deelt de mening van de VVD-fractie dat goede onderlinge samenwerking tussen de autoriteit, de opsporings- en inlichtingendiensten, het Openbaar Ministerie en de Nationale Politie van groot

belang is. Artikel 8 van de Uitvoeringswet TOI-verordening bepaalt in dat verband dat er zogenoemde «deconflictie» plaatsvindt: de Autoriteit voert over de uitoefening van zijn taken en bevoegdheden overleg met de Nationale 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. Een mogelijke uitkomst van dit overleg kan zijn dat de autoriteit (vooralsnog) afziet van de inzet van bevoegdheden om daarmee de bedoelde doorkruising te voorkomen. Momenteel worden afspraken gemaakt met de AIVD, MIVD en de politie over hoe zij op de hoogte worden gesteld van het voornemen van de autoriteit om een verwijderingsbevel te ontvangen. Of het opportuun is deze afspraken in een protocol op te nemen is nog onderdeel van gesprek.

Bestuursrechtelijke aspecten

De leden van de VVD-fractie vragen of een hostingbedrijf, wanneer een bestuurlijke boete is opgelegd, wordt uitgesloten als leverancier van diensten aan de overheid en andere publieke instellingen? Zo nee, waarom niet en kan dit alsnog worden geregeld?

Op grond van artikel 5:46, tweede lid, van de Algemene wet bestuursrecht geldt 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 kabinet is van mening dat met het voldoen van de bestuurlijke boete in voldoende mate op het niet naleven van de verplichtingen is gereageerd.

II. ARTIKELSGEWIJS

Artikel 9. Bijzondere persoonsgegevens

De leden van de VVD-fractie merken op dat de voorliggende uitvoeringswet in artikel 9 een grondslag biedt voor de verwerking van bijzondere en strafrechtelijke persoonsgegevens door de Autoriteit. Deze grondslag ziet echter alleen op de verwerking van persoonsgegevens voor zover de verwerking noodzakelijk is voor de uitoefening van bevoegdheden op grond van deze wet. Dat betreft het tegengaan van verspreiding van terroristische online-inhoud. Wanneer de Autoriteit ook bevoegdheden zal uitoefenen voor de bestuursrechtelijke aanpak van online kinderpornografisch materiaal, is dan een nadere wettelijke grondslag vereist voor de verwerking van persoonsgegevens?

De taken van de autoriteit ten aanzien van de aanpak van online kinderpornografisch materiaal worden geregeld in het wetsvoorstel bestuursrechtelijke aanpak online kinderpornografisch materiaal. Dat wetsvoorstel bevat tevens een grondslag voor de autoriteit om bijzondere en strafrechtelijke persoonsgegevens te verwerken voor zover de verwerking van deze gegevens noodzakelijk is voor de uitoefening van zijn bevoegdheden op grond van die wet. Dit wetsvoorstel zal naar verwachting na de zomer bij uw Kamer worden ingediend.

De leden van de D66-fractie delen de zorgen van de Afdeling met betrekking tot de omgang met bijzondere persoonsgegevens en zijn niet gerustgesteld door de reactie van de regering. Waarom wordt gekozen voor een bewaartermijn van een jaar «na de laatste verwerking van de persoonsgegevens»? Leidt dit er in de praktijk niet toe dat de bewaartermijn verlengd wordt, iedere keer dat een nieuwe verwerking van persoonsgegevens plaatsvindt? Hoe wordt voorkomen dat gegevens van een bepaalde persoon langer worden opgeslagen door steeds nieuwe

gegevens te verzamelen? Is de regering bereid het advies van de Afdeling over te nemen en een concrete maximale bewaartermijn op te nemen?

Gelet op het beginsel van opslagbeperking is het uitgangspunt dat persoonsgegevens niet langer worden bewaard dan noodzakelijk is voor de doeleinden waarvoor zij zijn verzameld. Voor het onderhavige wetsvoorstel betekent dit dat persoonsgegevens in beginsel dertien maanden 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. Voor de verschillende typen procedures gelden immers bezwaar-, beroeps- en hoger beroepstermijnen waarbinnen een vervolgprocedure kan worden ingesteld. Een bewaartermijn van een jaar na de laatste verwerking van de persoonsgegevens wordt passend geacht, opdat ook de termijn voor het instellen van vervolgprocedures zal zijn verstreken. Na afronding van deze procedures en nadat een eventuele beroepstermijn is verstreken, zal de inhoud worden verwijderd. Gelet hierop kan niet aan het advies van de Afdeling advisering van de Raad van State om een concrete maximale bewaartermijn op te nemen tegemoet worden gekomen. Het is immers afhankelijk van de ingestelde beroep- of klachtenprocedure hoe lang de betreffende persoonsgegevens nodig zijn. Er is bij het voorbereiden van dit wetsvoorstel een Privacy Impact Assessment (hierna: PIA) uitgevoerd om de veiligheidsrisico's in kaart te brengen. Hierop is het beveiligingsniveau afgestemd en zijn passende en specifieke maatregelen genomen, zoals een loggingsverplichting en geheimhoudingsverklaring

Artikel 16. Inwerkingtreding

De leden van de VVD-fractie stellen dat op 7 juni 2022 de TOI-verordening van kracht is geworden. De korte implementatietermijn leidt ertoe dat de verordening niet reeds vanaf die datum kon worden uitgevoerd. Graag ontvangen deze leden een toelichting op het van toepassing worden van de verordening in relatie tot het Nederlandse implementatietraject, zoals ook in de beslisnota bij het wetsvoorstel wordt opgemerkt.

Zie beantwoording vragen fractie CDA over voortgang bij paragraaf 3.2

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